SIEMENS



Manual Collection

SIMATIC

ET 200AL

ET 200AL distributed I/O system

This document contains a compilation of all manuals for the ET 200AL system family.
Use the bookmarks on the edge of the screen to navigate.

Edition 04/2026

support.industry.siemens.com

SIEMENS
SIMATIC

Distributed I/O system ET 200AL

Compact Operating Instructions
Original instructions

1 Notes on Safety and Product Conformity

Function
SIMATIC products control, regulate and monitor applications in automation systems, for example in the field of industrial automation technology and process engineering.

EU and UK Declaration of Conformity

- You can find the EU Declaration of Conformity here on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert?ct=444&ci=526).
- You can find the UK Declaration of Conformity here on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert?ct=444&ci=5596).

Firmware
You will find the latest firmware versions (for devices that support a firmware update) on the Internet (https://support.industry.siemens.com/cs/search?t=all&search=et%20200al&type=Download&lc=en-WW).

Documentation
The complete documentation consists of product information, the system manual, equipment and function manuals. You can find these in the Manual Collection (https://support.industry.siemens.com/cs/ww/en/view/95242965) on the Internet.

Retention of the documentation
Retain this documentation for later use.

1. Download the documentation after receiving your product and before initial installation/commissioning.
2. Retain this version of the documentation.

Updating the documentation
The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above.
2. Also retain this version of the documentation.

© Siemens AG 2022 - 2024. All rights reserved

Intended use
SIMATIC products are intended for use in industry. If you plan to use the product in a different environment, check the conditions required for such use.
The product may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety information. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products.

⚠ WARNING

Intended use
SIMATIC products are intended for automation of machine plants, process control and process engineering. Refer to the associated documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965) to learn about the intended area of application of the respective product (e.g. ambient conditions, possible use in safety-critical systems).
If third-party products and components are used, these have to be recommended or approved by Siemens.
Proper transport, proper storage, setup, assembly/disassembly, installation, commissioning, operation, maintenance and decommissioning are required to ensure that the product and its accessories operate safely and without any problems.
Non-observance may result in death or serious physical injury.
Read the notes in the corresponding documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965)**.**

Observe the ambient conditions for intended operation as described in the "Technical specifications" section of the associated documentation.

⚠ WARNING

Connection of the power supply
The power supply may only be connected by qualified and authorized personnel. In particular, observe the information in the documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965) and on the nameplate of the device.

NOTE
The power supply must be connected by the operator/user in accordance with the national regulations regarding installation.

⚠ WARNING

Danger from voltage/current!
Only perform assembly and disassembly work when the device is de-energized.
Install products with degree of protection IP65/67 according to IEC 60529 weatherproof and stationary indoors.

⚠ WARNING

Safety functional extra low voltage
The product must be operated with safety functional extra low voltage (SELV, PELV). You can find more information on safety functional extra low voltage in the documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965) of the fail-safe I/O and in the data sheets of the power supplies to be used.
Use a power supply unit with output voltage that does not exceed 35 V DC even in the event of a fault.
Follow the notes and warnings in the respective manual.

Electromagnetic Compatibility
The I/O system is intended for operation in the EMC environment class Industry.
Ensure an EMC-compliant design of your automation system as described in the documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965) for the I/O system.

NOTICE
Interference emission / Interference immunity The operation of the I/O system can cause radio interference in residential areas. If higher EMI is expected at the place of use than is intended for the industrial area according to EN61000-6-2, additional measures are required (e.g. ESD, overvoltage protection).

Cleaning
When wired, the product complies with degree of protection IP65/IP67 and does not require any cleaning.
If you do have to clean the product, then use a dry or damp cloth. Take care to comply with the conditions of degree of protection IP65/IP67 when cleaning with liquids.

Maintenance and repair
The product is maintenance-free. Repairs to the product may only be carried out by the manufacturer.

Recycling and disposal
For environmentally sustainable recycling and disposal of your electronic waste, contact a company certified for the disposal of electronic waste. Dispose of the product in accordance with the applicable regulations in your country.

Accessories
You can find information on the approved accessories in the documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965).

Functional safety

⚠ WARNING
Danger to humans and the environment To avoid danger to people and the environment, under no circumstances may you bypass safety functions or take measures that amount to or result in bypassing safety functions. The manufacturer is not liable for the consequences of such manipulation or for damages resulting from the failure to heed this warning.

Perform a safety inspection for safety-related functions throughout the entire system, including all safety-related components. For fail-safe I/O, observe the notes and warnings in the documentation (https://support.industry.siemens.com/cs/ww/en/view/95242965) especially for:

- Connecting/wiring
- Parameter assignment
- Status, fault displays and alarms
- Maintenance (recurring tests, software/firmware updates)
- Checking for proper function
- Technical specifications

You can find use cases for achieving the required safety class (SIL) in the documentation.

⚠ WARNING

Check the firmware version for fail-safe approval
When using a new firmware version, check whether the firmware version is approved for the respective fail-safe I/O.
The attachments of the certificate (https://support.automation.siemens.com/WW/view/en/49368678/134200) for SIMATIC Safety specify the firmware version that is approved.

Ensure that fail-safe capability is enabled for F-CPUs.
The PROFIsafe address must be set or assigned for fail-safe I/O.
Perform function tests for safety functions according to your automation task. They may only be used in production when the correct operation of the safety-related functions is ensured.

2 Use of radio devices and cell phones

⚠ WARNING

Unexpected malfunctions of machines caused by radio devices/cell phones
Malfunctions are possible when radio devices or cell phones are used in the direct proximity of F-I/O. This can result in death, serious injury or property damage.
If you scan the 2D matrix code/ID Link or use the "SIEMENS Industry Support App" with a powered-on F-I/O, then deactivate all radio connections of the radio device/cell phone beforehand. Alternatively, power off the F-I/O before scanning.
Power off radio devices in the immediate proximity of the F-I/O.

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines, and networks.
In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For more information on protective industrial cybersecurity measures for implementation, please visit (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.
To stay informed about product updates at all times, subscribe to the Siemens Industrial Cybersecurity RSS Feed under (https://new.siemens.com/global/en/products/services/cert.html).

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Ⓟ 04/2026 Subject to change

Copyright © Siemens 2026.
All rights reserved

SIEMENS

SIMATIC

ET 200AL
Distributed I/O system

System Manual

08/2025
A5E31861578-AP

Introduction 1
Safety instructions 2
New properties/functions 3
System overview 4
Application planning 5
Mounting 6
Connecting 7
Configuring 8
Configuration control (option handling) 9
Commissioning 10
Maintenance 11
Technical specifications 12
Industrial cybersecurity 13
Safety-related shutdown of ET200AL standard modules A
Dimension drawings B
Accessories/spare parts C

Continued on next page

ET 200AL
Distributed I/O system

System Manual

Table of contents

1 Introduction 8

1.1 SiePortal 10

1.2 ET 200AL Documentation Guide 10

1.3 MultiFieldbus Configuration Tool (MFCT) 11

1.4 S7 Port Configuration Tool (S7-PCT) 12

1.5 S7 Failsafe Configuration Tool (S7-FCT) 13

1.6 SIMATIC Technical Documentation 13

2 Safety instructions 16

2.1 Warnings in this document 16

2.2 Safety-related symbols for IP65/IP67 modules 16

2.3 Intended use 17

2.4 Changes to the device and spare parts 17

2.5 Target group and personnel qualifications 17

2.6 Personal protective equipment 18

2.7 Working on electrical parts 18

2.8 Residual risks 18

2.8.1 Live parts 18

2.8.2 Conductive pollution 19

2.8.3 Overheating 19

2.8.4 Uncontrolled movements 20

2.8.5 Unsafe operating states 20

2.9 Behavior in case of emergency 20

2.10 Material damage 20

2.10.1 Transport and storage 20

2.10.2 Installation and connection 21

3 New properties/functions 22

4 System overview 24

4.1 What is the SIMATIC ET 200AL distributed I/O system? 24

4.2 What are fail-safe automation systems and fail-safe modules? 26

4.3 Components 28

5 Application planning 31
5.1 Hardware configuration 31
5.2 Configuration variants with ET-Connection 32
5.2.1 ET 200AL with ET-Connection 32
5.2.2 Hybrid configuration ET 200AL/ET 200SP with ET-Connection 34

6 Mounting 36
6.1 Basics 36
6.2 Mounting modules 37

7 Connecting 41
7.1 Rules and regulations for operation 41
7.2 Additional rules and regulations for the operation of the ET 200AL with fail-safe modules 44
7.2.1 Safety extra-low-voltage (SELV, PELV) for fail-safe modules 44
7.2.2 Requirements for sensors and actuators for fail-safe modules 45
7.2.3 Crosstalk of digital input/output signals 47
7.3 Operation of the ET 200AL on grounded/non-grounded infeed 48
7.4 Electrical configuration of the ET 200AL distributed I/O system 51
7.5 Connecting ET 200AL to functional earth 56
7.5.1 Mounting ET 200AL modules on conductive substrate 57
7.5.2 Mounting ET 200AL modules on non-conductive substrate 58
7.6 Connecting cables for ET 200AL 60
7.6.1 Wiring rules for the interface module and I/O modules 60
7.6.2 Connecting cables for voltage distributor PD 24VDC 61
7.7 Wiring 62
7.8 ET 200AL marking 66
7.8.1 Factory markings 66
7.8.2 Optional markings 67
7.8.3 Mounting identification labels 68

8 Configuring 69
8.1 Introduction 69
8.2 Requirements 69
8.3 Configuration 72
8.3.1 MultiFieldbus maximum configuration 72
8.3.2 PROFINET maximum configuration 73
8.3.3 PROFIBUS maximum configuration 74
8.4 Assigning the PROFIsafe addresses 75

9 Configuration control (option handling) 76
9.1 Configuration control 76

9.2 Configuring ... 78

9.3 Creating the control data record ... 80
9.3.1 Introduction ... 80
9.3.2 Control data record for the ET 200AL distributed I/O system ... 82
9.3.3 Feedback data record at the ET200AL distributed I/O system ... 84
9.3.4 Example of a configuration control ... 85

9.4 Transferring the control data record in the user program of the CPU ... 88

9.5 Behavior during operation ... 90

10 Commissioning ... 91

10.1 PROFINET IO ... 91
10.1.1 Commissioning ET 200AL on PROFINET IO ... 91
10.1.2 Startup on PROFINET IO ... 92
10.1.3 PROFIenergy ... 93

10.2 EtherNet/IP ... 94
10.2.1 Commissioning the ET 200AL on EtherNet/IP ... 94
10.2.2 Startup on EtherNet/IP ... 96

10.3 Modbus TCP ... 98
10.3.1 Commissioning the ET 200AL on Modbus TCP ... 98
10.3.2 Startup on Modbus TCP ... 99

10.4 PROFIBUS DP ... 101
10.4.1 Commissioning ET 200AL on PROFIBUS DP ... 101
10.4.2 Startup on PROFIBUS DP ... 102

10.5 Identification and maintenance data ... 103
10.5.1 Reading out and entering I&M data ... 103
10.5.2 Data record structure for I&M data ... 105

11 Maintenance ... 108

11.1 Replacing modules ... 108

11.2 Firmware update ... 110

11.3 Resetting interface module to factory settings ... 111

11.4 Reactions to errors of the F module ... 113

11.5 Cleaning modules ... 115

12 Technical specifications ... 116

12.1 Marks and approvals ... 116

12.2 Certificates ... 119

12.3 Standards and requirements ... 119

12.4 Electromagnetic compatibility ... 121

12.5 Transport and storage conditions ... 123

12.6 Mechanical and climatic ambient conditions ... 124

12.7 Details on insulation, protection class, degree of protection and rated voltage 126

13 Industrial cybersecurity 128

13.1 Cybersecurity information 128

13.2 Security update notification 129

13.3 Basic information on industrial cybersecurity 129
13.3.1 Definition of industrial cybersecurity 129
13.3.2 Objectives of industrial cybersecurity 129

13.4 Integrated security concept and security strategies 130
13.4.1 Comprehensive security concept "Defense in Depth" 130
13.4.2 Security management 131

13.5 Operational application environment and security assumptions 133
13.5.1 Intended use 133
13.5.2 Requirements for the operational application environment and security assumptions 133

13.6 Security properties of the devices 135

13.7 Secure operation of the system 135
13.7.1 Hardening measures 135
13.7.2 Secure configuration 135
13.7.3 Handling of sensitive data 135
13.7.4 Regular firmware updates 136
13.7.5 Notifications about security vulnerabilities (Siemens Security Advisories) 136
13.7.6 Data backup 137
13.7.7 Security checks 137
13.7.8 Secure decommissioning 137
13.7.8.1 Securely removing data 137
13.7.8.2 Recycling and disposal 139

13.8 Secure operation of the engineering software 139

13.9 Secure operation of interface modules 139
13.9.1 Data integrity for interface modules 139
13.9.2 Signed firmware update for interface modules 141
13.9.3 Secure Boot 142

13.10 Safe operation of I/O modules 143
13.10.1 Data integrity for I/O modules 143
13.10.2 Signed firmware update for I/O modules 143

A Safety-related shutdown of ET200AL standard modules 145

B Dimension drawings 149

C Accessories/spare parts 150

C.1 Accessories/spare parts 150

C.2 UL-approved cables 154

C.3 Cables 154

C.5 Pin assignment and core color 164

D SIMATIC ET 200AL data 166

D.1 Data of the interface and I/O modules 166

Introduction

1

Purpose of the documentation

This documentation provides you with important information on how to configure, install, wire and commission the SIMATIC ET 200AL distributed I/O system.

Basic knowledge required

A basic knowledge of automation technology is required to understand the documentation.

Scope of the documentation

This documentation is valid for the SIMATIC ET 200AL distributed I/O system.

Conventions

Observe the notes labeled as follows:

NOTE

A note contains important information on the product described in the documentation and on the handling of the product to which particular attention should be paid.

Standards

You can find a dated reference to the respective standards or the EC Declaration of Conformity on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert?ct=444&ci=526).

Special information

NOTE

Important note for maintaining the operational safety of your plant

Plants with safety-related features are subject to special operational safety requirements on the part of the operator. The supplier is also obliged to comply with special product monitoring measures. For this reason, we inform you in personal notifications about product developments and features that are (or could be) relevant to the operation of plants from a safety perspective.

You should subscribe to the corresponding notifications in order to obtain the latest information and to allow you to make any necessary modifications to your system.

Log into SiePortal. Follow the links below and click on "Email on update" on the right-hand side in each case:

- SIMATIC S7-300/S7-300F (https://support.industry.siemens.com/cs/ww/en/ps/13751)
- SIMATIC S7-400/S7-400H/S7-400F/FH (https://support.industry.siemens.com/cs/ww/en/ps/13828)
- SIMATIC WinAC RTX (F) (https://support.industry.siemens.com/cs/ww/en/ps/13915)
- SIMATIC S7-1500/SIMATIC S7-1500F (https://support.industry.siemens.com/cs/ww/en/ps/13716)
- SIMATIC S7-1200/SIMATIC S7-1200F (https://support.industry.siemens.com/cs/ww/en/ps/13683)
- Distributed I/O (https://support.industry.siemens.com/cs/ww/en/ps/14029)
- STEP 7 (TIA Portal) (https://support.industry.siemens.com/cs/ww/en/ps/14667)

NOTE

When using F-CPUs in safety mode and fail-safe modules, note the description of the fail-safe system SIMATIC Safety Programming and Operating Manual SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/de/view/54110126/en).

ID Link for the digital nameplate



Figure 1-1 ID Link example DI 16x24VDC 8xM12

The ID Link is a globally unique identifier according to IEC 61406, which you will find in the future as a QR code on your product.

The figure shows an example of an ID Link for the I/O device digital inputs DI 16x24VDC 8xM12.

You can recognize the ID Link by the frame with a black corner at the bottom right. The ID Link takes you to the digital nameplate of your product.

Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner or reader app. Call the ID Link.

In the digital nameplate, you will find product data, manuals, Declarations of Conformity, certificates, and other useful information about your product.

1.1 SiePortal

You can find current information on the following topics quickly and easily here:

- **Catalog and ordering system**
  Ordering system for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).
- **Product support**
  All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.
- **Application examples**
  Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.
- **Services**
  Information about Industry Services, Field Services, Technical Support, spare parts and training offers.
- **Forums**
  For answers and solutions concerning automation technology.
- **mySiePortal**
  Your personal work area in the SiePortal for notifications, support requests, and configurable documents.

This information is provided by SiePortal on the Internet (https://sieportal.siemens.com/).

1.2 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.3 MultiFieldbus Configuration Tool (MFCT)

MultiFieldbus Configuration Tool

MultiFieldbus Configuration Tool (MFCT) is a PC-based software and supports the configuration of MultiFieldbus- and DALI-devices. In addition, the MFCT offers convenient options for mass firmware updates of ET 200 devices with MultiFieldbus- support and reading service data for many other Siemens devices.

Functional scope of the MFCT

- MultiFieldbus configuration:
  Engineering, configuration and diagnostics of MultiFieldbus-devices, provision of the required project files (project, UDT-, CSV- and EDS-file), transfer/export of the files to device and/or data memory.
- DALI configuration:
  Device selection and online configuration of DALI devices.

- TM FAST:
  Generation and download of FPGA-UPD- and FPGA-DB-files.
- Maintenance:
  Topology scan of a Ethernet network, reading of service data, parameter assignment and firmware update.
- Settings:
  Language switching German / English, network scanner speed, setting of the network adapter, installation of GSDML-and EDS-files.

System/installation requirements for MFCT

The MFCT runs under Microsoft Windows and does not require installation or administrator rights.

For MFCT you must also install the following software:

- Microsoft .NET Framework 4.8 (You can find an Offline Installer on the Internet. (https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0))
- NPcap from directory "Misc"
- PG/PC interface from directory "Misc"
- Microsoft C++ Redistributable for x86-systems (you can find the installation data for download on the Internet. (https://aka.ms/vs/15/release/vc_redist.x86.exe))

The download of the tool and further information as well as documentation on the individual functions of the MFCT can be found on the Internet.
(https://support.industry.siemens.com/cs/de/en/view/109773881)

1.4 S7 Port Configuration Tool (S7-PCT)

SIMATIC S7-PCT

The Port Configuration Tool (PCT) is a PC-based software for the parameter assignment of Siemens IO-Link Master modules and IO-Link devices from any manufacturer.

You integrate IO-Link-devices using the standardized device description "IODD", which you get from the respective device manufacturer. S7-PCT supports version 1.0 and V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link Master from STEP 7. When STEP 7 is not used or the IO-Link Master is not operated on a SIMATIC controller, "standalone"-operation is also possible.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

1.5 S7 Failsafe Configuration Tool (S7-FCT)

SIMATIC S7-FCT

Failsafe Configuration Tool (FCT) enables you to GSD configure the following devices in third-party engineering systems:

- Selected, functionally fail-safe SIMATIC I/O devices
- Functionally fail-safe SIRIUS ACT PROFINET interfaces

The engineering system must meet the following requirements for this:

- Support of the CPD system integration acc. to "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO"
- TCI implementation to Conformance Class C3

Additional information on S7-FCT can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109762827).

1.6 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)
     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:
     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Safety instructions

2

2.1 Warnings in this document

You can find explanations of the warnings used in this document in the "Legal information" section.

2.2 Safety-related symbols for IP65/IP67 modules

The following table contains an explanation of the symbols located on your IP65/IP67 modules, their packaging or in the accompanying documentation.

Symbol	Meaning
	General warning sign **Caution/Notice** You must read the product documentation. The product documentation contains information about the type of potential hazard and enables you to recognize risks and implement countermeasures.
	The assigned safety symbols apply to devices **with Ex approval**. You must read the product documentation. The product documentation contains information about the type of potential hazard and enables you to recognize risks and implement countermeasures.
	Read the information provided by the product documentation. ISO 7010 M002
	Ensure the device is only installed by an electrically skilled person. IEC 60417 No. 6182
	Note that connected mains lines must be designed according to the expected minimum and maximum ambient temperature.
	Note that the device must be constructed and connected in accordance with EMC regulations.

Symbol	Meaning
 230V MODULES	Note that a 230 V device can be exposed to electrical voltages which can be dangerous. ANSI Z535.2
 24V MODULES	Note that a device of Protection Class III may only be supplied with a protective low voltage according to the standard SELV/PELV. IEC 60417-DB Symbol 5180 "Class III equipment"
 INDOOR USE ONLY INDUSTRIAL USE ONLY	Be aware that the device is only approved for the industrial field and only for indoor use.

2.3 Intended use

The system is used to control machines and plants.

Intended use also includes observance of this documentation, in particular the safety instructions and conditions of use. See section Technical specifications (Page 116).

2.4 Changes to the device and spare parts

Modifications to the module may affect the safety and the function of the module:

- Do not make any changes or attachments to the module.
- Do not remove or paste over safety instructions on the module.
- Only use original spare parts and accessories.

2.5 Target group and personnel qualifications

All persons working with this module require the following knowledge:

- Contents of this document as well as contents of the enclosed documents.
- Handling the module (after instruction)
- Relevant standards and regulations
- Accident prevention regulations

The following activities are reserved for specially qualified personnel:

Working on electrical parts
Work on electrical parts may only be performed by the following persons:

- Qualified electricians
- Persons trained in electrical engineering under the direction and supervision of qualified personnel.

Commissioning and configuration
Commissioning and configuration requires general knowledge in the field of automation technology.

2.6 Personal protective equipment

The personal protective equipment depends on the activity and is determined by the operator. To avoid material damage during packing, unpacking and installation activities we recommend:

- ESD wrist strap
- ESD shoes

2.7 Working on electrical parts

Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualifications (Page 17)).

- Always observe the country-specific safety rules.
- Notify all those who will be affected by the procedure.
- Follow the 5 safety rules according to DIN EN 50110-1 (VDE 0105-1):

1. Disconnect
2. Secure to prevent reconnection
3. Verify safe isolation from the supply (all poles)
4. Ground and short-circuit
5. Erect barriers around or cover adjacent live parts

After completing work:

- Restore operational readiness in reverse order.

2.8 Residual risks

Despite all the technical and procedural risk reductions that have been carried out, not all dangers can be avoided. The following sections describe these residual risks and measures to avoid them.

2.8.1 Live parts

Electrocution on contact with live parts leads to life-threatening injuries (death).

Operation

- Do not open the module.
- Do not use damaged modules.
- Pull the plug and not the cable.

Installation and connection

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualifications (Page 17)).
- Adhere to the protective measures for safe working on electrical parts (see section Working on electrical parts (Page 18))
- Fuse the connection cables according to the current-carrying capacity of the cable used, taking into account the applicable standards.
- Ground the module according to regulations.
- For the 24 V DC supply (SELV/PELV), only use power supply units that provide safe electrical extra-low voltage in accordance with IEC 61131-2 or IEC 61010-2-201.

Maintenance

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualifications (Page 17)).
- Adhere to the protective measures for safe working on electrical parts (see section Working on electrical parts (Page 18)).

2.8.2 Conductive pollution

Electrocution during transmission of electrical energy via conductive contamination to the body leads to life-threatening injuries (death).

- Seal unused connections with a suitable and approved sealing cap.
- Keep the module free from conductive pollution.

2.8.3 Overheating

Smoke development and fire due to overheating of module and cables result in burns and life-threatening injuries (death).

To avoid overheating:

- Ensure the correct installation position.
- Ensure sufficient air supply (e.g. maintain mounting clearances).
- Only use undamaged cables.

Installation and connection

- Follow the instructions for the mounting position.
- Adhere to the specified ventilation clearances.
- Fuse the connecting cables according to the cable cross-section.

Maintenance

- Check plug-in connections and cables regularly for damage.

2.8.4 Uncontrolled movements

Uncontrolled movements of driven machine or system parts during commissioning, operation, maintenance and repair.

- Follow the safety instructions described in the function manuals.

2.8.5 Unsafe operating states

Unsafe operating states may result in personal injury of unknown extent.
The following factors can be triggers:

- Manipulation of the software, e.g. viruses, trojans or worms.

Manipulation of the software, e.g. viruses, trojans or worms.

- Adhere to the protective measures against tampering with the software (see section Industrial cybersecurity (Page 128)).
- Perform available updates in a timely manner.
- Protect files stored on removable media from malware with appropriate protective measures, e.g. virus scanner.
- Set up access protection for the CPU.

2.9 Behavior in case of emergency

- Force EMERGENCY OFF

When the safe operating state has been restored:

- Unlock the EMERGENCY OFF mechanism.
- The person responsible for the system ensures that the system starts up in a controlled and defined manner.

2.10 Material damage

2.10.1 Transport and storage

- Only pack, store, transport and ship electronic components, modules or devices in the original product packaging or in other suitable materials, e.g. conductive foam rubber or aluminum foil.
- Observe the limits during transport and storage. See Technical specifications (Page 116) section.

2.10.2 Installation and connection

- We recommend touching components, modules and devices only if they are grounded by one of the following measures:
  - With an ESD wrist strap.
  - With ESD shoes or ESD grounding strips in ESD areas with conductive flooring.
- Place electronic components, modules and devices only on conductive surfaces (e.g. tables with ESD coating, conductive ESD plastic foam, ESD packing bags, ESD transport containers).
- Ensure that there is sufficient overvoltage protection.

Installation/disassembly with voltage switched on

- Refer to section Mounting (Page 36)
- Refer to section Replacing modules (Page 108)

New properties/functions

3

What's new in the ET 200AL System Manual, Edition 08/2025 compared to Edition 03/2025?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	ID Link	Here you will find a description of the ID Link	Section Introduction (Page 8)
	The module "Communications module CM 4xIO-Link 4xM12" has been added	In various sections contents on the module "Communications module CM 4xIO-Link 4xM12" have been added.	Section Marks and approvals (Page 116) Section Safety-related shutdown of ET200AL standard modules (Page 145)
	The module "Communications module CM 8xIO-Link + DIQ 6x24VDC/-0.5A 8xM12" has been added	In various sections contents on the module "Communications module CM 8xIO-Link + DIQ 6x24VDC/0.5A 8xM12" have been added.	
	The module "Voltage distributor PD 24VDC" has been added	In various sections, content has been added to the module "Voltage distributor PD 24VDC".	Section Components (Page 28) Section Connecting (Page 41) Section Marks and approvals (Page 116) Section Safety-related shutdown of ET200AL standard modules (Page 145)
	Accessories for power supply M12-L	M12-L cables for voltage supply are now also included in the section	Section Accessories/spare parts (Page 150)
	Importer addresses	You can find the importer addresses for specific countries here.	Standards and requirements (Page 119) section
	SIMATIC ET 200AL data	This section provides an overview of the data that is generated by the SIMATIC ET 200AL automation system and accessible to you.	SIMATIC ET 200AL Data (Page 166) section
Changed contents	Technical specifications	Various specifications have been adapted in the "Technical specifications" section	Section Technical specifications (Page 116)
	"Industrial Cybersecurity" section	The content of the "Industrial Cybersecurity" section has been updated	Section Industrial cybersecurity (Page 128)
	Ambient conditions	The operating conditions and storage conditions have been adapted.	Section Transport and storage conditions (Page 123) Section Mechanical and climatic ambient conditions (Page 124)

What's new in the ET 200AL System Manual, Edition 03/2025 compared to Edition 10/2024?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	The "Digital input/digital output module DIQ 8x24VDC/0.5A 8xM8" has been added.	In various sections, content has been added to the module "Digital input/digital output module DIQ 8x24VDC/0.5A 8xM8".	Section Marks and approvals (Page 116) Section Mechanical and climatic ambient conditions (Page 124)
Changed contents	"Industrial Cybersecurity" section	The content of the "Industrial Cybersecurity" section has been updated	Section Industrial cybersecurity (Page 128)

What's new in the ET 200AL System Manual, Edition 10/2024 compared to Edition 12/2023?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	"Industrial Cybersecurity" section	These sections have been added to the "Industrial Cybersecurity" section: • Secure Boot • Secure operation of I/O modules	Section Secure Boot (Page 142) Section Safe operation of I/O modules (Page 143)
	Use above 2000 m is possible.	Information and this table have been added to the section "Mechanical and climatic environmental conditions": Derating factor of installation altitude and ambient temperature for use above 2000 m above sea level.	Section Mechanical and climatic ambient conditions (Page 124)
Changed contents	"Introduction" section	The contents have been updated in the "Introduction" section	Section Introduction (Page 8)
	"Configuring" section	The "Configuring" section has been newly structured	Section Configuring (Page 69)
	Update of the section	Various values have been added and updated in the "Technical specifications" section	Section Technical specifications (Page 116)

What's new in Edition 12/2023 of the ET 200AL System Manual compared with Edition 12/2022?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	General security instructions	The section contains a compilation of general security instructions for the ET 200AL distributed I/O system.	Section Safety instructions (Page 16)
	"Industrial Cybersecurity" section	Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities. The section contains the following information: • Basic information on the subject of industrial cybersecurity • Measures to protect individual components and the entire system against manipulation and unwanted access.	Section Industrial cybersecurity (Page 128)
	Supplement IM 157-1 MF module	The MultiFieldbus interface module IM 157-1 MF	Starting with section System overview (Page 24)

What's new in Edition 12/2022 of the ET 200AL System Manual compared with Edition 08/2021?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Technical specifications of the plug	The technical specifications of the plug-in connections are listed in the section.	Starting with section Connectors (Page 162)
Changed contents	Update of the section	The UKCA approval has been added.	Section Marks and approvals (Page 116)
	Update of the section	The table "Pulse-shaped disturbance variables" has been revised.	Section Electromagnetic compatibility (Page 121)

System overview

4

4.1 What is the SIMATIC ET 200AL distributed I/O system?

SIMATIC ET 200AL

The SIMATIC ET 200AL distributed I/O system is a scalable and highly flexible, distributed I/O system for connecting process signals to a higher-level control system with a field bus.

Customer benefits of the system

Compact design

- High IO configuration limits for module widths of 30 mm or 45 mm and up to 32 modules for each ET 200AL
- High degree of protection IP65/IP67
- Adequate for temperatures from -30 °C/-25 °C to +55 °C and accelera-tions up to 10g

Easy to use

- Easy wiring thanks to color-coded connectors
- CAx compliant labeling of all interfaces
- Fast, convenient configuration and commissioning with STEP 7 (TIA Portal)
- Configuration customizing for future extension through integrated configurationcontrol

Flexible mounting

- Easy mounting in all mounting positions - even in small spaces
- Spatially separated mounting of the modules by means of a backplane bus designed as a cable(= ET Connection)
- Flexible connection to MultiFieldbus, PROFIBUS or integration in SIMATIC ET 200SP
- Integration of sensors and actuators through M8 and M12 connection technology



Energy efficiency

- PROFIenergy as integrated function

Communication standards

- PROFINET IO
- EtherNet/IP
- Modbus TCP
- PROFIBUS DP
- IO-Link
- PROFIsafe

Powerful technology

- Module with counting function
- Fail-safe modules

Figure 1-2 ET 200AL benefits

Area of application

The SIMATIC ET 200AL distributed I/O system is especially well suited for use in tight spaces, moving applications and for assembly and handling technology. Thanks to its scalable construction, you have the option to precisely customize its configuration to your on site needs.

The SIMATIC ET 200AL distributed I/O system features degree of protection IP65/IP67. The I/O modules are suitable for distributed use indoors on a machine or assembly line.

Setup

The SIMATIC ET 200AL distributed I/O system is made up of the following components:

- Interface modules (MultiFieldbus/PROFINET/PROFIBUS)
- Digital and analog I/O modules
- Communications modules
- Fail-safe modules

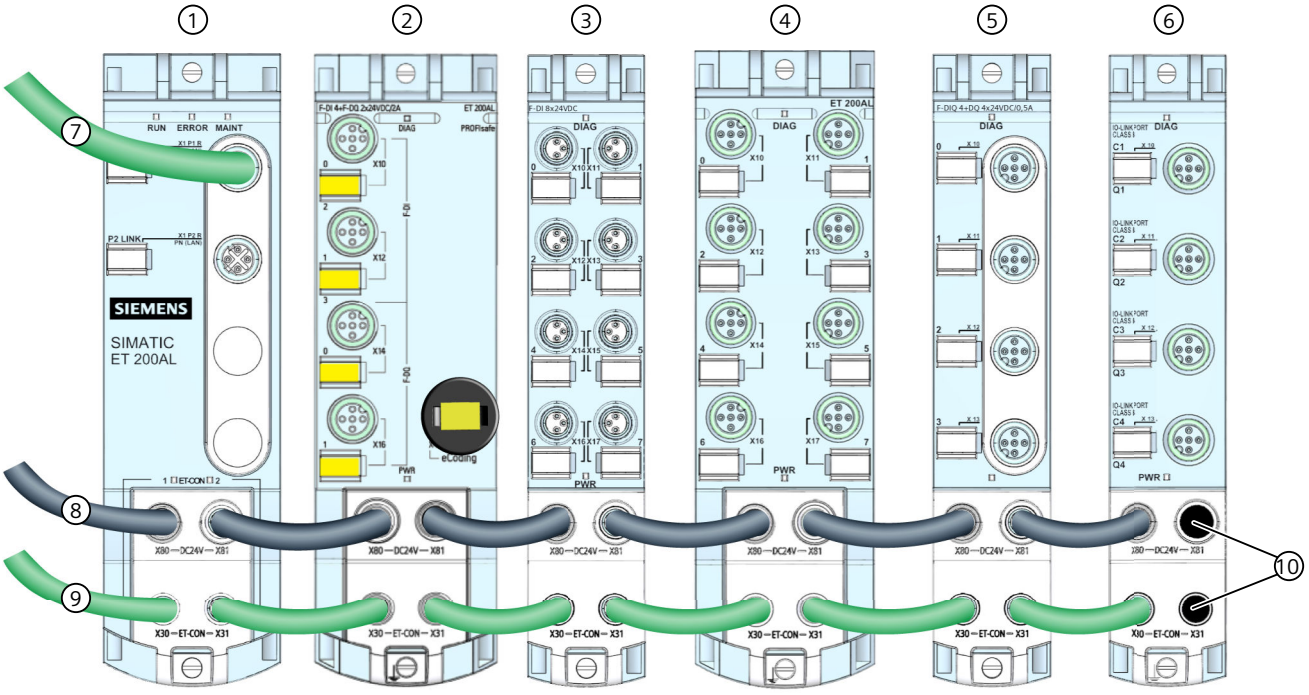
After an interface module you can configure 2 lines (ET-Connection), each with 16 modules.

Alternatively, you can configure a line with 16 I/O modules on the SIMATIC ET 200SP distributed I/O system with BaseUnit BU-Send and the BusAdapter BA-Send 1xFC.

The ET-Connection backplane bus is designed as a cable. This allows you to create spatial distances of up to 15 m between the modules.

Configuration example

The figure below shows a configuration example of the SIMATIC ET 200AL distributed I/O system with a PROFINET interface module.



① Interface module (PROFINET)
② Fail-safe digital input / digital output module
③ Digital input/output module
④ Digital output module
⑤ Analog input module
⑥ Communication module
⑦ PROFINET cable
⑧ Power supply cable
⑨ ET-Connection cable
⑩ Sealing caps

Figure 1-3 Configuration example of the ET 200AL

4.2 What are fail-safe automation systems and fail-safe modules?

Fail-safe automation systems

Fail-safe automation systems are mainly used in applications where failure could have consequences for the safety of people and/or the environment. Fail-safe systems are therefore intended to reduce hazards or failures that could cause physical damage. Their purpose is to ensure a tolerable level of risk.

F-systems are used to control processes and provide a safe operating state when faults are detected. Fault detection is ensured by a very high level of diagnostic coverage. When a fault is detected, appropriate actions are initiated to bring the affected application to a safe state.

F-systems offer improved fault detection and fault localization through detailed diagnostics and diagnostic messages. This is the most important difference between fail-safe systems and standard systems. The use of fail-safe systems should be considered for applications where hazards are inherent and can cause physical damage.

Safety Integrated

Safety Integrated is the integrated safety concept for automation and drive technology from Siemens.

Proven technologies and systems from automation technology are used for safety systems. Safety Integrated includes the complete safety sequence, ranging from sensor, actuator and fail-safe modules right through to the controller, including safety-related communication via standard fieldbuses. Drives and controllers handle safety tasks in addition to their actual functions.

Fail-safe modules

The key difference between fail-safe modules (F-modules) and standard modules is that they have an internal two-channel design. This means the two integrated processors monitor each other, automatically test the input and output circuits, and switch the fail-safe module to a safe state in the event of a fault.

The F-CPU communicates with a fail-safe module via the safety-related PROFIsafe bus profile.

Possible uses of ET 200AL with fail-safe modules

The use of ET 200AL with fail-safe modules makes it possible to replace conventional mounting technology in safety technology with PLC components. This also includes the replacement of switchgear for EMERGENCY STOP, safety door monitoring, ambidextrous operation, etc.

Fail-safe modules for ET 200AL are supported together with the STEP 7 Safety Advanced V17 or higher option package.

F-modules for ET 200AL can be used either with an ET 200AL PROFINET interface module (IM), a direct ET connection to an ET 200SP F-CPU or a direct ET connection to an ET 200SP IM (mixed configuration).

Use in SIMATIC Safety F-systems

The fail-safe ET 200AL modules can be used with STEP 7 Safety Advanced from V17 with PROFINET and direct ET connection configurations together with an F-CPU.

The fail-safe modules can only be used in safety mode. Fault safe and non-fault safe modules can be combined within one ET 200AL ET connection.

Achievable safety classes

The fail-safe modules are equipped with integrated safety functions for safety mode.
You can achieve the safety classes of the table below:

- With the appropriate parameter assignment of the safety functions in STEP 7
- With a specific combination of fail-safe and non-fail-safe I/O modules
- With a special arrangement and wiring of the sensors and actuators

Table 1-1 Safety classes that can be achieved with ET 200AL in safety mode

Safety class in safety mode		
According to IEC 61508	**According to ISO 13849-1**	
SIL2	Category 3	(PL) Performance Level d
SIL3	Category 3	(PL) Performance Level e
SIL3	Category 4	(PL) Performance Level e

⚠ WARNING

The safety performance of your installation depends on the design and ongoing maintenance of the individual complete safety function.
SIMATIC fail-safe CPUs and ET 200AL fail-safe modules have logic processing components with certified safety integrity levels, provided they are operated in accordance with classifications, specifications, and instructions.
Failure to adhere to this may cause damage or unpredictable operation, resulting in fatal or serious injury and/or property damage.
To achieve the level of safety you require, you need to select all components of your plant and construct and maintain them in accordance with accepted safety standards and practices.

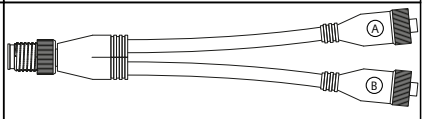
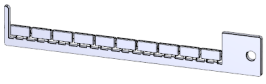
4.3 Components

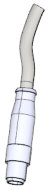
Components of the ET 200AL distributed I/O system

The following table shows and explains the function of the most important components of the ET 200AL distributed I/O system.

Table 1-2 Components of the ET 200AL distributed I/O system

Components	Function	View
Interface module for MultiFieldbus	• The interface module connects the distributed I/O system ET 200AL with one or more I/O controllers, scanners, Modbus clients • Exchanges data with the I/O modules via ET-Connection	

Components	Function	View
Interface module for PROFINET IO	• The interface module connects the ET 200AL distributed I/O system with the IO controller • Exchanges data with the I/O modules via ET-Connection	
Interface module for PROFIBUS DP	• The interface module connects the ET 200AL distributed I/O system with the DP master • Exchanges data with the I/O modules via ET-Connection	
I/O modules	• The I/O modules form the interface to the process • Recording and controlling the current process status via the connected sensors and actuators	
Voltage distributor	• The voltage distributor distributes the voltage 24 V DC to the I/O modules • 1 input M12-L connector • 4 outputs M8 socket with electronic fusing of 4 A per output for 1L+ and 2L+	
eCoding plug connector	Electronic coding element with an overwritable electronic memory for module-specific fail-safe address data (for example, the F-destination address)	
Y-cable	Y-cable connects multiple actuators or sensors to inputs or outputs. There are two types: • Y-cable: Connects inputs or outputs of the module to several actuators or sensors. • Inverted Y-cable: Connects several fail-safe inputs or outputs of the F-module with one or more sensors and actuators	
Identification labels	• The identification labels come with the module and can be machine printed • Can be ordered separately in white or yellow for fail-safe modules	

Components	Function	View
Bus cable and M8 connector for ET-Connection	The bus cable creates the bus connection between the modules	
Power cable and M8 connector for power supply	The power cable provides power to the modules	
Stripping tool ET-Connection	The stripping tool is used to strip the ET-Connection bus cable	

Application planning

5

5.1 Hardware configuration

Mechanical maximum configuration

The following tables show the rules of the mechanical configuration. As soon as one of the following rules applies, the maximum configuration has been reached.

Table 1-3 Maximum mechanical configuration - on ET 200AL interface module

Properties	Rule (max.)	
	Interface modules as of firmware version V1.0.0	Interface modules as of firmware version V1.0.1
Number of ET 200AL I/O modules in the configuration	32	
Number of ET-Connection outlets	2	
Number of I/O modules per ET-Connection outlet	16	
Spatial extension per ET-Connection line	160 m	240 m
Cable length between the modules	10 m	15 m

Table 1-4 Maximum mechanical configuration - on ET 200SP with interface module

Properties	Rule (max.)	
	Interface modules as of firmware version V3.0.0	Interface modules as of firmware version V3.3.0
Number of ET 200AL I/O modules in the configuration	16	
Number of ET-Connection outlets	1	
Spatial extension ET-Connection line	160 m	240 m
Cable length between the modules	10 m	15 m

Table 1-5 Maximum mechanical configuration - on ET 200SP with CPU

Properties	Rule (max.)
	CPUs with firmware version as of V2.0.0
Number of ET 200AL I/O modules in the configuration	16
Number of ET-Connection outlets	1
Spatial extension ET-Connection line	240 m
Cable length between the modules	15 m

Electrical maximum configuration

The number of usable I/O modules of a potential group is limited by the following points:

- Power requirements of the I/O modules
- Power requirements of the components supplied via these I/O modules

The maximum infeed current of the I/O modules is 4 A with 1L+ supply voltage (non-switched) and 2L+ load voltage (switched). When the maximum infeed current has been reached, you must open a new potential group.

Reference

You will find more information in the section Wiring rules for the interface module and I/O modules (Page 60).

5.2 Configuration variants with ET-Connection

5.2.1 ET 200AL with ET-Connection

Every ET 200AL interface module has 2 ET-Connection I/Os.

From every ET-Connection, you have the option to set up a line with a maximum of 16 ET 200AL I/O modules.

ET-Connection1

The figure below shows a configuration in the IP65/IP67 environment with one ET-Connection line.

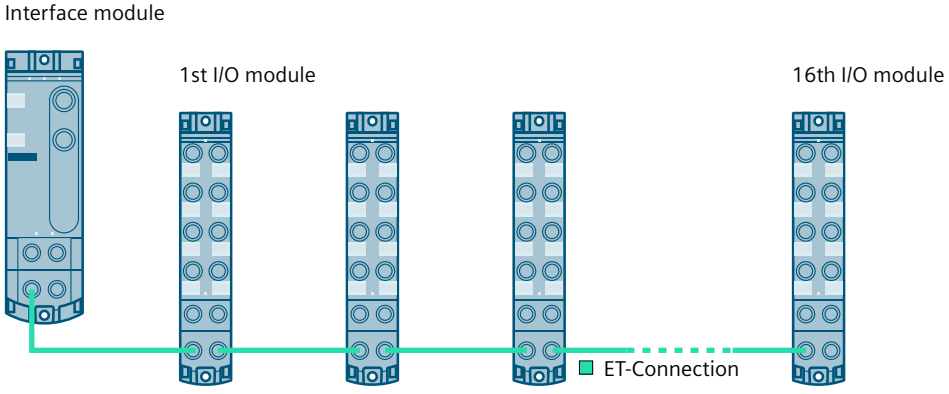


Figure 1-4 ET 200AL with ET-Connection1

ET-Connection1 and ET-Connection2

The figure below shows a configuration in the IP65/IP67 environment with two ET-Connection lines

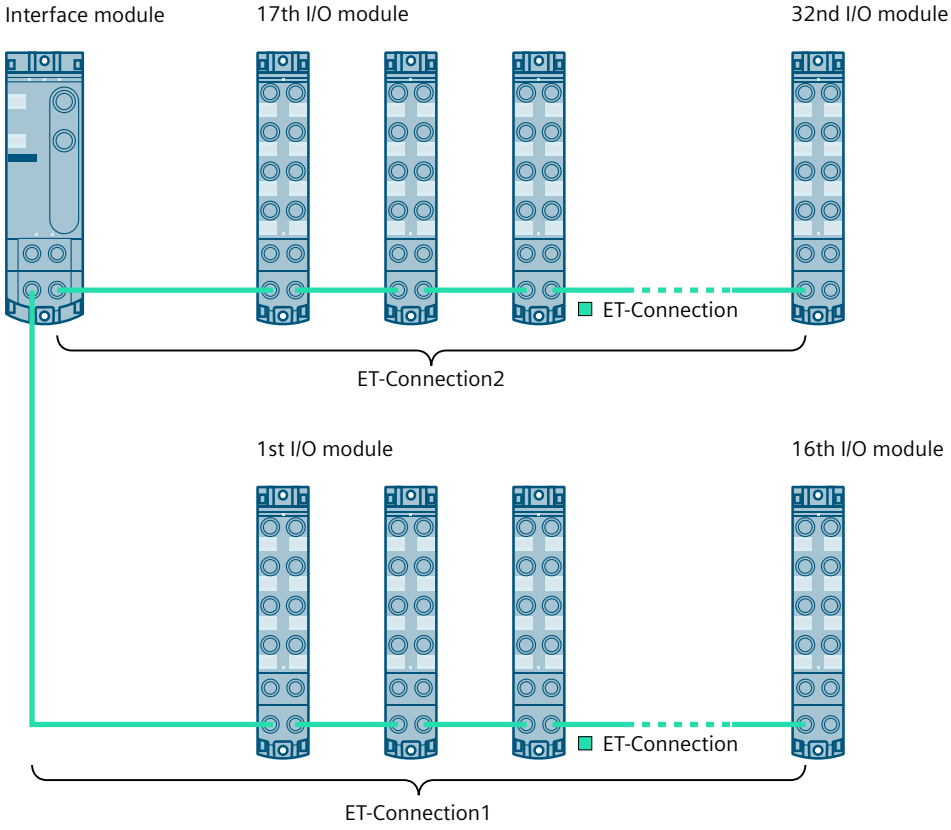


Figure 1-5 ET 200AL with ET-Connection1 and ET-Connection2

5.2.2 Hybrid configuration ET 200AL/ET 200SP with ET-Connection

Hybrid configuration ET 200AL and ET 200SP

You have the possibility to integrate standard and fail-safe I/O modules of the distributed I/O systems ET 200AL (IP65/IP67) into a configuration of the distributed I/O system ET 200SP (IP20). Fail-safe and non-fail-safe modules may be combined at will in the ET 200AL distributed I/O system.

The figure below shows a combination of the modules of the ET 200AL and ET 200SP distributed I/O systems.

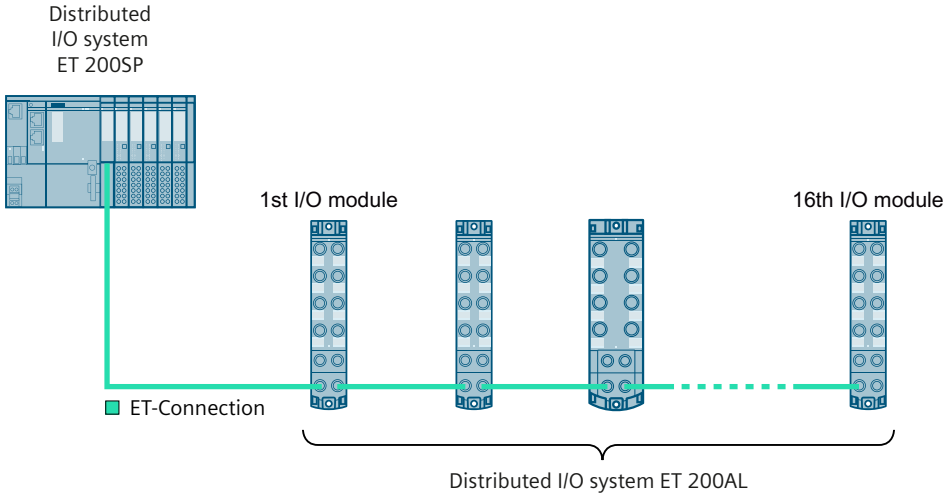


Figure 1-6 Hybrid configuration ET 200SP and ET 200AL with ET-Connection

Requirement

For a hybrid configuration, you need at least the following components:

- Interface module or CPU

NOTE

Use of a F-CPU with F-modules

A fail-safe CPU must also be used when using a fail-safe module in the ET 200AL.

- BaseUnit BU-Send with BusAdapter BA-Send 1xFC
- ET-Connection cable pre-assembled on one side
- Power cable pre-assembled on one side

Rules

When putting together a hybrid configuration, you must observe the following rules:

- The bus length of the ET 200SP distributed I/O system is a maximum of 1 m (excluding interface module/CPU, including BU-Send, BA-Send 1×FC and server module).
- A maximum of 16 ET 200AL I/O modules can be connected to ET-Connection.
- The maximum length of the bus cable for ET-Connection between two modules is 15 m.

Rules

The following table shows a rough overview of the functions of the ET 200AL I/O modules in combination with the ET 200SP.

Function	Hybrid configuration		
	ET 200SP		ET 200AL I/O modules on ET connection
	IM	CPU	
Isochronous mode	●	--	--
Configuration control	●	●	●
Shared device	●	●	●
PROFIenergy	●[1]	--	●[1]
System redundancy S2	●[2]	--	●[2]

1) PROFIenergy is not supported by fail-safe I/O module F-DI 4+F-DQ 2x24VDC/2A, 4xM12

2) With IM 155-6 PN/3 HF and IM 155-6 PN/2 HF as of V4.2

Details on the hybrid configuration are available here (https://support.industry.siemens.com/cs/de/en/view/100300517).

Procedure

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/95886672)

Proceed as follows to put together a multi-tier configuration:

1. Mount the BaseUnit BU-Send directly to the right of the ET 200SP interface module or the ET 200SP CPU.
2. Then install the other BaseUnits/I/O modules for the ET 200SP distributed I/O system and the server module.
3. Connect the bus cable for ET-Connection to the BusAdapter BA-Send 1×FC and install it on the BaseUnit BU-Send.
4. Fasten the BusAdapter BA-Send 1×FC with the BaseUnit BU-Send (1 screw with tightening torque of 0.2 Nm). Use a screwdriver with a 3 to 3.5 mm blade to do this.
5. Connect the other end of the bus cable for ET-Connection (with M8 plug) to the first ET 200AL I/O module (socket X30 ET-Connection IN).
6. Connect the supply voltage (24 V DC) to the ET 200AL I/O modules (X80 plug).

Mounting

6

6.1 Basics

Introduction

All the modules of the ET 200AL distributed I/O system are designed for the degree of protection IP65/IP67. This means that you can directly mount this system in your plant.

Installation position

You can mount the ET 200AL distributed I/O system in any position.

Minimum clearances

At ambient temperatures of >50 °C or higher, ensure that the module is mounted at a distance of least 1 cm from an adjacent module or other device.

With the voltage distributor PD 24VDC (6ES7194-2CA00-0AA0), maintain a minimum clearance of 1 cm from adjacent modules or other devices when mounting.

Mounting rules

When mounting the modules, you do not need to following any special rules.

NOTE

Mounting of the modules
Mount the ET 200AL distributed I/O system only with disconnected supply voltages.

NOTICE
Mounting of the interface modules When mounting the interface modules of the ET 200AL, ensure that the rear of the module is protected against mechanical damage.

6.2 Mounting modules

Introduction

The modules of the ET 200AL distributed I/O system are designed for installation on a level, firm surface.

Thanks to the axisymmetrical drill holes in the modules, you have the option to fasten the modules on an aluminum profile using tee nuts.

The following images shows the aluminum profile on which you can mount the modules.

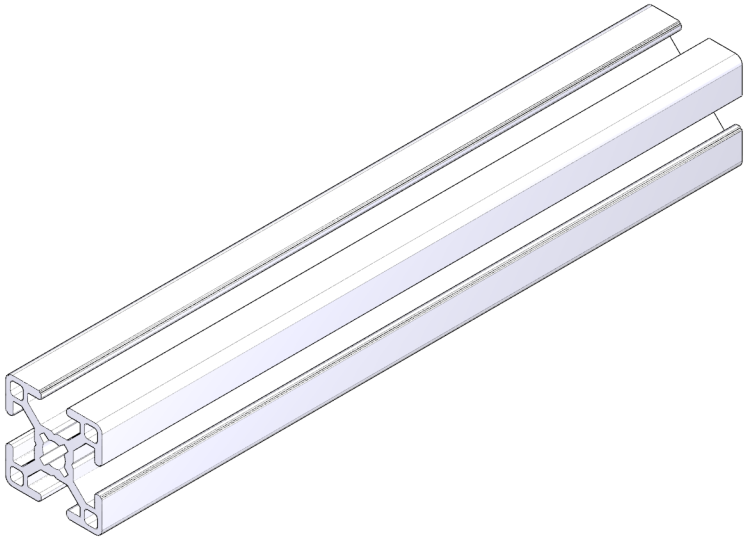


Figure 1-7 Aluminum profile

Required tools

For installation, you need a screwdriver or an Allen wrench.

Required screws

The following table shows and explains the screw types required to mount the modules.

Table 1-6 Recommended screws

Screw type	Explanation
Socket head cap screw M4 according to DIN EN ISO 1207 / DIN EN ISO 1580	The screw length must be at least 30 mm. If you need washers, use DIN EN ISO 7089/DIN EN ISO 7090 washers.
Hexagon socket head cap screw M4 according to DIN EN ISO 4762	

Drill holes of the modules

All modules of the ET 200AL distributed I/O system feature a uniform drill pattern.

- All module housings are axisymmetrical.
- The distance between the top and bottom drill hole is identical for all modules.

Mounting interface module and 45 mm I/O modules (front)

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/95886672)

The interface modules and the 45 mm I/O modules have an attachment point on top and on the bottom.

To mount an interface module or 45 mm I/O module, follow these steps:

1. Drill 2 fastening holes with 4.5 mm diameter at a distance of 149.6 mm.
2. Fasten the interface module or the 45 mm I/O module with the screws to both fastening points (tightening torque 1.2 Nm).

The figure below shows the dimensions for fastening the IM 157-1 PN interface module and the DQ 8x24VDC/2A 8xM12 45 mm I/O module.

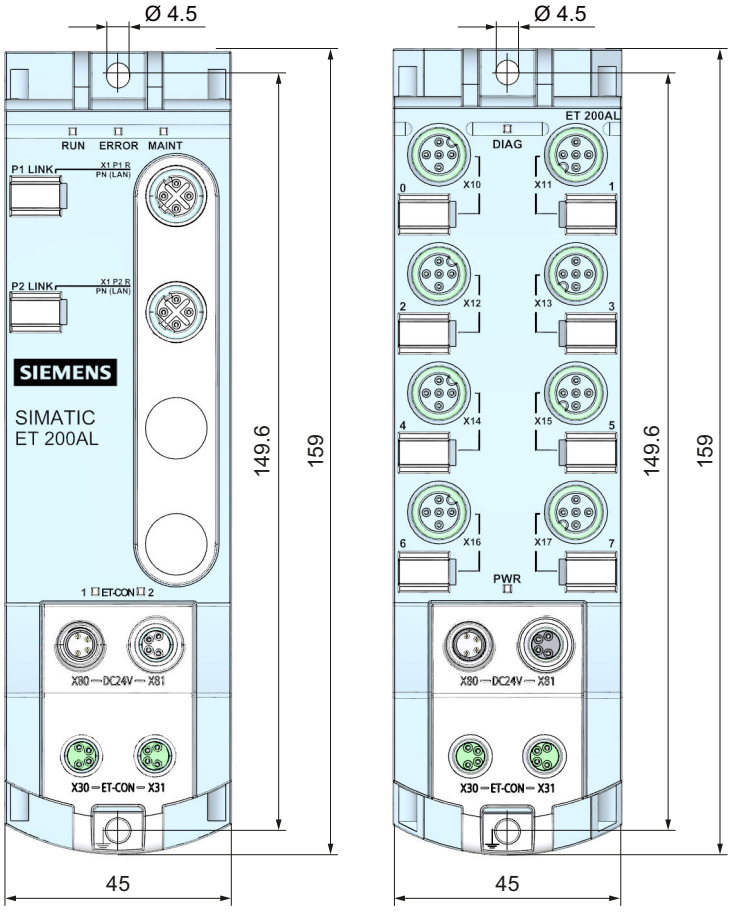


Figure 1-8 Dimensions for mounting interface modules and 45 mm I/O modules

Mounting 30 mm I/O modules (front or side)

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/95886672)

The 30 mm I/O modules have an attachment point on top and on the bottom. You also have the option of fastening the 30 mm I/O modules at the side. When fastening them at the side, you must use the supplied spacers.

To mount a 30 mm I/O module, follow these steps:

1. Drill 2 fastening holes with 4.5 mm diameter at a distance of 149.6 mm.
2. Use the supplied spacers for side fastening of the I/O module on the top and bottom (on one side adjacent to the fastening surface).
3. Fasten the I/O module with the screws to both fastening points (tightening torque 1.2 Nm).

The figure below shows the dimensions for fastening the 30 mm I/O modules using the example of the DIQ 4+DQ 4x24VDC/0.5A 8xM8 I/O module.

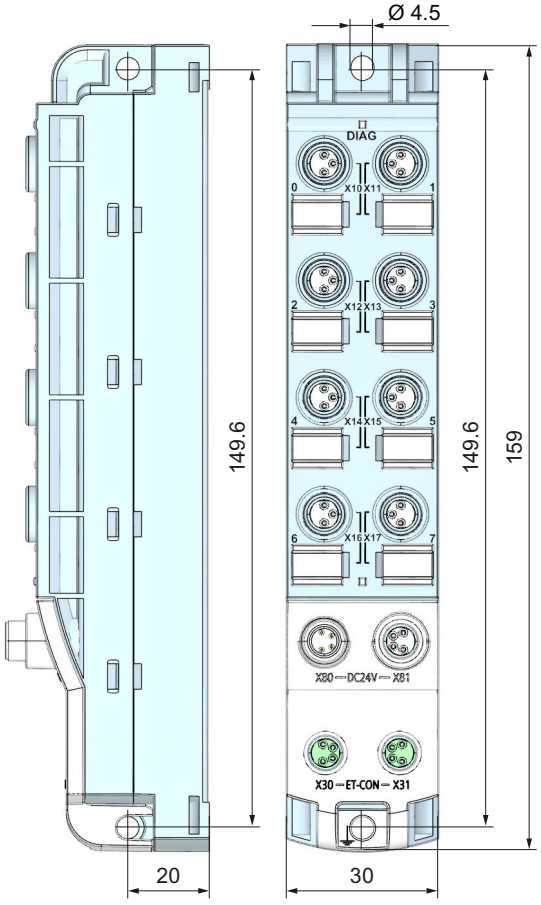


Figure 1-9 Dimensions for mounting 30 mm I/O modules

Fastening for cable ties

All module of the ET 200AL distributed I/O system have an integrated attachment point for cable ties. The attachment points are found on all four corners of the modules.

The figure below shows the top left attachment point for 2.5 mm wide cable ties for fastening the cables.

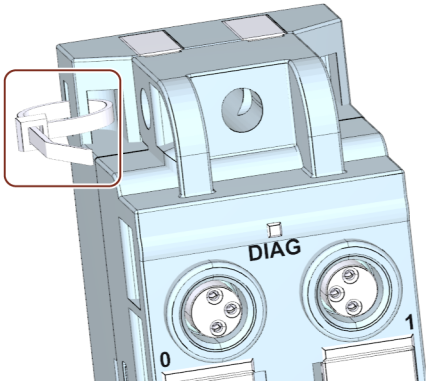


Figure 1-10 Top left attachment point for cable ties

Connecting 7

7.1 Rules and regulations for operation

Introduction

Depending on the area of application, the ET 200AL distributed I/O system, as a component of plants and systems, requires that special rules and specifications be observed.

This section gives an overview of the most important rules to be followed for integration of the ET 200AL distributed I/O system in a plant or in a system.

Specific application

Follow the safety and accident prevention regulations applicable to specific applications, e.g. the machinery directive.

EMERGENCY-STOP device

EMERGENCY-STOP devices according to IEC 60204 (corresponds to DIN VDE 113) must remain in effect in all operating modes of the plant or system.

Excluding hazardous system conditions

Hazardous plant states must not occur.

Ensure that dangerous system conditions are excluded, even in the following situations:

- In the event of a voltage dip or power outage
- When the plant restarts after a voltage dip or power outage
- When the ET 200AL distributed I/O system restarts after interruption of PROFINET communication

If necessary, force the EMERGENCY OFF.

An uncontrolled or undefined startup is not permitted after the "EMERGENCY STOP" is unlocked.

Cables and wires

The cables and lines used including the connector must fulfill the following requirements:

- Designed for at least the supply voltage used
- Designed for continuous cable temperature of at least 20 K above the ambient air temperature of the ET 200AL modules.
- Conductor cross-section suitable for the application and fusing.

An example for the line voltage drop at the used cables and lines is available in the section "Connecting cables for ET 200AL (Page 60)".

External fuses/switches

External fuses and switches must be installed so that they meet the standards for cable and device protection applicable to your application.

Line voltage of the SELV/PELV power supply

The following section describes what you need to pay attention to with respect to the line voltage (you will find additional information in the section Information on insulation, protection class, degree of protection, and rated voltage (Page 126)):

- For stationary plants or systems without an all-pole line disconnector, there must be a disconnector unit (all-pole) fitted in the building installation.
- For load current supplies, the configured rated voltage range must correspond to the local line voltage.
- For all power circuits of the ET 200AL distributed I/O system, the fluctuation/deviation of the line voltage from the rated value must be within the permitted tolerance.

24 V DC supply

Below there is a description of what you need to pay attention to with 24 V DC supply:

- For buildings:
  If there is a danger due to overvoltages, you must take lightning protection measures for external lightning protection (e.g. lighting protection elements).
- With 24 V DC supply lines and signal lines:
  If there is a danger due to overvoltages, you must take lightning protection measures for internal lightning protection (e.g. lightning protection elements. You will find additional information in the Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566) function manual).

- For 24 V DC supply:
  Ensure that there is safe (electrical) separation of low voltage (SELV/PELV) according to IEC 61010-2-201 or IEC 60950-1.
  Use a UL/IEC-approved fuse for the infeed supply voltages.
  - For interface modules and I/O modules: 28.8 V DC/4 A fuse (type B or type C tripping characteristic). Ensure that the fuse used blows within 120 s at a current of 8.33 A.

    NOTE

    The 4 A fuse is not required if you use the voltage distributor PD 24VDC for the voltage supply.

  - For voltage distributor PD 24VDC:

    For UL approval usage: 28.8 V DC/10 A or 28.8 V DC/15 A (tripping characteristic type T according to UL 248-15), depending on the cable cross-section used.

    For IEC usage: 28.8 V DC/10 A or 28.8 V DC/16 A (tripping characteristic type B or type C), depending on the cable cross-section used.
- Continuous operation of fail-safe modules with more than 28.8 V DC can result in personal injury and equipment damage.

⚠ WARNING

Continuous operation of fail-safe modules with more than 28.8 V DC can result in personal injury and equipment damage.
Certain transients from certain source impedances (for example according to EN 61000-4-2, 61000- 4-4 and 61000-4- 5), as specified in the "Electromagnetic compatibility" section, can act on this voltage without interrupting operation or causing damage.
Operate the fail-safe module within the voltage parameters specified in the technical specifications. This will avoid unacceptable temperature increases and heat damage that will cause the module to lose its functionality.

Requirements for power supplies in the event of a power interruption

To ensure compliance with IEC 61131-2, use only power supply units/power supplies with a power failure bridging time of at least 20 ms. Observe the relevant requirement in your product standards (e.g. 30 ms for "burners" according to EN 298) with regard to possible voltage interruptions. You can find the latest information on power supply components on the Internet.

Protection against outside electrical influences

Below is a description of what you must pay attention to in terms of protection against electrical impacts and/or faults:

- For all plants or systems in which the ET 200AL distributed I/O system is integrated, you must ensure that the equipment or system is functionally grounded to discharge electromagnetic interference.
- For supply, signal and bus cables, you must ensure that the cable routing and installation is correct.
- For signal and bus cables, you must ensure that a wire/cable breakage or a cross-wire does not lead to undefined states of the plant or system.

Reference

Additional information can be found in the function manual Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566).

7.2 Additional rules and regulations for the operation of the ET 200AL with fail-safe modules

7.2.1 Safety extra-low-voltage (SELV, PELV) for fail-safe modules

⚠ WARNING

The fail-safe modules must be operated with a safe extra-low voltage (SELV, PELV).
You can find additional information on safety extra-low voltage (SELV, PELV) in the data sheets of the applicable power supplies, for example.
The fail-safe modules operate at a rated voltage of 24 V DC. The tolerance range is 20.4 V DC to 28.8 V DC.
Within the overvoltage range from 28.8 V DC to 35 V DC, the F-modules react in a fail-safe manner and the inputs and outputs are passivated. For overvoltages higher than 35 V DC, the F-modules are permanently de-energized.
Use a power supply unit that does not exceed U_m = 35 V DC even in the event of a fault. For more on this, refer to the information in the data sheet on overvoltage protection in the case of an internal error. Or implement appropriate measures to limit the voltage, e.g. use of an overvoltage protector.
All system components that can supply electrical energy in any form whatsoever must fulfill this condition.
Each additional circuit (24 V DC) used in the system must have a safety extra-low voltage (SELV, PELV). Refer to the relevant data sheets or contact the manufacturer.
Sensors and actuators with an external power supply can also be connected to F-modules. Make sure that power is supplied to these components from safety extra-low voltage (SELV, PELV) as well. The process signal of a 24 V DC digital module must not exceed a fault voltage U_m in the event of a fault.

⚠ WARNING

Even when a fault occurs, the permissible potential difference between the supply of the interface module (bus voltage) and the load voltage must not be exceeded.
An external direct electrical connection is one way to meet this requirement. This also prevents potential differences from causing voltage additions at the individual voltage sources, which would cause the fault voltage U_m to be exceeded.

Immunity to surge voltages

To meet the product standard for burner controls (EN 298), the wiring must be equipped with external protection against coupled surge voltages caused by lightning. Further information on this can be found in the function manual Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566).

7.2.2 Requirements for sensors and actuators for fail-safe modules

General requirements for sensors and actuators

Note the following important warning regarding safety-related use of sensors and actuators:

⚠ WARNING

Note that instrumentation with sensors and actuators bears a considerable **safety responsibility**. Remember, too, that sensors and actuators do not generally withstand proof-test intervals of 20 years as defined in IEC 61508 without considerable loss of safety.
The probability of hazardous faults and the rate of hazardous faults of safety functions must comply with an SIL-defined high limit. A listing of values achieved by F-modules in the technical specifications of the F-modules is available under "Fail-safe performance characteristics".
To achieve the required safety class, suitably qualified sensors and actuators are necessary.

Additional sensor requirements

General rule: To achieve SIL3/Cat. 3/PLe, a single-channel sensor is adequate. However, to achieve SIL3/Cat. 3/PLe with a single-channel sensor, the sensor itself must be SIL3/Cat. 3/PLe-capable; otherwise the sensor must be connected by two channels to achieve this safety level.

To achieve SIL3/Cat. 4/PLe, sensors must be connected by two channels.

⚠ WARNING

In the case of fail-safe input modules, the value "0" is output to the F-CPU after detection of faults. You therefore need to make sure that the sensors are implemented in such a way as to ensure the reliable reaction of the safety program when the sensor is in the "0" state.
Example: In its safety program, an EMERGENCY-STOP sensor must achieve the shutdown of the relevant actuator when it is in the "0" state (EMERGENCY-STOP button pressed).

Duration requirements for sensor signals

⚠ WARNING

Observe the following requirements for sensor signals:

- To ensure the correct detection of the sensor signals via fail-safe modules with inputs, you need to make sure that the sensor signals are output for a minimum duration.
- For pulses to be detected with certainty, the time between two signal changes (pulse duration) must be greater than the PROFIsafe monitoring time.

Reliable detection by F-modules with inputs

The minimum duration of sensor signals for F-modules with inputs depends on the configured input delay, the parameters of the short circuit test of the sensor supplies, and the configured discrepancy behavior for 1oo2 evaluation. The signal must be greater than the maximum response time of the configured application. Information on calculating the maximum response time can be found in the section "Response times" of the relevant F-module.

The maximum permitted switching frequency of the sensor signals results from the minimum duration.

Additional requirements for actuators

The fail-safe output modules test the outputs at regular intervals. The F-module briefly switches off the activated outputs and, if necessary, switches on the deactivated outputs. You can assign the maximum duration of the test pulses (dark and light period) with parameters.

Fast reacting actuators may briefly drop out or be activated during the test. If your process does not tolerate this, set the pulse duration of the light or dark test correspondingly or use actuators that have sufficient lag.

⚠ WARNING

If the actuators switch voltages greater than 24 V DC (e.g. 230 V AC), the outputs of a fail-safe output module and the parts carrying a higher voltage must be electrically isolated (in accordance with IEC 60664-1).
This is generally the case for relays and contactors. Particular attention must be paid to this with semiconductor switching devices.

Technical specifications of sensors and actuators

Refer to the manuals of the fail-safe modules for technical specifications to assist you in selecting sensors and actuators.

7.2.3 Crosstalk of digital input/output signals

Readback errors may occur on the F-DQ channels if the fail-safe digital output signals and fail-safe digital input signals are routed through a single cable.

Cause: capacitive crosstalk

During the bit pattern test of the outputs or the sensor supply of the inputs, the steep switching edge of the output drivers caused by the coupling capacitance of the line may result in crosstalk to other non-activated output or input channels. This may then lead to a response of the readback circuit in these channels. A cross circuit/short-circuit is detected, which leads to safety-related tripping.

Remedy:

- Separate cables for fail-safe DQ modules and non-fail-safe DQ modules
- Separate cables for F-DQ channel and F-DI channels
- Coupling relay or diodes in the outputs
- Disable the sensor supply test if safety class requirements allow it.

Cause: magnetic crosstalk

Note that an inductive load connected to the F-DQ channels can induce coupling of a strong magnetic field.

Remedy:

- Separate the inductive loads spatially or shield against the magnetic field.
- Configure the readback time to 50 ms or higher.

7.3 Operation of the ET 200AL on grounded/non-grounded infeed

Introduction

Information is provided below on the overall configuration of an ET 200AL distributed I/O system on a grounded incoming supply (TN-S network). The specific subjects discussed are:

- Disconnecting devices, short-circuit and overload protection to IEC 60364 (corresponding to DIN VDE 0100) and IEC 60204 (corresponding to DIN VDE 0113)
- Load current supplies and load circuits
- Supply voltages of the ET 200AL distributed I/O system

Grounded infeed

In grounded incoming supplies, the neutral conductor of the supply system is grounded. A simple ground fault between a live conductor and ground or a grounded section of the plant causes the protective devices to trip.

Supply voltages

Provide the ET 200AL distributed I/O devices with a SELV/PELV supply voltage for 1L+.
The supplied SELV/PELV load voltage for 2L+ can be switched, depending on the application.

- 1L+: Supply voltage (non-switched)
- 2L+: Load voltage (switched)

Safe electrical separation (SELV/PELV)

For operating the ET 200AL distributed I/O system, mains devices/power supply modules with safe electrical separation SELV/PELV are required. These power supplies/power supply modules must comply with IEC 61010-2-201.

The wiring of SELV/PELV circuits must be separated from the wiring of non-SELV/PELV circuits. Alternatively, the insulation of all conductors must be dimensioned for the higher voltage.

NOTICE
Operation in damp/wet environments When operating in a damp/wet environment, other voltage limits apply for SELV/PELV according to IEC 61010-2-201.

Configuring ET 200AL with grounded reference potential

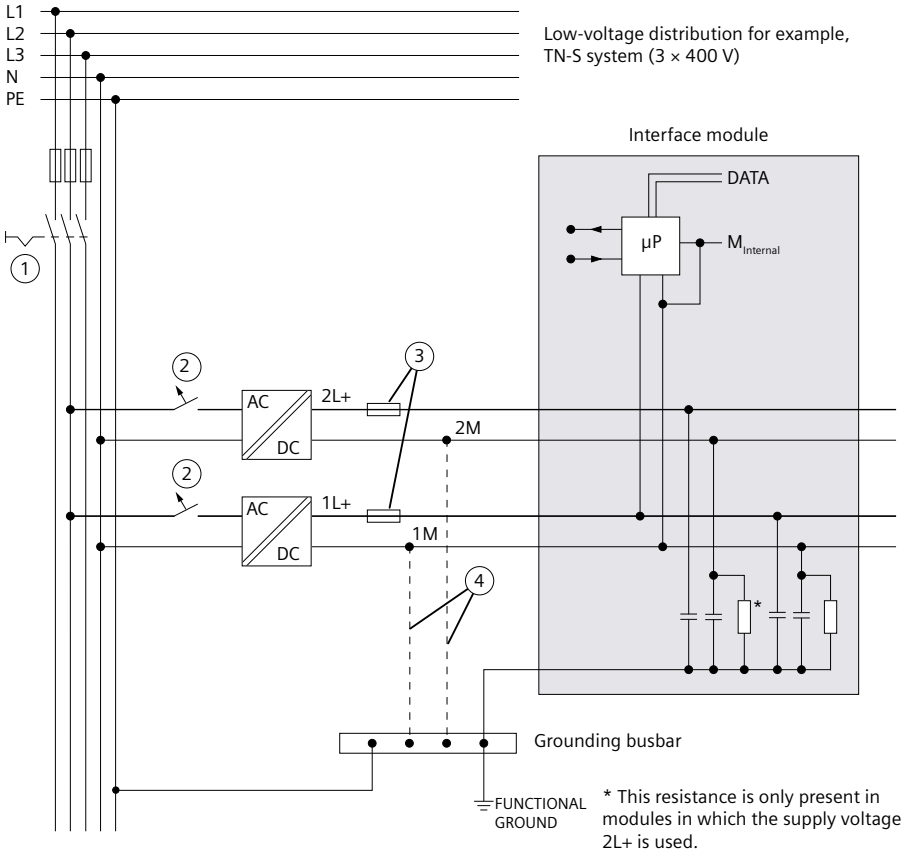
When configuring the ET 200AL distributed I/O system with grounded reference potential, occurring interference currents are discharged into functional ground. The connections must be externally connected (connection between 1M and functional ground).

Configuring ET 200AL with ungrounded reference potential

When configuring the ET 200AL distributed I/O system with non-grounded reference potential, occurring interference currents are discharged via an internal RC network to functional ground (no external connection between 1M and functional ground).

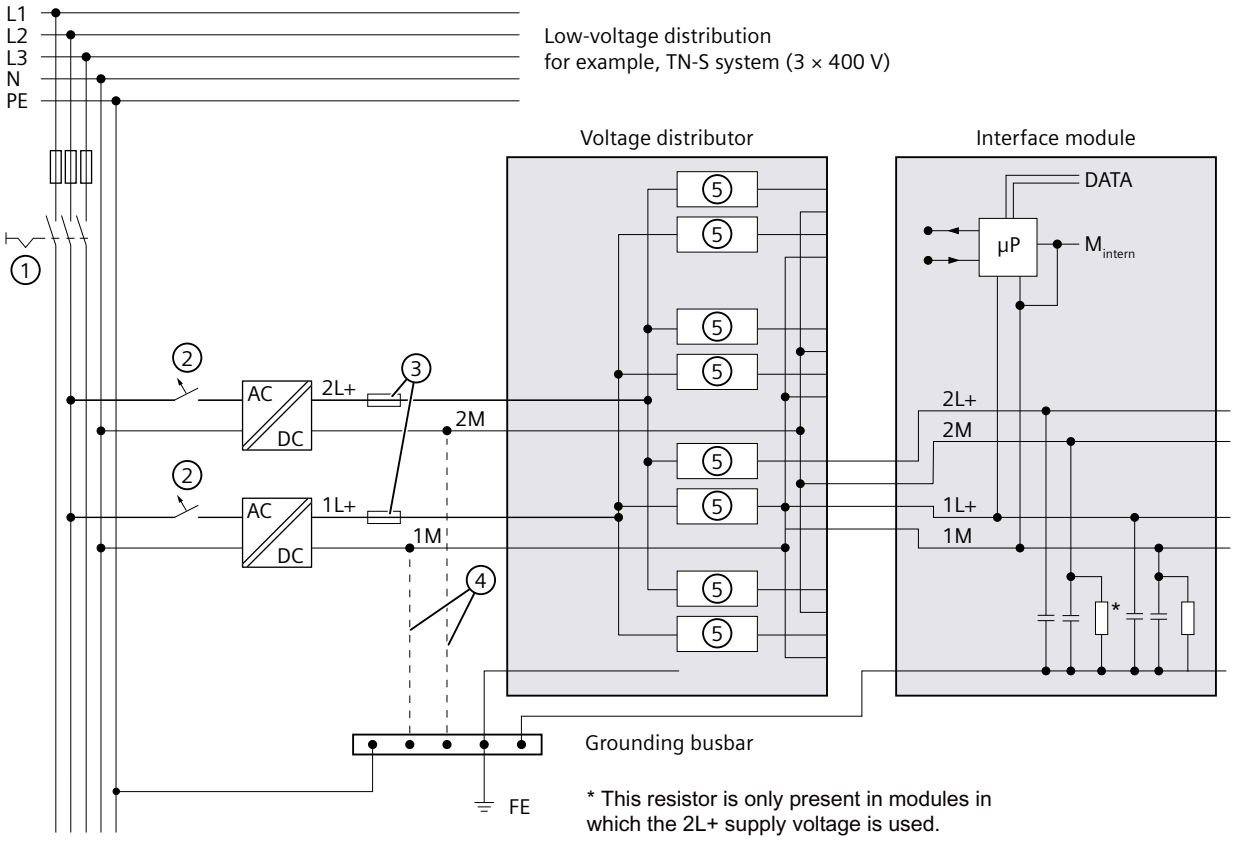
ET 200AL in the overall configuration

The figures below show the ET 200AL distributed I/O system in the complete electrical configuration using an interface module with and without voltage distributor as the example.



① Main switch
② Short-circuit and overvoltage protection
③ Fuses for cable protection (fuse for 4 A)
④ When configuring the ET 200AL distributed I/O system with non-grounded reference potential, no connection is made between 1M, 2M and functional ground

Figure 1-11 Electrical configuration



① Main switch
② Short-circuit and overvoltage protection
③ Fuses for cable protection (see Rules and regulations for operation (Page 41))
④ When configuring the ET 200AL distributed I/O system with non-grounded reference potential, no connection is made between 1M, 2M and functional ground
⑤ Integrated short-circuit protection electronic 4 A

Figure 1-12 Electrical configuration with voltage distributor

Components and protective measures

Various components and protective measures are stipulated for setting up a complete plant. The types of components and the degree to which the protective measures are mandatory depend on the IEC regulation that applies to your plant setup.

The following table shows the components of the electrical configuration with reference to the previous figure and compares the IEC regulations.

Table 1-7 Components of electrical configuration

	Reference to illustration	IEC 60364 (DIN VDE 0100)	IEC 60204 (DIN VDE 0113)
Disconnection element for controller, sensors, and actuators	①	Main switch	Disconnector
Short-circuit / overload protection	②	Single-pole protection of circuits Secure all incoming supply cables with a circuit breaker. (See Rules and regulations for operation (Page 41))	Secure single pole for a grounded secondary circuit
Cable protection	③	Protection of cables and wires against overcurrent	-

Insulation monitoring

In the following situations, you must provide insulation monitoring:

- When configuring the ET 200AL distributed I/O system with non-grounded reference potential
- When hazardous system conditions may occur due to errors

7.4 Electrical configuration of the ET 200AL distributed I/O system

Electrical isolation

When electrically configuring the ET 200AL distributed I/O system, there is electrical isolation between:

- Load voltage 2L+ and all other switching parts
- Communication interfaces (PROFINET/PROFIBUS) of the interface modules and all other switching parts
- ET-Connection and all other switching parts

The following images show the potential conditions of the modules of the ET 200AL distributed I/O system.

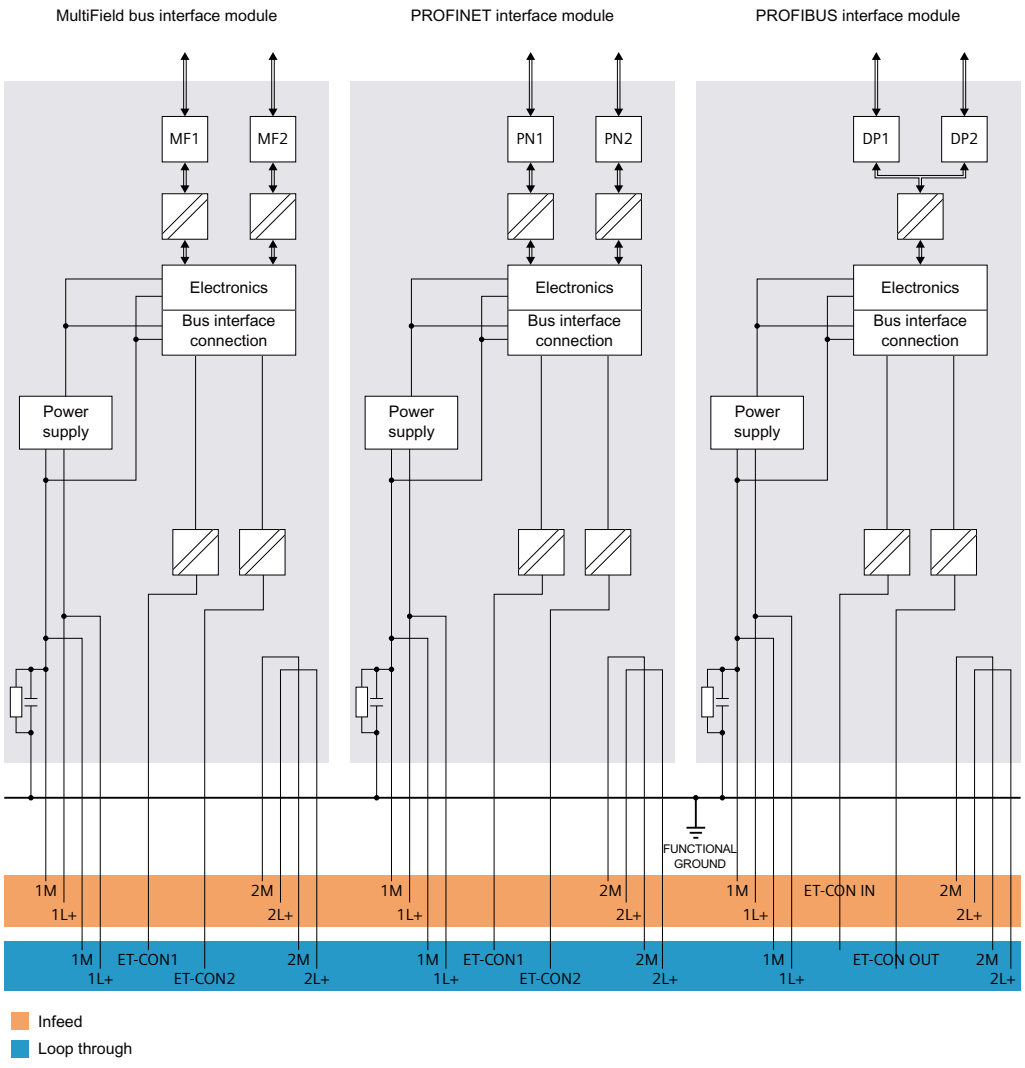


Figure 1-13 Potential conditions of the ET 200AL distributed I/O system (Part 1)

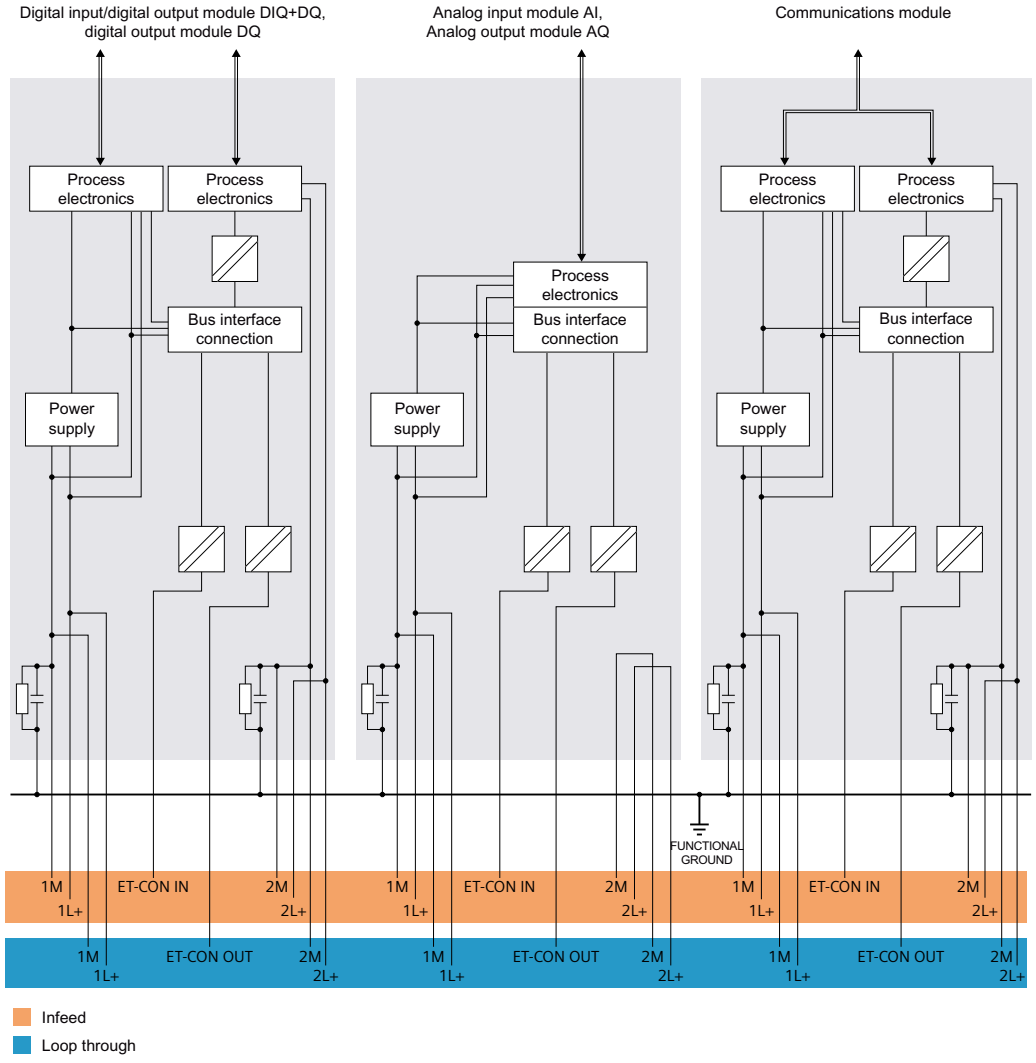


Figure 1-14 Potential conditions of the ET 200AL distributed I/O system (Part 2)

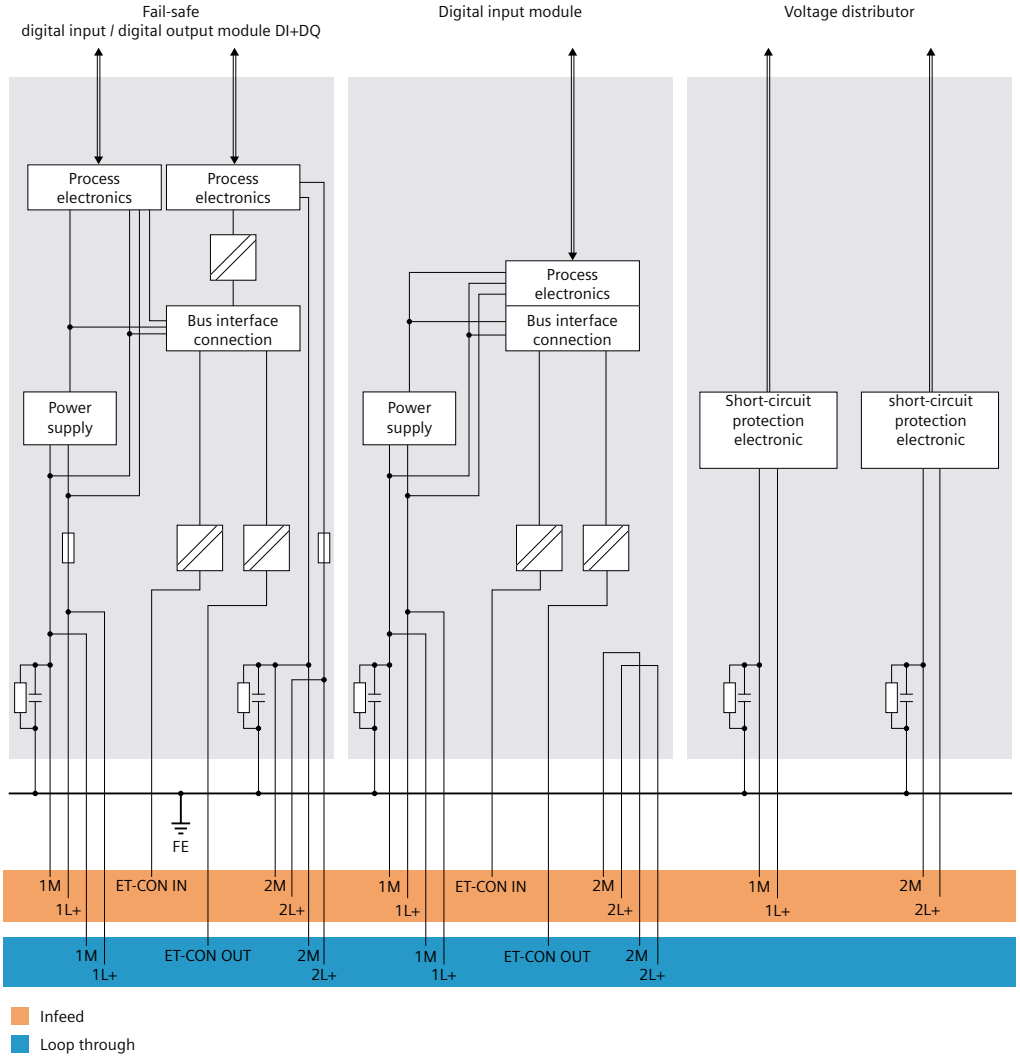


Figure 1-15 Potential conditions of the ET 200AL distributed I/O system (Part 3)

Connection of a digital output with a digital input

NOTICE
Pay attention to the potential group When a digital output is connected to a digital input, pay attention to the potential groups. Depending on the configuration, 1M and 2M may then be connected, resulting in elimination of the electrical isolation between 1L+ and 2L+. The possible compensating currents can destroy the digital module.

⚠ WARNING

Note potential groups for safety-related shutdown
When a digital output is connected to a digital input, pay attention to the potential groups. Depending on the configuration, 1M and 2M may then be connected, resulting in elimination of the electrical isolation between 1L+ and 2L+.
Safety-related shutdown is not permitted if electrical isolation has been eliminated.

Cable protection

According to IEC 60364, cable protection is required. Secure the supply cables externally.

Information about the fuses can be found in the section "Rules and regulations for operation (Page 41)" under "24 V DC supply".

Power supply of the configuration

Two voltage groups are available for the distributed I/O system ET 200AL: 1L+ (supply voltage) and 2L+ (load voltage).

A second infeed may be needed to supply all the modules of a configuration with the required voltage. Renewed voltage supply of 1L+ and 2L+ can be necessary to configure different potential groups or because the voltage is not sufficient for all modules due to the voltage drop. Create a power balance for the selection of the infeed point of the voltage.

NOTE

Turning 1L+ and 2L+ on and off
In contrast to the load voltage 2L+, the operational switching on and off of the supply voltage 1L+ results in a restart of the module.

The figure below shows a configuration with a new voltage infeed for the modules. The different potential groups have a gray background.

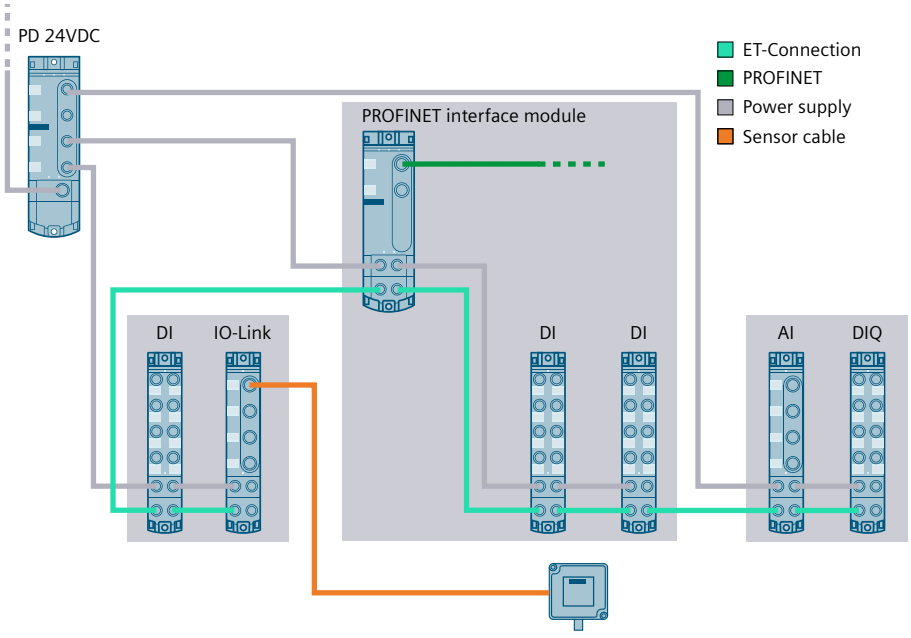


Figure 1-16 Wiring of the power supply

Reference

You will find additional information on electrical configuration and the voltage drop in the section Connecting cables for ET 200AL (Page 60).

7.5 Connecting ET 200AL to functional earth

Introduction

You must connect the distributed I/O system ET 200AL to functional earth (FE)

What is functional earth?

All ET 200AL modules feature a functional earth connection. This connection is used to suppress interference sensitivity, but not for protection purposes. With the functional earth connection, you create an electrical connection directly to a point of your system or shielding. This discharges the EMC interference directly into the earth. By discharging the EMC interference, the interference safety of the entire module is increased.

The figure below shows the symbol with which the functional earth connection is identified on the ET 200AL modules.

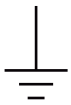


Figure 1-17 Functional earth

7.5.1 Mounting ET 200AL modules on conductive substrate

Requirement

Conductive substrate for mounting of the module

Required tools

To connect to functional earth, you need the following tools:

- Screwdriver

Required accessories:

To connect to functional earth, you need the following accessories:

- 2 x M4 fastening screws.

Mounting

To connect modules of the ET 200AL distributed I/O system to functional earth with a conductive mounting substrate, proceed as follows:

1. Drill two fastening holes.
2. Screw the module with the M4 fastening screws using a torque of 1.2 Nm.

NOTE

Earthing with conductive mounting substrate

When you fasten a module of the ET 200AL distributed I/O system on a conductive, grounded substrate, the bottom fastening screw provides a conductive connection to the ground potential.

Ensure that there is a low-impedance connection between the module and conductive underground as well as between the conductive underground and functional earth.

Reference

You will find more information on installing the modules in the section Mounting modules (Page 37).

7.5.2 Mounting ET 200AL modules on non-conductive substrate

Requirement

Conductive substrate for mounting of the module

Required tools

To connect to functional earth, you need the following tools:

- Screwdriver
- Stripping tool
- Crimp tool

Required accessories:

To connect to functional earth on a non-conductive fastening substrate, you need the following accessories:

- 2 x M4 fastening screws.
- Cable lug suitable for M4 screws
- Grounding cable (braided copper cable) with a minimum cross section of 4 mm^2

Mounting

To connect modules of the ET 200AL distributed I/O system to functional earth, proceed as follows:

1. Drill two fastening holes.
2. Strip the grounding cable.
3. Fasten the cable lug to the grounding cable.
4. Screw the module and the cable lug with the M4 fastening screws using a torque of 1.2 Nm.

The figure below shows how to connect functional earth using the example of the IM 157-1 PN interface module.

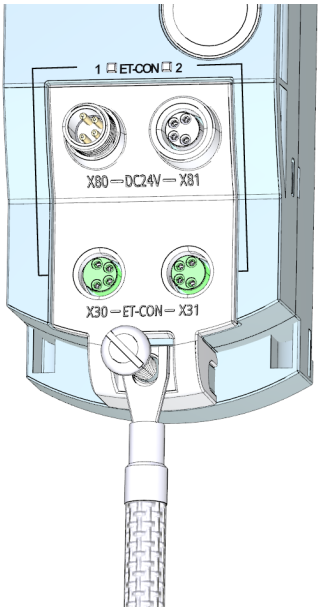


Figure 1-18 Connecting the functional earth

NOTE

Earthing with non-conductive mounting substrate

Make sure there is a low-impedance connection between the module and the functional earth.

Reference

You will find more information on installing the modules in the section Mounting modules (Page 37).

7.6 Connecting cables for ET 200AL

7.6.1 Wiring rules for the interface module and I/O modules

Impact of cable length on the supply voltage

When you wire your configuration, you must take into account the impact of the cable length on the supply voltage of the ET 200AL distributed I/O system.

CAUTION

Pay attention to maximum incoming currents
For interface modules and I/O modules, you may feed a maximum of 4 A per power supply (1L+, 2L+).
Comply with the maximum infeed currents and the required cable cross-sections. If you do not comply with the specifications, then an increased infeed current can lead to overheating of the cable insulation and the contacts. This could result in damage to the modules.

The figure below shows the voltage drop depending on the cable length for 4 current strengths, using the example of a copper cable with ∅ 0.5 mm².

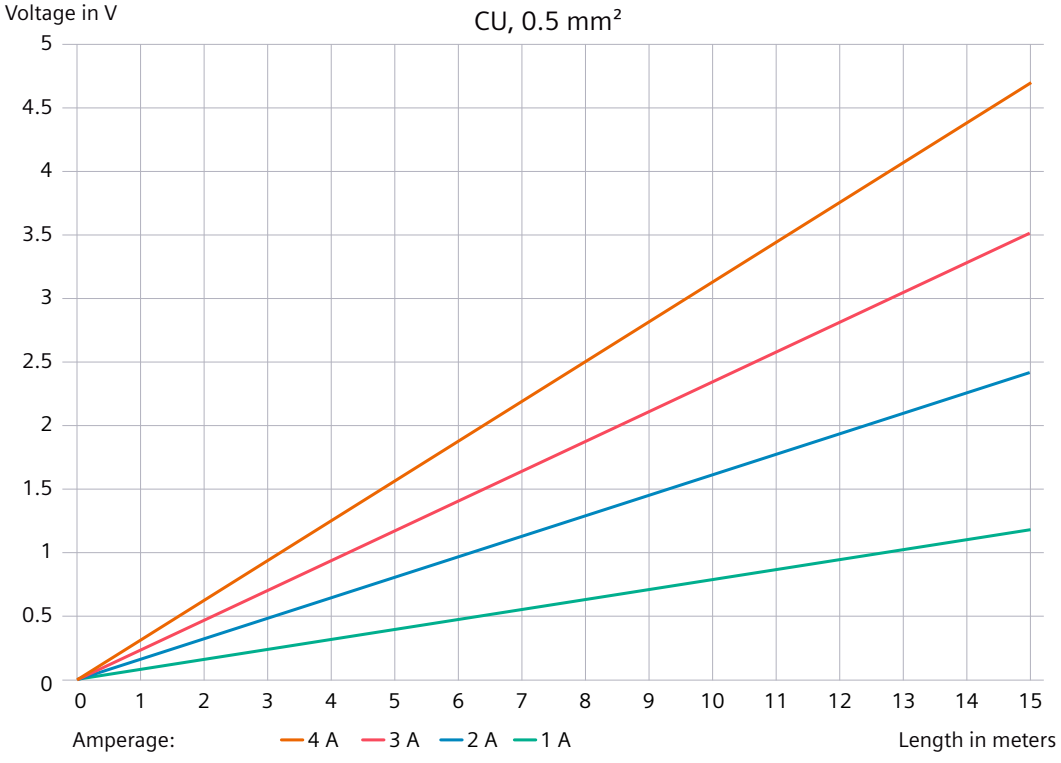


Figure 1-19 Voltage drop with a cable cross-section of 0.5 mm²

To estimate the voltage drop in your ET 200AL distributed I/O system, you must add the voltage drops of the different cables. For every module used, you must add an additional voltage drop of around 0.1 V.

Example

If you have a 7 m power supply cable with ∅ 0.5 mm², the voltage drop is around 1.5 V with a load of 3 A.

7.6.2 Connecting cables for voltage distributor PD 24VDC

Impact of cable length on the supply voltage

When you wire your configuration, you must take into account the impact of the cable length on the supply voltage of the ET 200AL distributed I/O system.

⚠ CAUTION

Pay attention to maximum incoming currents
For each power supply (1L+, 2L+), you can feed in a maximum of 15 A.
Comply with the maximum infeed currents and the required cable cross-sections. If you do not comply with the specifications, then an increased infeed current can lead to overheating of the cable insulation and the contacts. This could result in damage to the modules.

To estimate the voltage drop in your ET 200AL distributed I/O system, you must add the voltage drops of the different cables.

Voltage drop for copper cable with ∅ 2.5 mm²

The figure below shows the voltage drop depending on the cable length for 4 current strengths, using the example of a copper cable with ∅ 2.5 mm².

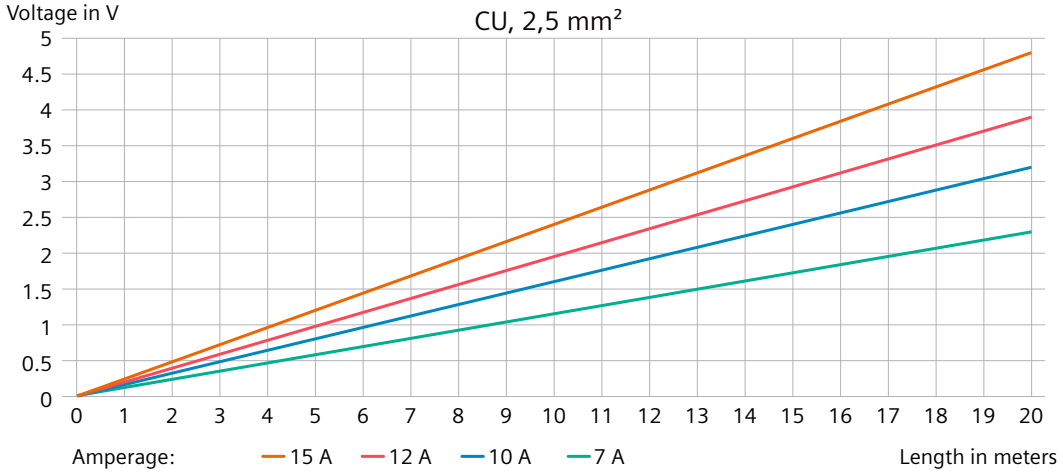


Figure 1-20 Voltage drop with a cable cross-section of 2.5 mm²

Example

If you have a 15 m power supply cable with ∅ 2.5 mm², the voltage drop is around 2.4 V with a load of 10 A.

7.7 Wiring

Connection

Connect all cables to the front side of the modules:

- Supply voltage and ET-Connection to the 4-pin M8 round sockets and M8 round connectors
- Signal lines to the 3-pin M8 or 4/5-pin M12 round sockets
- Fieldbus lines to the 4/5 pole M12 round sockets and M12 round connectors

NOTE

Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Requirement

Wire the modules with the supply voltage off.

Required tools

If you are not using pre-assembled cables, you need the following tools:

- Stripping tool
- Screwdriver to wire the connection plugs
- Stripping Tool for ET-Connection

Required accessories when connecting the supply voltage

You need the following accessories:

- Cables
  - Pre-assembled power cable, M8, 4-pin, or
  - Flexible 4-wire copper cable (wire cross section: 0.25 to 0.5 mm^2)
- 4-pin M8 connection plug

Accessories required for the connection of ET-Connection

You need the following accessories:

- ET-Connection cables
- 4-pin M8 connection plug

NOTE

ET-Connection cables
When connecting ET-Connection **use only** the offered cables.

Connecting M8 plugs

To connect M8 plugs, proceed as follows:

1. Insert the connector in the appropriate round socket on the module.
   Make sure that there is proper locking between the connector and socket.
2. Tighten the connector using the knurled screw with a torque of 0.4 Nm.

The figure below shows the connection of the M8 plugs, using the example of the DIQ 4+DQ 4x24VDC/0.5A 8xM8 digital input / digital output module.

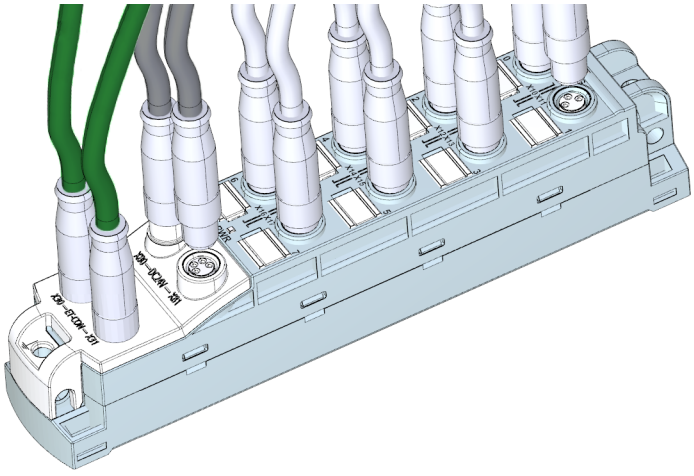


Figure 1-21 Connecting M8 plugs

Connecting M12 plugs

To connect M12 plugs, proceed as follows:

1. Insert the connector in the appropriate round socket on the module.
   Make sure that there is proper locking between the connector and socket (nut and spring).
2. Tighten the connector using the knurled screw with a torque of 1 Nm.

The figure below shows the connection of the M12 plugs, using the example of the analog input module AI 4xU/I/RTD 4xM12.

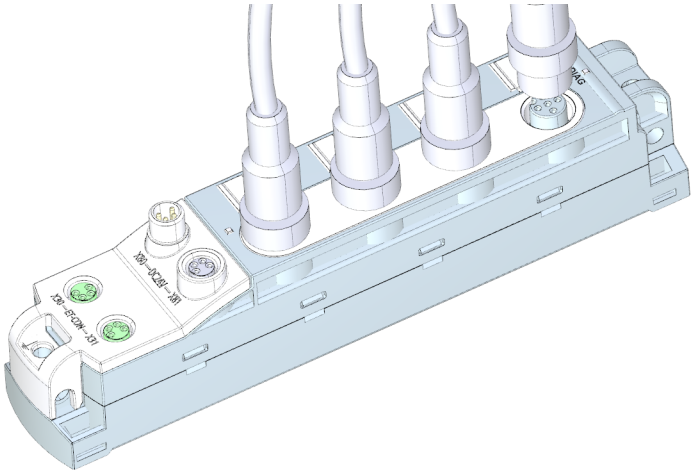


Figure 1-22 Connecting M12 plugs

Pin assignment of the sockets

The pin assignment of the sockets can be found in the manuals for the interface modules (https://support.industry.siemens.com/cs/ww/en/ps/14246/man) and I/O modules (https://support.industry.siemens.com/cs/ww/en/ps/14247/man) in the section on pin assignment and on the side surface of the module.

Y-cable

The Y-cable allows you to connect two actuators or sensors to the inputs or outputs.

The use of a Y-cable is particularly recommended when two channels are occupied for each socket of an I/O device. The Y-cable distributes the channels to two circular connectors.

- Y-cable (6ES7194-6KA00-0XA0) for connecting 2 actuators or sensors for double connection of inputs (also fail-safe inputs) or double connection of outputs with one cable
- Y-cable (6ES7194-6KB00-0XA0) for connecting 2 sensors for double connection F-DI with one cable. Only suitable for use with the F-DI module.

You can find details about connection in the respective user manual of the product.

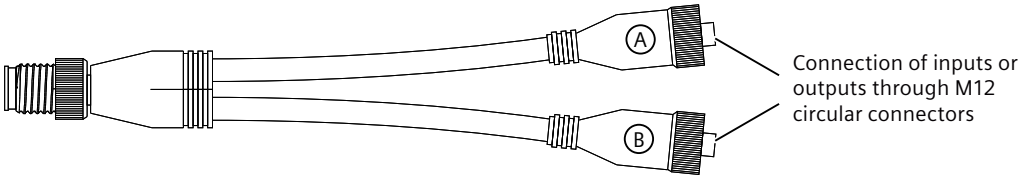
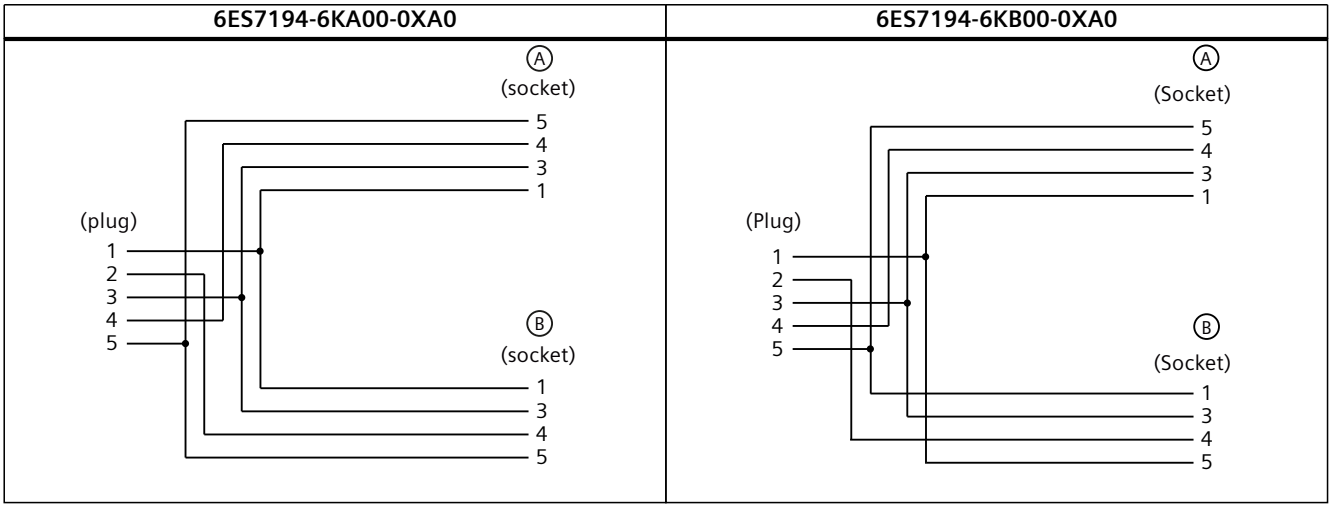


Figure 1-23 Y-cable

The following figure shows the wiring of the Y-cables.



Inverted Y-cable

The inverted Y-cable enables the connection of fail-safe inputs and a fail-safe output to an I/O device (for example a Siemens SIRIUS safety position switch with interlock) with only one cable.

You can find details about connection in the respective user manual of the product.

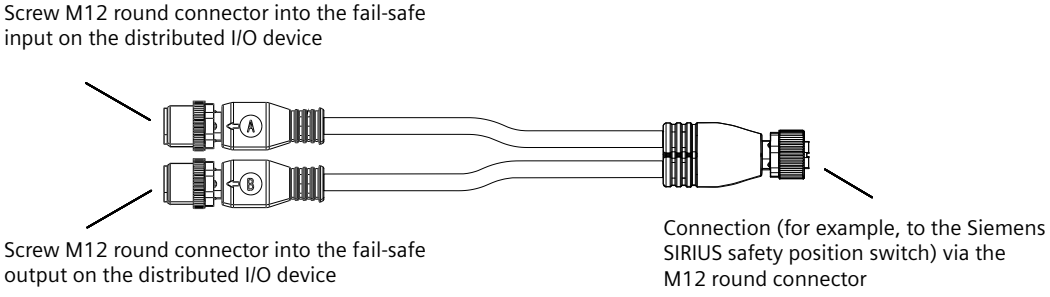


Figure 1-24 Inverted Y-cable

The following figure shows the wiring of the Y-cables.

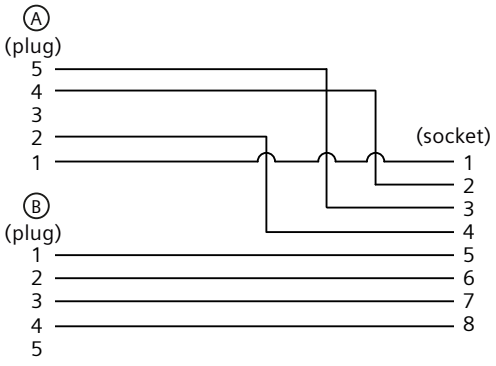


Figure 1-25 Y-cable 6ES7194-6KC00-0XA0

Sealing of unused sockets

To ensure IP65 or IP67 degree of protection, seal off all unused sockets with sealing caps.

Article numbers for accessories/spare parts.

You will find the article numbers in the Appendix in section Accessories/spare parts (Page 150).

7.8 ET 200AL marking

7.8.1 Factory markings

Introduction

For better orientation, the ET 200AL distributed I/O system is identified using various markings which will help you when configuring and connecting the modules.

Marking of the interfaces

The interfaces of the modules are factory-labeled.

The table below shows the labeling of the interfaces.

Table 1-8 Interface labeling

interface	Labeling
PROFINET IO interfaces MultiFieldbus interfaces	X1 P1R and X1 P2R
PROFIBUS DP interfaces	X1 DP1 and X1 DP2
I/O input and output interfaces	X10 to X17
ET-Connection interfaces (interface modules)	X30 (ET-CON1) and X31 (ET-CON2)
ET-Connection interfaces (I/O modules)	X30 (ET-CON IN) and X31 (ET-CON OUT)
Power supply interfaces	X80 (IN) and X81, X82, X83, X84 (OUT)

NOTE

Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

NOTICE
ET-Connection/supply voltage Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Pin assignment

The pin assignments of the various interfaces are lasered at the factory, on the side of every module.

7.8.2 Optional markings

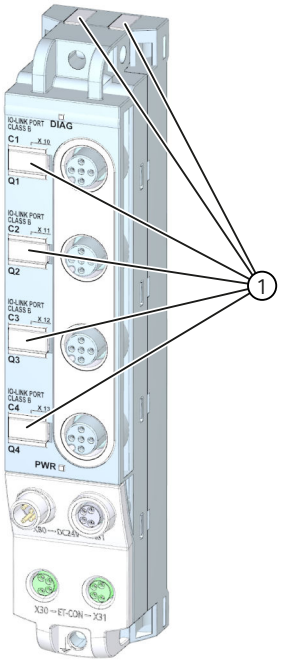
Introduction

In addition to the factory markings, there are also optional possibilities for labeling and/or identifying interfaces and modules on the ET 200AL distributed I/O system.

Identification label

The identification labels come with each module as strips and can be machine-printed. A strip has 10 identification labels measuring 10 x 5 mm in the color RAL9016. The identification labels can be inserted into every module at the points provided. The identification labels are used for channel, module and slot labeling.

The figure below shows all points where you can use the identification labels using the example of the IO-Link Master CM 4xIO-Link 4xM12 communication module.



① Identification labels

Figure 1-26 Optional marking

7.8.3 Mounting identification labels

Introduction

This section describes how to mount or remove identification labels.

Required tools

You need a screwdriver with 3 mm blade width (only to remove identification labels).

Mounting procedure

To mount an identification label, proceed as follows:

1. Print the identification label using commercially available marking systems.
2. Press the identification label out of its holder.
3. Stick the identification labels into the cutouts provided, as shown in the figure Optional marking (Page 67).

Mounting the identification labels is the same for all modules.

Removal procedure

To remove an identification label, proceed as follows:

1. Carefully use a screwdriver to pull out the identification label.

Removing identification labels is the same for all modules.

8 Configuring

8.1 Introduction

You configure and assign parameters for the ET 200AL distributed I/O system (interface modules and I/O modules) using STEP 7 or the configuration software of another manufacturer.

8.2 Requirements

Configuration software and requirements

The following table shows the configuration software that can be used and the associated requirements.

Table 1-9 Configuration software and requirements

Configuration software	Requirements	Installation information
STEP 7 (TIA Portal) as of V19 for modules: • IM 157-1 MF • CM 8xIO-Link + DIQ 6x24VDC/0.5A 8xM12 • CM 4xIO-Link 4xM12	As of Support Package HSP 0419	STEP 7 online help
STEP 7 Safety (TIA Portal) as of V17 for modules: • F-DI 4+F-DQ 2x24VDC/2A 4xM12	• PROFINET-compliant F-CPU (with CP expansion modules) • PROFIsafe-compliant F-PLC controller, 2.6.X (RIOforFA safety profile) or PROFIsafe 2.4	
STEP 7 (TIA Portal) as of V16 for modules: • AI 4xRTD/TC 4xM12	As of Support Package HSP 0313	
STEP 7 (TIA Portal) as of V14 for modules: • DIQ 16x24VDC/0.5A 8xM12 • AQ 4XU/I, 4XM12	As of Support Package HSP 0194	
STEP 7 (TIA Portal) V13 SP1 or higher for modules: • DI 8x24VDC 4xM12 • DI 16x24VDC 8xM12	As of Support Package HSP 0155	
STEP 7 (TIA Portal) V13 SP1 or higher for modules: • DIQ 4+DQ 4x24VDC/0.5A 4xM12 • DQ 8x24VDC/2A 8xM12	As of Support Package HSP 0156	
STEP 7 (TIA Portal) V13 SP1 or higher for modules: • IM 157-1 PN • IM 157-1 DP • DI 8x24VDC 8xM8 • DIQ 4+DQ 4x24VDC/0.5A 8xM8 • AI 4xU/I/RTD 4xM12 • CM 4xIO-Link 4xM12	None, integrated in STEP 7	
STEP 7 as of V5.5 SP4 for modules: • IM 157-1 PN • IM 157-1 DP	• PROFINET IO: As of Support Package HSP 0259 • PROFIBUS DP: as of Support Package HSP 0258	
STEP 7 as of V5.5 SP4 for all IO modules	As of Support Package HSP 0260	
STEP 7 (TIA Portal) as of V13 Update 3	• PROFINET IO GSD file: GSDML-Vx.y-Siemens-ET200AL-"Date in format yyyymmdd".xml (https://support.industry.siemens.com/cs/ww/en/view/92346477) for EXAMPLE: GSDML-V2.31-Siemens-ET200AL-20140507.xml • PROFIBUS DP GSD file: siem81A9.gsg (https://support.industry.siemens.com/cs/ww/en/view/92346281)	
Software of third-party manufacturer		Manufacturer documentation

Configuring the ET 200AL distributed I/O system

See the STEP 7 online help or the documentation of the configuration software manufacturer.

8.3 Configuration

8.3.1 MultiFieldbus maximum configuration

MultiFieldbus configuration

Each of the connections for ET-Connection occupies a slot in the configuration. The slots for ET-Connection1 and ET-Connection2 are pre-defined statically in the GSD file.
ET-Connection1 is always at slot 1 and ET-Connection2 at slot 18.

The fixed slot assignment of ET-Connection1 and ET-Connection2 offers you the following advantages:

- You can expand ET-Connection1 and ET-Connection2 without a high workload
- Transparency in configuration control
- Simplification of diagnostics alarms and troubleshooting

The figure below shows the maximum configuration with modules of the ET 200AL distributed I/O system.

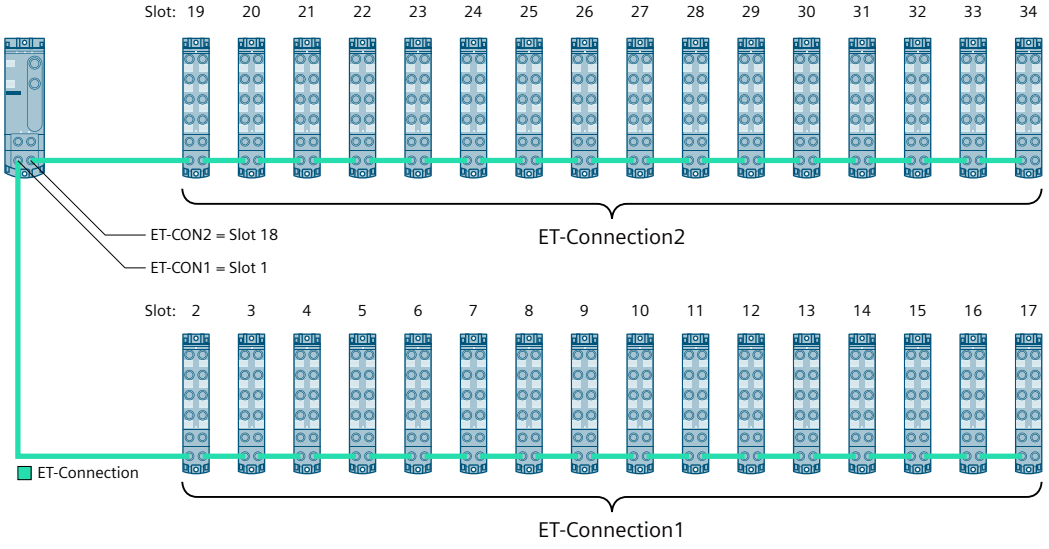


Figure 1-27 MultiFieldbus maximum configuration

Reference

You can find additional information on this topic in section Configuration control (option handling) (Page 76).

8.3.2 PROFINET maximum configuration

PROFINET configuration

Each of the connections for ET-Connection occupies a slot in the configuration. The slots for ET-Connection1 and ET-Connection2 are specified statically in the PROFINET GSD file. ET-Connection1 is permanently on slot 1 and ET-Connection2 on slot 18.

The fixed slot assignment of ET-Connection1 and ET-Connection2 offers you the following advantages:

- You can expand ET-Connection1 and ET-Connection2 without a high workload
- Transparency in configuration control
- Simplification of diagnostics alarms and troubleshooting

The figure below shows the maximum configuration with modules of the ET 200AL distributed I/O system.

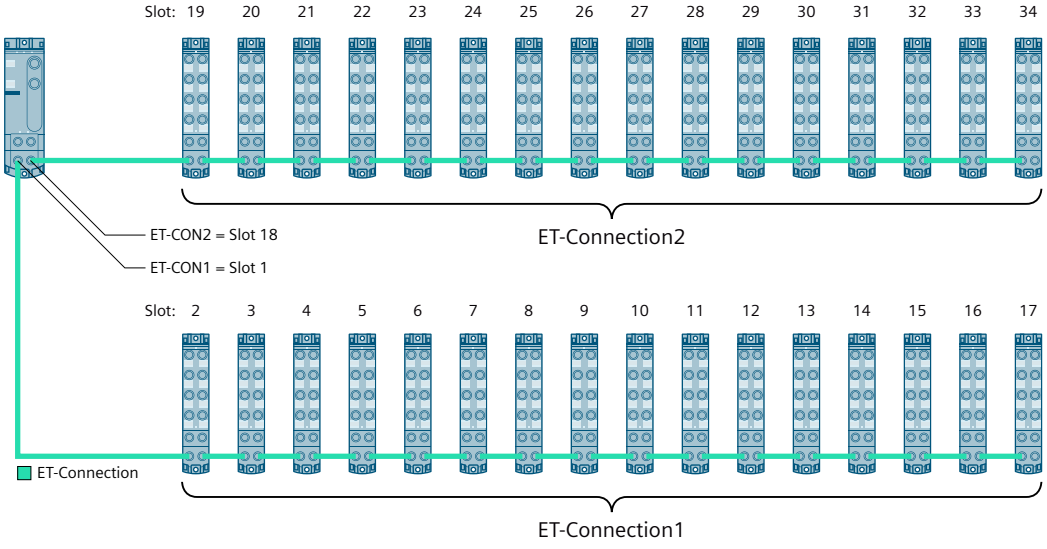


Figure 1-28 PROFINET maximum configuration

Reference

You can find additional information on this topic in section Configuration control (option handling) (Page 76).

8.3.3 PROFIBUS maximum configuration

PROFIBUS configuration

Each of the connections for ET-Connection occupies a slot in the configuration. The slot for ET-Connection1 is statically defined in the PROFIBUS GSD file. ET-Connection1 is always permanently installed in slot 1. Always place the topology module for ET-Connection2 on slot 18. You do not need to fill slots in the configuration for ET-Connection1 with dummy modules.

The fixed slot assignment of ET-Connection1 and ET-Connetion2 offers you the following advantages:

- You can expand ET-Connection1 and ET-Connection2 without a high workload; for ET-Connection1 you need to remove the placeholder, the I/O module is placeable (no placeholders are needed for ET-Connection2)
- You cannot configure more modules on ET-Connection1 or ET-Connection2 than are allowed.
- Transparency in configuration control
- Simplification of diagnostics alarms and troubleshooting

The figure below shows the maximum configuration with modules of the ET 200AL distributed I/O system.

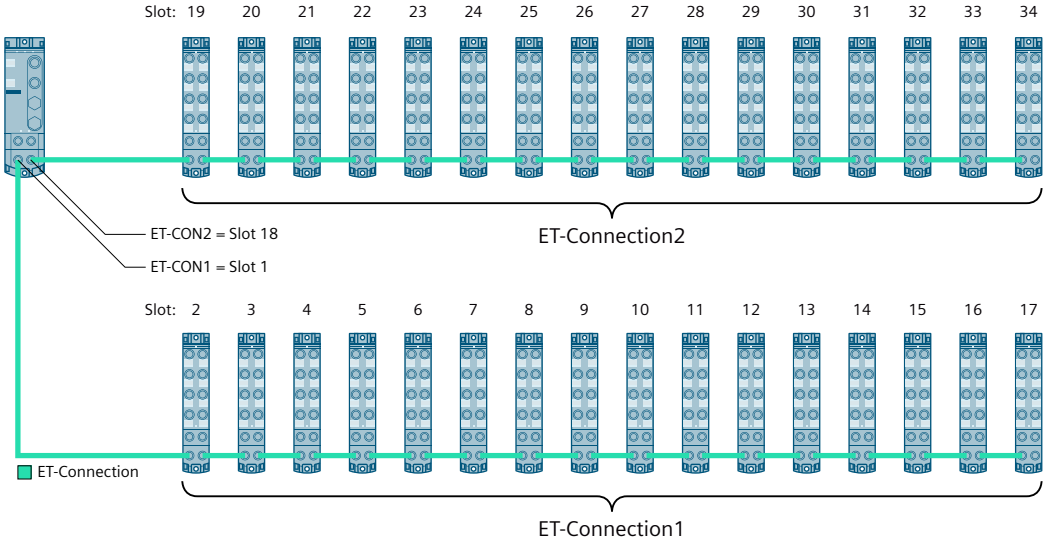


Figure 1-29 PROFIBUS maximum configuration

Reference

You can find additional information on this topic in section Configuration control (option handling) (Page 76).

8.4 Assigning the PROFIsafe addresses

The F-destination address is permanently stored in the eCoding plug connector of the fail-safe ET 200AL I/O modules.

NOTE

When assigning the PROFIsafe addresses, the F-modules must be supplied with voltage 1L+.

NOTE

Follow these points in conjunction with the configuration control:
Before you can use the configuration control together with F-modules, the PROFIsafe addresses must be assigned to the F-modules in the designated slots.
For this, each F-module must be plugged into the slot configured for it. The actual configuration may differ from the set configuration.

You can find additional information about the assignment of the PROFIsafe addresses in the manual SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126).

Reference

You can find additional information on this topic in section Configuration control (option handling) (Page 76).

Configuration control (option handling) 9

9.1 Configuration control

Introduction

With configuration control (option handling), you handle various standard machine configuration levels in one project without having to change the hardware configuration or user program.

Operating principle of configuration control

You can use configuration control to operate different standard machine configurations with a single configuration of the ET 200AL distributed I/O system.

- A station master (maximum configuration) is configured in a project. The station master comprises all modules needed for all possible equipment components of a modular standard machine.
- Provision is made in the user program of the project for various station options for the different configuration levels of the standard machine and for selection of a station option. A station option uses, for example, only some of the modules of the station master and these modules are not inserted in the configured order.
- Manufacturers of standard machines select a station option for a configuration level of the standard machine. They do not have change the project or download the modified configuration.

You use a control data record you have programmed to notify the CPU/interface module as to which modules are missing or located on different slots in a station option as compared to the station master. If a module with the configuration control is moved to another slot, it retains its parameter assignment.

The configuration control allows you to flexibly vary the centralized/distributed configuration. As a precondition for this, the station option must be able to be derived from the station master.

The following figure shows 3 configurations of a standard machine with the corresponding station options of the ET 200AL distributed I/O system.

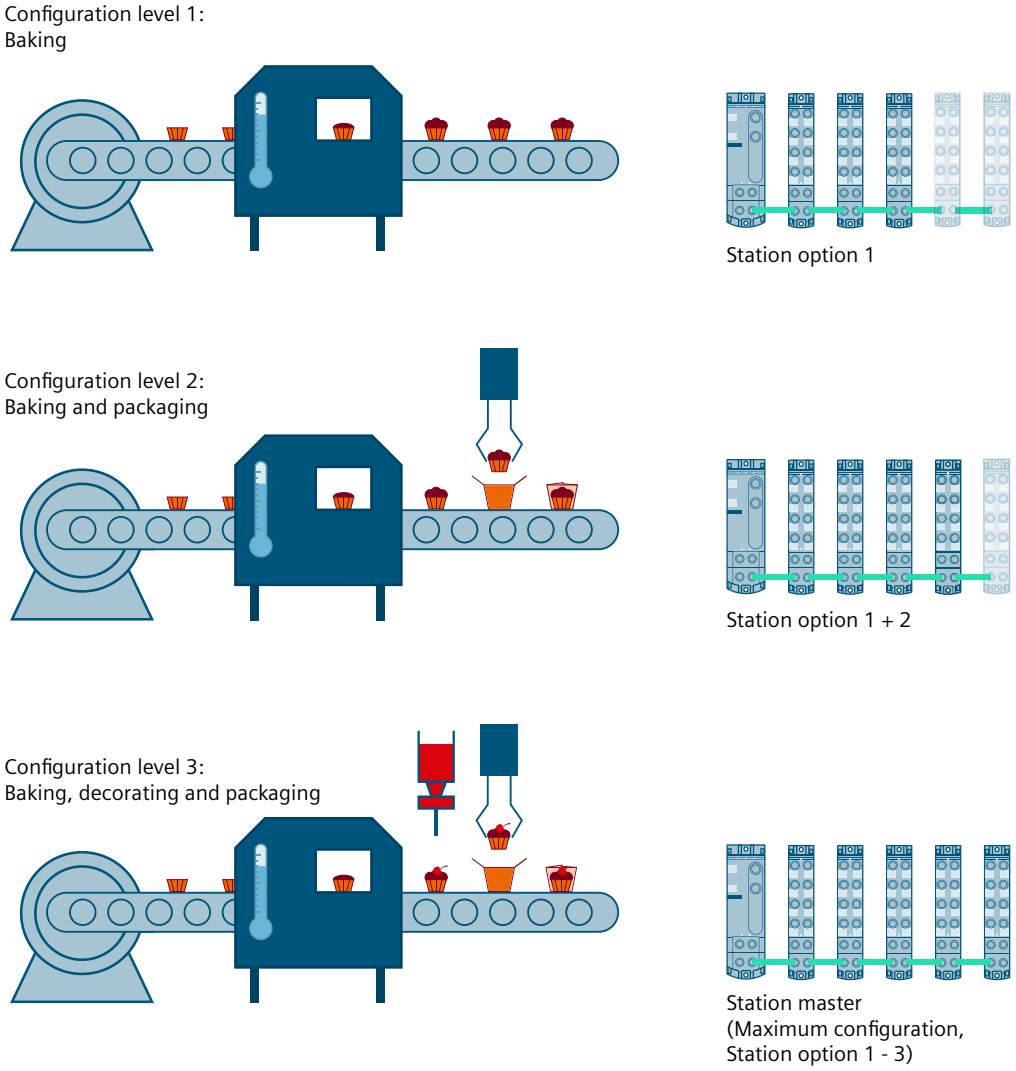


Figure 1-30 Various configuration levels of a standard machine with the corresponding station options of the ET 200AL distributed I/O system.

Benefits

- Easy project handling and commissioning through use of a single STEP 7 project for all station options.
- Easy handling during maintenance, versioning and upgrades.
- Hardware savings: Only the I/O modules needed for the current station option of the machine are installed.
- Potential savings when building, commissioning and creating documentation for standard machines.

Procedure

To set up the configuration control, follow these steps in the order given:

Step	Procedure	See...
1	Enable configuration control in STEP 7	Section Configuring (Page 78)
2	Create control data record	Section Creating the control data record (Page 80)
3	Transfer control data record	Section Transferring the control data record in the user program of the CPU (Page 88)

Library for configuration control

A library for configuration control is available for download (https://support.industry.siemens.com/cs/ww/en/view/29430270) on the internet. The library contains data types with the structure of the control data records for the ET 200AL distributed I/O system. You can implement your flexible automation solution economically with the help of these data types.

9.2 Configuring

Requirements

Via PROFINET IO:

- Configuration software, for example STEP 7 Professional as of V13
- IM 157-1 PN or IM 157-1 MF
- You have assigned the interface module to an IO controller in STEP 7

Via PROFIBUS DP:

- Configuration software, for example STEP 7 Professional as of V13
- IM 157-1 DP
- You have assigned the interface module to a DP master in STEP 7

- The parameter "Operation if preset configuration does not match actual configuration" is activated.
  The parameter "Operation if preset configuration does not match actual configuration" is located in STEP 7 in the properties of the interface module under "Module parameters" > "Start-up".

NOTE

Disabled parameter "Startup if preset configuration does not match actual configuration"
If an I/O module is missing or an incorrect or additional I/O module is plugged in and the "Startup if preset configuration does not match actual configuration" parameter is disabled, the ET 200AL distributed I/O system does not start up.
The diagnostic "Slot x no module" or "Slot x wrong module" is generated.
If the IM 157-1 DP interface module does not start up in this status, the RUN and ERROR LEDs on the interface module flash red. The DIAG LEDs flash green on all I/O modules as well.

NOTE

Follow these points in conjunction with the configuration control:
Before you can use the configuration control together with F-modules, the PROFIsafe addresses must be assigned to the F-modules in the designated slots.
For this, each F-module must be plugged into the slot configured for it. The actual configuration may differ from the set configuration.

Required steps

Enable the "Allow to reconfigure the device via the user program" parameter when configuring the interface module.

- The parameter "Enable reconfiguration of device via user program" is located in the properties of the interface module under "Module parameters" > "Configuration control".

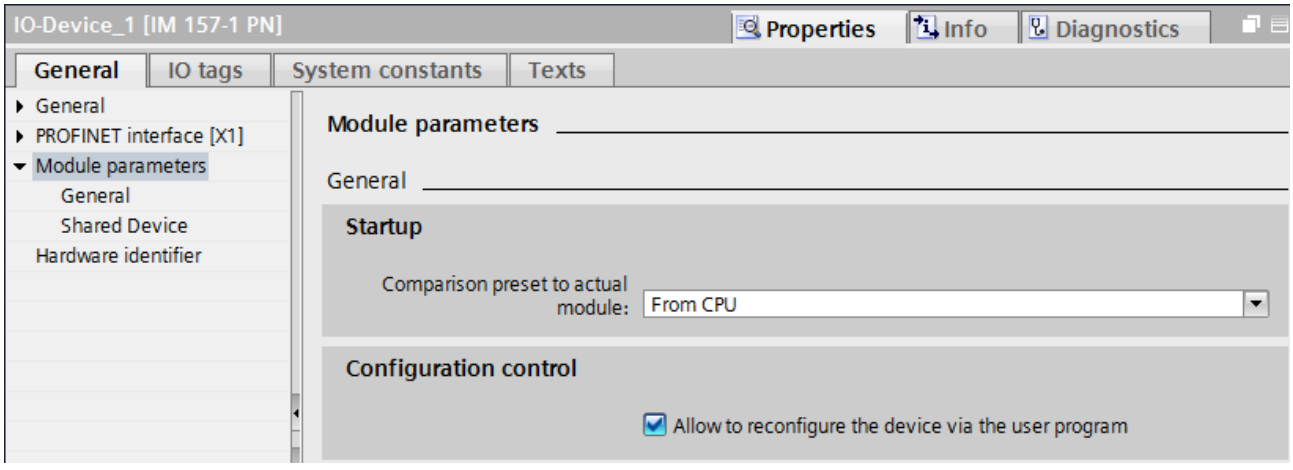


Figure 1-31 Enabling configuration control using the IM 157-1 PN as an example

9.3 Creating the control data record

9.3.1 Introduction

Required steps

The following description shows as an example how you can create a control data record for the configuration control in STEP 7 (TIA Portal).

To create a control data record for the configuration control, follow these steps:

1. Create a PLC data type that contains the structure of the control data record for an ET 200AL interface module.

   You can find the structure of the control data record in section Control data record for the ET 200AL distributed I/O system (Page 82)

CTR_REC

	Name	Data type	Default value	A...	W...	V..	S...	Comment
1	Block_Lenght	USInt	76	☑	☑	☑	☐	
2	Block_ID	USInt	196	☑	☑	☑	☐	
3	Version	USInt	2	☑	☑	☑	☐	
4	Subversion	USInt	1	☑	☑	☑	☐	
5	ET-Connection1	Struct		☑	☑	☑	☐	ET-Connection1 slots 2-17
6	Topology module	USInt	1	☑	☑	☑	☐	ET-Connection1 topology module
7	Reserved 1	USInt	0	☑	☑	☑	☐	
8	Slot 2	USInt	2	☑	☑	☑	☐	assigned "real" slot
9	Reserved 2	USInt	0	☑	☑	☑	☐	
10	Slot 3	USInt	3	☑	☑	☑	☐	assigned "real" slot
11	Reserved 3	USInt	0	☑	☑	☑	☐	
12	Slot 4	USInt	4	☑	☑	☑	☐	assigned "real" slot
13	Reserved 4	USInt	0	☑	☑	☑	☐	
14	Slot 5	USInt	5	☑	☑	☑	☐	assigned "real" slot
15	Reserved 5	USInt	0	☑	☑	☑	☐	
		USInt	6	☑	☑	☑	☐	assigned "real" slot

Figure 1-32 Creating control data record 196

2. Create a global data block.
3. Create an array of the data type of the above created PLC data type in the data block.

   The following figure shows a data block containing the control data records for an ET200AL interface module. In this example the data block contains three control data records.

ConfDB

	Name	Data type	Start value	R..	A...	V..	S...	Comment
1	Static			☐	☐	☐	☐	
2	Option	Int	0	☑	☑	☑	☐	Selection of record
3	ConfigControl	Array[0..2] of "CTR_REC"		☐	☑	☑	☐	
4	ConfigControl[0]	"CTR_REC"		☐	☑	☑	☐	
5	ConfigControl[1]	"CTR_REC"		☐	☑	☑	☐	
6	Block_Lenght	USInt	36	☐	☑	☑	☐	4+number of slots

Figure 1-33 Data block for configuration control

4. In the "Start value" column of the control data records, enter which module is located at which slot.

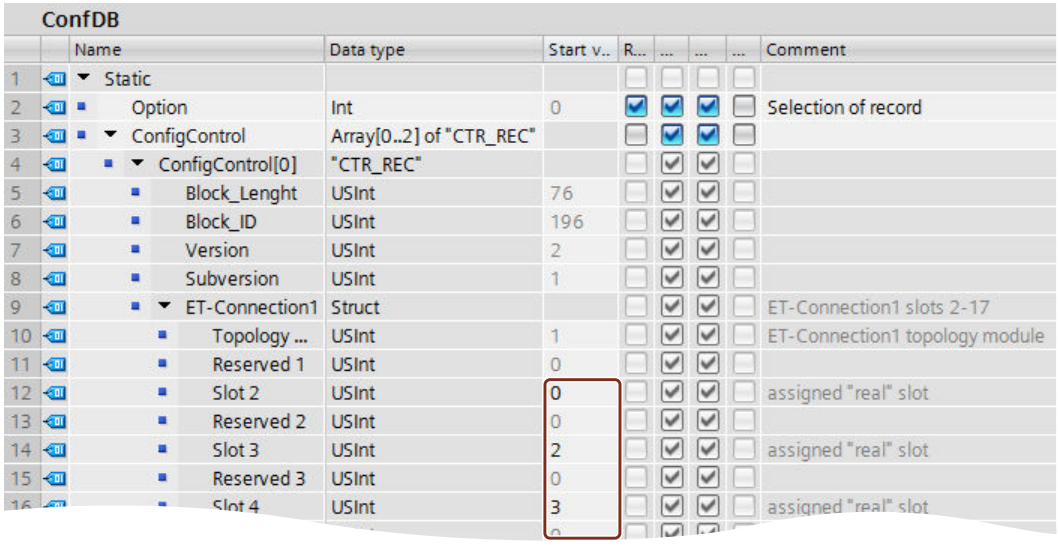


Figure 1-34 Assigning slots

Rules

Observe the following rules:

- Slot entries in the control data record outside the station master are ignored by the interface module.
- The control data record must contain the entries up to the last slot of the station option.
- Each slot of a station option may only be present once in the control data record.
- Each slot of a station option may only be assigned to one slot in the station master.
- The interface module (slot 0) is not an element of the configuration control, but instead controls this.
- The topology modules always have to exist in the data record:
  - The topology module ET-Connection 1 is always located on Slot 1.
  - The topology module ET-Connection 2 is always located on Slot 18.

9.3.2 Control data record for the ET 200AL distributed I/O system

Slot assignment

NOTE

Topology modules ET-Connetion1 and ET-Connection2
Both topology modules ET-Connection1 and ET-Connection2 should be treated like real modules during configuration control.
Restriction: ET-Connetion1 is always placed in Slot 1 and ET-Connection2 is always placed in Plot 18.

The following table shows the possible slots for the various modules for an ET 200AL interface module:

Table 1-10 Slot assignment

Modules	Possible slots	Comment
Topology ET-Connection1	1	The topology module ET-Connection 1 is always located on Slot 1.
I/O modules ET-Connection1	2-17	-
Topology module ET-Connection2	18	The topology module ET-Connection2 is always located on Slot 18.
I/O modules ET-Connection2	19-34	-

Control data record

For configuration control of the ET 200AL distributed I/O system, you define a control data record 196 V2.1, which contains a slot assignment for the modules. The table below shows the structure of a control data record with explanations of the individual elements.

Table 1-11 Configuration control: Structure of control data record 196

Byte	Element	Code	Explanation
0	Block length	4 + (number of slots x 2)	Header
1	Block ID	196	
2	Version	2	
3	Subversion	1	

Byte	Element	Code	Explanation
4	Slot topology module ET-Connection1	1 The topology module ET-Connection 1 is always located on Slot 1.	**Control element** Contains information on which module is inserted in which slot. The following rule determines which value you must enter in the respective byte: • If the module is included in the station option, enter the slot number of the module. • If the module does not exist in the station option, enter 0.
5	Reserved		
6	Slot 2 of the station master	Slot assignment in the station option	
7	Reserved		
:	:	:	
38	Slot topology module ET-Connection2	18 The topology module ET-Connection2 is always located on Slot 18	
39	Reserved		
40	Slot 19 of the station master	Slot assignment in the station option	
41	Reserved		
:	:	:	
4 + ((max. slot - 1) x 2))	Maximum slot of the station master	Slot assignment in the station option	
5 + ((max. slot - 1) x 2))	Reserved		

Combination of configuration control and shared device (for PROFINET)

The configuration control function in a shared device is therefore only for the I/O modules of the IO controller to which the interface module has subscribed. I/O modules that are assigned to no controller or a different controller behave like a station without activated configuration control.

In the control data record change the slots only for those modules that are assigned to the IO-Controller.

In the control data record do not move modules to slots that are assigned to a different IO controller or no IO controller. The interface module does not check whether a control data record 196 exists for these slots. The interface module assumes a 1-to-1 assignment for these slots.

Combination of configuration control and PROFIenergy (at PROFINET)

You can use configuration control together with PROFIenergy for the ET 200AL distributed I/O system.

Ensure that you use the slots of the used station option when creating Data record 3. Do not use the slots configured in the station master.

Example: You want to set up PROFIenergy for a DQ module of an IM 157-1 PN that works with configuration control. You have configured the DQ module to Slot 5 in the station master. You have moved the DQ module to Slot 2 in the station option. In order to set up PROFIenergy for this module use Slot 2 in Data record 3.

You can find more information about PROFIenergy in the Interface module IM 157-1 PN (https://support.industry.siemens.com/cs/ww/en/view/89254863) Equipment Manual.

9.3.3 Feedback data record at the ET200AL distributed I/O system

Operating principle

The feedback data record informs you about the accuracy of the module assignment and gives you the option of detecting assignment errors in the control data record. The feedback data record is mapped via a separate data record 197 V2.0.

Feedback data record

The feedback data record exists only when configuration control is configured and always refers to the maximum configuration limits **without interface module**, i.e., 34 slots. Partial reading of the feedback data record is possible.

Table 1-12 Feedback data record

Byte	Element	Code	Explanation
0	Block length	66	Header
1	Block ID	197	
2	Version	2	
3		0	
4	Slot 1 status	0/1	Status = 1: • Module from station master is inserted in the station option • Slot is marked as not available in the control data record Status = 0: • Module pulled • Incorrect module inserted in the station option*
5	Reserved	0	
6	Status slot 2	0/1	
7	Reserved	0	
:	:	:	
70	Status Slot 34	0/1	
71	Reserved	0	

* Not possible if the slot is marked as not available.

NOTE

The data in the feedback data record is always mapped for all modules. In a Shared Device configuration, it is therefore irrelevant which IO controller the respective modules are assigned to.

As long as no control data record was sent, a one-to-one module assignment is assumed for the compilation of data record 197 (station master → station option).

Error messages

In the case of an error when reading the feedback data record, the RDREC instruction returns the following error messages via the STATUS block parameter:

Table 1-13 Error messages

Error code	Meaning
$80B1_H$	Invalid length; the length information in data record 197 is not correct.
$80B5_H$	Configuration control not configured

Error code	Meaning
$80B8_H$	Parameter error The following events cause a parameter error: • Incorrect block ID in the header (not equal to 197) • Invalid version identifier in the header • A reserved bit was set • Multiple slots in the station master are assigned to the same slot in the station option

9.3.4 Example of a configuration control

Introduction

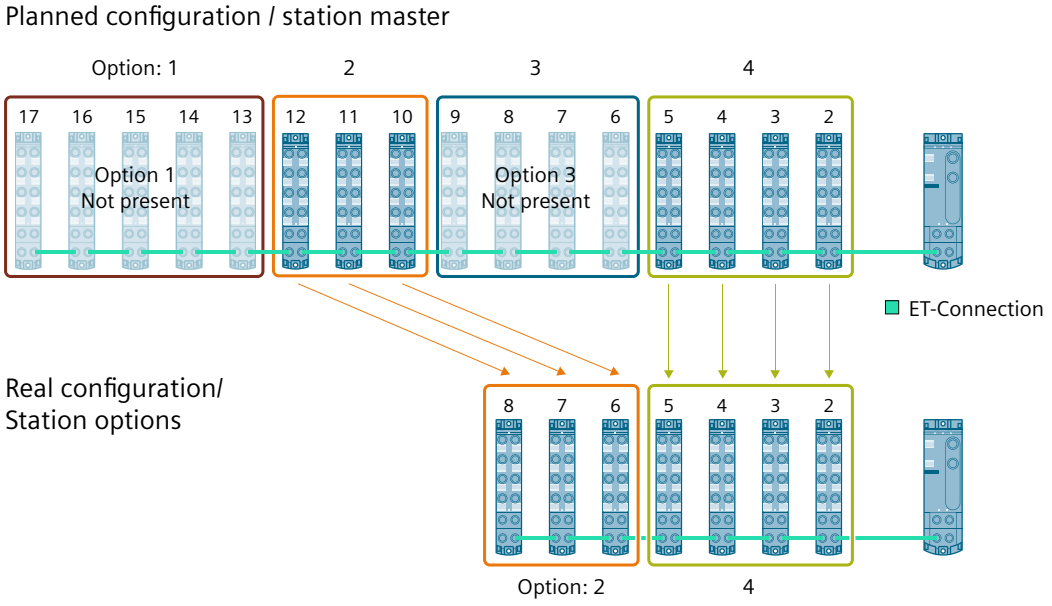
Several options/functional variations often exist for machines designed as series products. Or you have a plant that can operate in different modes.
Combine the modules that are needed for a function. With configuration control (option handling), you have the option to switch these functions on and off or expand their configuration.

The following examples show how you can form the control data record for a station option. The station master consists of an interface module IM 157-1 PN and 15 I/O modules in this case.

Station option with associated control data record

The configuration with the station options 2 and 4 differ from the station master as follows:

- The modules for options 1 and 3 do not exist.

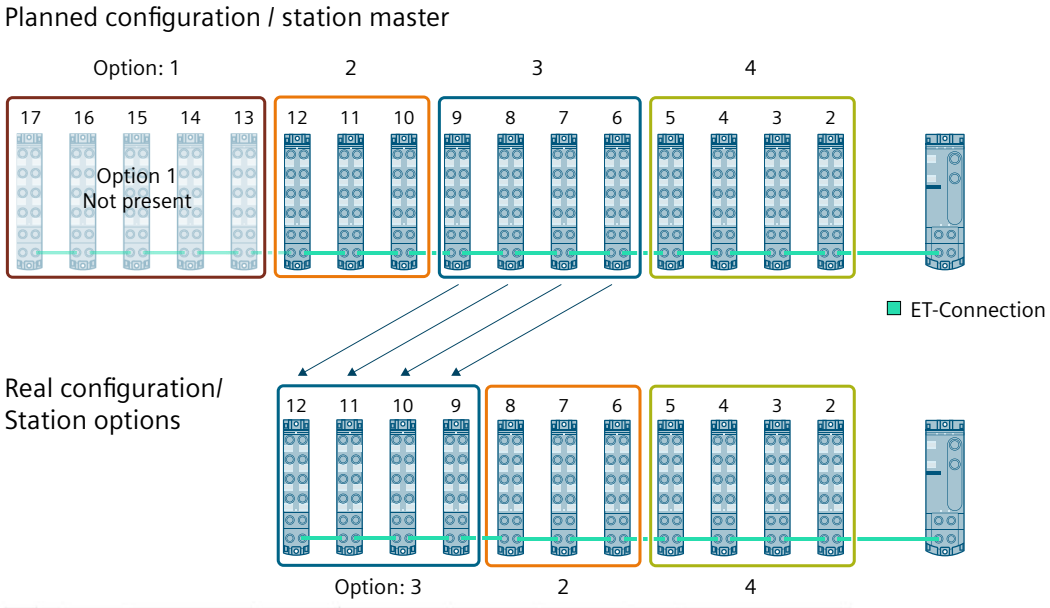


9		ET-Connection1	Struct		ET-Connection1 slots 2-17
10		Topology ...	USInt	1	ET-Connection1 topology module
11		Reserved 1	USInt	0	
12		Slot 2	USInt	2	assigned "real" slot
13		Reserved 2	USInt	0	
14		Slot 3	USInt	3	assigned "real" slot
15		Reserved 3	USInt	0	
16		Slot 4	USInt	4	assigned "real" slot
17		Reserved 4	USInt	0	
18		Slot 5	USInt	5	assigned "real" slot
19		Reserved 5	USInt	0	
20		Slot 6	USInt	0	assigned "real" slot
21		Reserved 6	USInt	0	
22		Slot 7	USInt	0	assigned "real" slot
23		Reserved 7	USInt	0	
24		Slot 8	USInt	0	assigned "real" slot
25		Reserved 8	USInt	0	
26		Slot 9	USInt	0	assigned "real" slot
27		Reserved 9	USInt	0	
28		Slot 10	USInt	6	assigned "real" slot
29		Reserved 10	USInt	0	
30		Slot 11	USInt	7	assigned "real" slot
31		Reserved 11	USInt	0	
32		Slot 12	USInt	8	assigned "real" slot
33		Reserved 12	USInt	0	
34		Slot 13	USInt	0	assigned "real" slot
35		Reserved 13	USInt	0	
36		Slot 14	USInt	0	assigned "real" slot
37		Reserved 14	USInt	0	
38		Slot 15	USInt	0	assigned "real" slot
39		Reserved 15	USInt	0	
40		Slot 16	USInt	0	assigned "real" slot
41		Reserved 16	USInt	0	
42		Slot 17	USInt	0	assigned "real" slot
43		Reserved 17	USInt	0	

Figure 1-35 Example: Hardware configuration of Station option 2 and 4 with the associated control data record in STEP 7

Extension by a station option

The following figure shows the configuration with the Station options 2 and 4 that has subsequently been extended by the Station option 3.
The modules of option 3 are added to the modules already existing.



10	ET-Connection1	Struct		ET-Connection1 slots 2-17
11	Topology module	USInt	1	ET-Connection1 topology module
12	Reserved 1	USInt	0	
13	Slot 2	USInt	2	assigned "real" slot
14	Reserved 2	USInt	0	
15	Slot 3	USInt	3	assigned "real" slot
16	Reserved 3	USInt	0	
17	Slot 4	USInt	4	assigned "real" slot
18	Reserved 4	USInt	0	
19	Slot 5	USInt	5	assigned "real" slot
20	Reserved 5	USInt	0	
21	Slot 6	USInt	9	assigned "real" slot
22	Reserved 6	USInt	0	
23	Slot 7	USInt	10	assigned "real" slot
24	Reserved 7	USInt	0	
25	Slot 8	USInt	11	assigned "real" slot
26	Reserved 8	USInt	0	
27	Slot 9	USInt	12	assigned "real" slot
28	Reserved 9	USInt	0	
29	Slot 10	USInt	6	assigned "real" slot
30	Reserved 10	USInt	0	
31	Slot 11	USInt	7	assigned "real" slot
32	Reserved 11	USInt	0	
33	Slot 12	USInt	8	assigned "real" slot
34	Reserved 12	USInt	0	
	Slot 13	USInt		assigned "real" slot

Figure 1-36 Example: Hardware configuration of station option 2 to 4 with the associated control data record in STEP 7

Detailed application example

You can find a detailed application example for the configuration control in S7-1500 in here under the keyword "Application example for ET 200SP (PROFINET) and S7-1500 based on the library" on the Internet (https://support.industry.siemens.com/cs/ww/en/view/29430270).

9.4 Transferring the control data record in the user program of the CPU

Required steps

Transfer the created control data record 196 to the interface module using the WRREC (Write data record) instruction.

Parameters of the WRREC instruction

Below, you will find explanations of individual parameters of the WRREC instruction which you must supply with specific values in the configuration control context. You can find additional information on the WRREC instruction in the STEP 7 online help.

ID	HW identifier of the interface module. If you have selected the interface module in the network view or device view, the HW identifier is available in the **System constants** tab of the Inspector window. Use the value of the system constant "<Name_of_interface_module> Head".
INDEX	Data record number: 196 (decimal)
RECORD	Control data record to be transferred. You can find the structure of the control data record in section Control data record for the ET 200AL distributed I/O system (Page 82).

Selection of the station option in the user program

In order for the CPU to know which station option you want to operate, you must set up a possibility to select between the various control data records in the user program. You can implement the selection, for example, via an Int tag that references an array element. Note that the tag used to select the control data record must be stored in the retentive memory area. If the tag is not retentive, it will be initialized during startup of the CPU and will thus be unavailable for selection of the station option.

Special requirements relating to the transfer of the control data record to the interface module

- If you have enabled configuration control, the ET 200AL station is not ready for operation without a control data record. As long as no valid control data record has been transferred, the I/O modules are considered as failed by the CPU and exhibit substitute value behavior. The interface module continues to exchange data.
- The control data record is stored retentively in the interface module. Note:
  - If the configuration is unchanged, you do not have to rewrite the control data record 196 during restart.
  - If you write a control data record with modified configuration, this will result in a station failure in the distributed I/O system. The original data record 196 is deleted and the new data record 196 is saved retentively. The station will then restart with the modified configuration.

Error messages

In case of error, the WRREC instruction returns the following error messages via the STATUS block parameter:

Table 1-14 Error messages

Error code	Meaning
$80B1_H$	Invalid length; the length information in data record 196 is not correct.
$80B2_H$	Invalid slot: The configured slot is not assigned
$80B5_H$	Configuration control parameters not assigned.
$80B8_H$	Parameter error Reasons for a parameter error are: • Incorrect block ID in the header (not equal to 196) • Invalid version identifier in the header • A reserved bit was set • A station master slot was assigned an invalid slot in the station option • Multiple slots in the station master are assigned to the same slot in the station option • For shared device on submodule level: violation of defined restrictions
$80C5_H$	DP slave or module not available. Indicates that a data record has not been acknowledged due to the system.

If you receive the error code $80A2_H$, $80B2_H$ or $80C5_H$ when writing to control data record 196, check whether the required configuration was accepted despite the error code.

9.5 Behavior during operation

Effect of discrepancy between station master and station option

For the online display and for the display in the diagnostics buffer (module OK or module faulty), the station master is always used and not the differing station option.

Example: A module outputs diagnostics data. This module is configured in slot 4 in the station master, but is inserted in slot 3 in the station option (missing module; see example in the next section). The online view (station master) shows an incorrect module in slot 4. In the real configuration, the module in slot 3 indicates an error via an LED display.

Response to modules that are not present

If modules are entered as not present in the control data record, the automation system behaves as follows:

- Modules designated as not present in the control data record do not supply diagnostics and their status is always OK. The value status is OK.
- Direct writing access to the outputs that are not present or writing access to the process image of outputs that are not present: Remains without effect; no access error is signaled.
- Direct reading access to the inputs that are not present or reading access to the process image of inputs that are not present: Value "0" is supplied; no access error is signaled.
- Write data record to module that is not present: Remains without effect; no error is signaled.
- Read data record from module that is not present: The output parameter STATUS of the instruction RDREC supplies the value $80A3_H$ "General CM error".

Commissioning

10

10.1 PROFINET IO

10.1.1 Commissioning ET 200AL on PROFINET IO

Introduction

The commissioning of your distributed I/O system depends on the system configuration. The following procedure describes the commissioning of the ET 200AL distributed I/O system on an IO controller.

Requirements for the ET 200AL distributed I/O system on PROFINET IO

NOTE

Performing tests

You must ensure the safety of your plant. You therefore need to perform a complete functional test and the necessary safety checks before the final commissioning of a plant. Also plan the tests to include any possible foreseeable errors. This will allow you to prevent people or plants from being placed in danger during operation.

Procedure

The following table shows the chapters/documents in which the required actions are described.

Table 1-15 Requirements for the ET 200AL distributed I/O system on PROFINET IO

Step	Procedure	See...
1	Mounting the ET 200AL interface module	Section Mounting (Page 36)
2	Wiring the ET 200AL interface module	Section Connecting (Page 41)
3	Configuring the ET 200AL interface module	Section Configuring (Page 69)
4	Turning on the supply voltage for the ET 200AL interface module	Equipment Manual • IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) • IM 157-1 MF interface module (https://support.industry.siemens.com/cs/ww/en/view/109824723)
5	ET 200AL interface module automatically switches to RUN mode	-

Reference

You can find additional information on assigning the PROFINET IO parameters in the PROFINET with STEP 7 V14 (https://support.industry.siemens.com/cs/ww/en/view/49948856) function manual.

10.1.2 Startup on PROFINET IO

Principle of operation

The figure below schematically shows the startup of the ET 200AL distributed I/O system on the PROFINET IO (= IO device) as a flow chart.

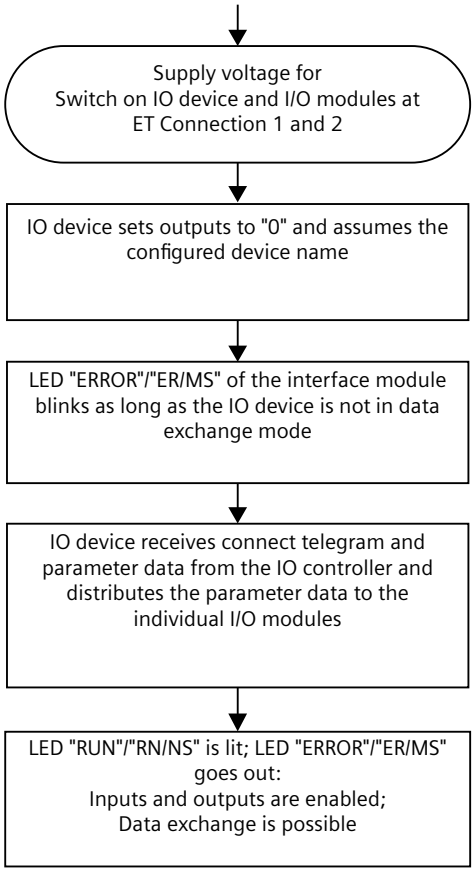


Figure 1-37 Startup of the ET 200AL distributed I/O system on the PROFINET IO

The figure below schematically shows the startup of an ET 200AL I/O module after an ET 200AL PROFINET interface module.

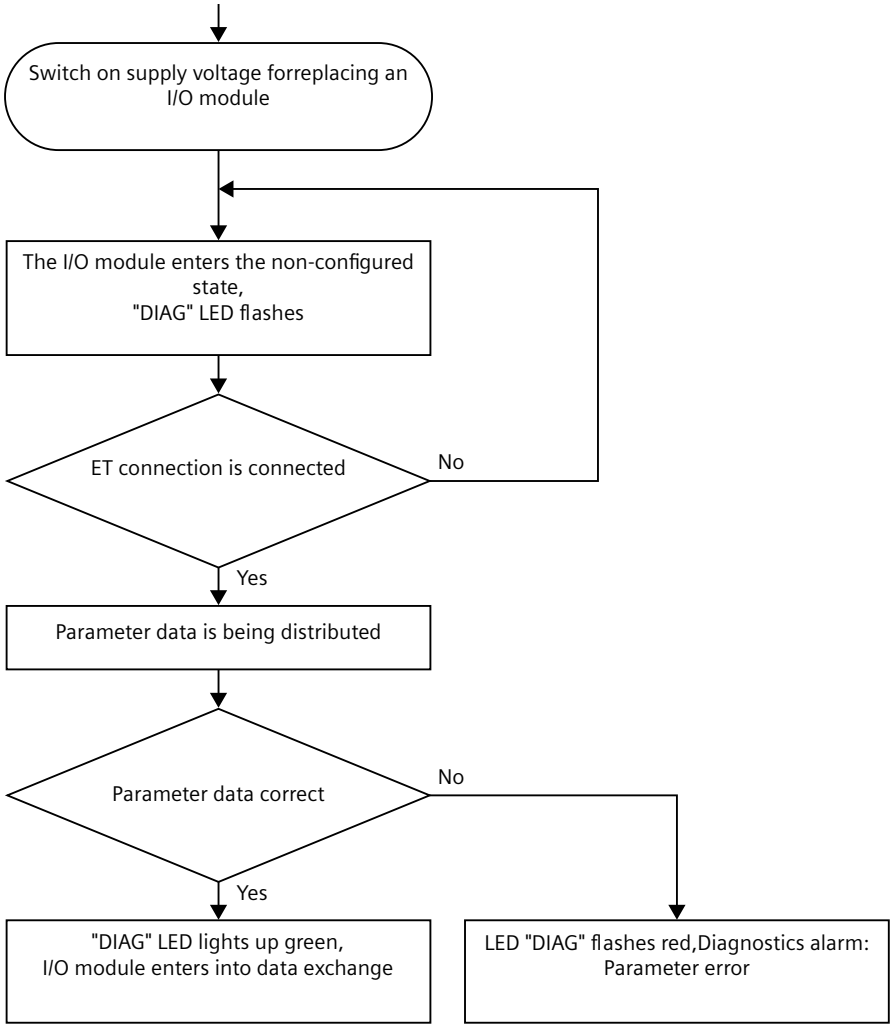


Figure 1-38 Startup of the ET 200AL I/O module

10.1.3 PROFIenergy

NOTE

PROFIenergy is not supported by fail-safe I/O module F-DI 4+F-DQ 2x24VDC/2A, 4xM12.

PROFIenergy (for PROFINET) makes it possible to reduce the energy consumption of the device using the PROFIenergy command during production downtime.

Additional information

You will find more information on the Internet (https://www.profibus.com) under Common Application Profile PROFIenergy; Technical Specification for PROFINET; as well as in the following documentation:

- IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) manual
- I/O modules (https://support.industry.siemens.com/cs/ww/en/ps/14247/man) manuals
- PROFINET System Description (https://support.industry.siemens.com/cs/ww/en/view/19292127) system manual
- PROFINET with STEP 7 V14 (https://support.industry.siemens.com/cs/ww/en/view/49948856), function manual, Section: Saving energy with PROFIenergy
- Application guide for implementation of shutdown concepts with PROFIenergy. (https://support.industry.siemens.com/cs/ww/en/view/96837137)
- Saving energy with SIMATIC S7 (STEP 7 as of V5.5) (https://support.industry.siemens.com/cs/ww/en/view/41986454)
- Saving energy with SIMATIC S7 and SIMATIC HMI (TIA Portal) (https://support.industry.siemens.com/cs/ww/en/view/58235225)
- SIMATIC S7 library for simple configuration of PROFIenergy. (https://support.industry.siemens.com/cs/ww/en/view/109478388)
- You can find additional information on the PROFIenergy FBs ("PE_START_END" - FB 815, "PE_CMD" - FB 816) in the online help for STEP 7 V5.5 as of SP2, Help on system functions/function blocks.

10.2 EtherNet/IP

10.2.1 Commissioning the ET 200AL on EtherNet/IP

Introduction

The commissioning of your distributed I/O system depends on the system configuration. The following procedure describes the commissioning of the ET 200AL distributed I/O system on an scanner.

Requirements for the ET 200AL distributed I/O system on EtherNet/IP

NOTE

Performing tests

You must ensure the safety of your plant. You therefore need to perform a complete functional test and the necessary safety checks before the final commissioning of a plant. Also plan the tests to include any possible foreseeable errors. This will allow you to prevent people or plants from being placed in danger during operation.

Procedure

The following table shows the chapters/documents in which the required actions are described.

Table 1-16 Requirements for the ET 200AL distributed I/O system on EtherNet/IP

Step	Procedure	See...
1	Mounting the ET 200AL interface module	Section Mounting (Page 36)
2	Wiring the ET 200AL interface module	Section Connecting (Page 41)
3	Configuring the ET 200AL interface module	Section Configuring (Page 69)
4	Turning on the supply voltage for the ET 200AL interface module	Equipment manual IM 157-1 MF interface module (https://support.industry.siemens.com/cs/ww/en/view/109824723)
5	ET 200AL interface module automatically switches to RUN mode	-

Reference

You can find additional information about the configuration of EtherNet/IP parameters in the MultiFieldbus function manual (https://support.industry.siemens.com/cs/ww/en/view/109773209).

10.2.2 Startup on EtherNet/IP

Principle of operation

The following figure shows a schematic flow chart of the startup of the ET 200AL distributed I/O system on EtherNet/IP. The interface module is in the network of the EtherNet/IP adapter and communicates with the scanner.

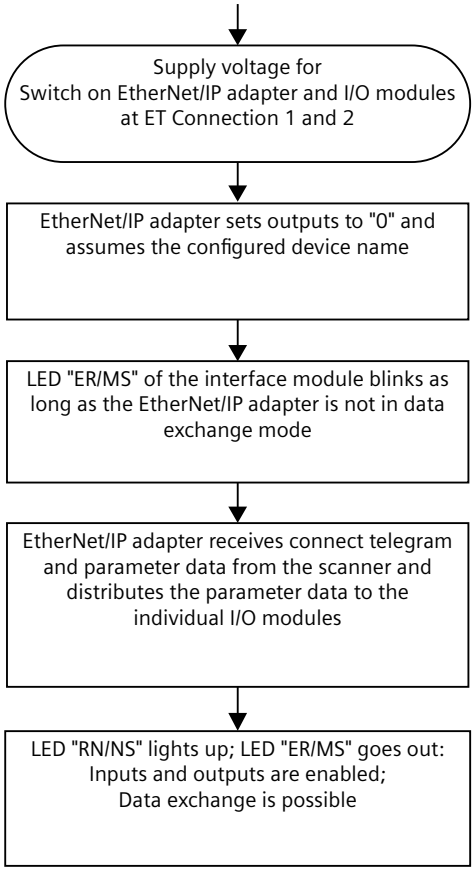


Figure 1-39 Startup of the ET 200AL distributed I/O system on EtherNet/IP

The figure below schematically shows the startup of an ET 200AL I/O module after an ET 200AL EtherNet/IP interface module as a flow chart.

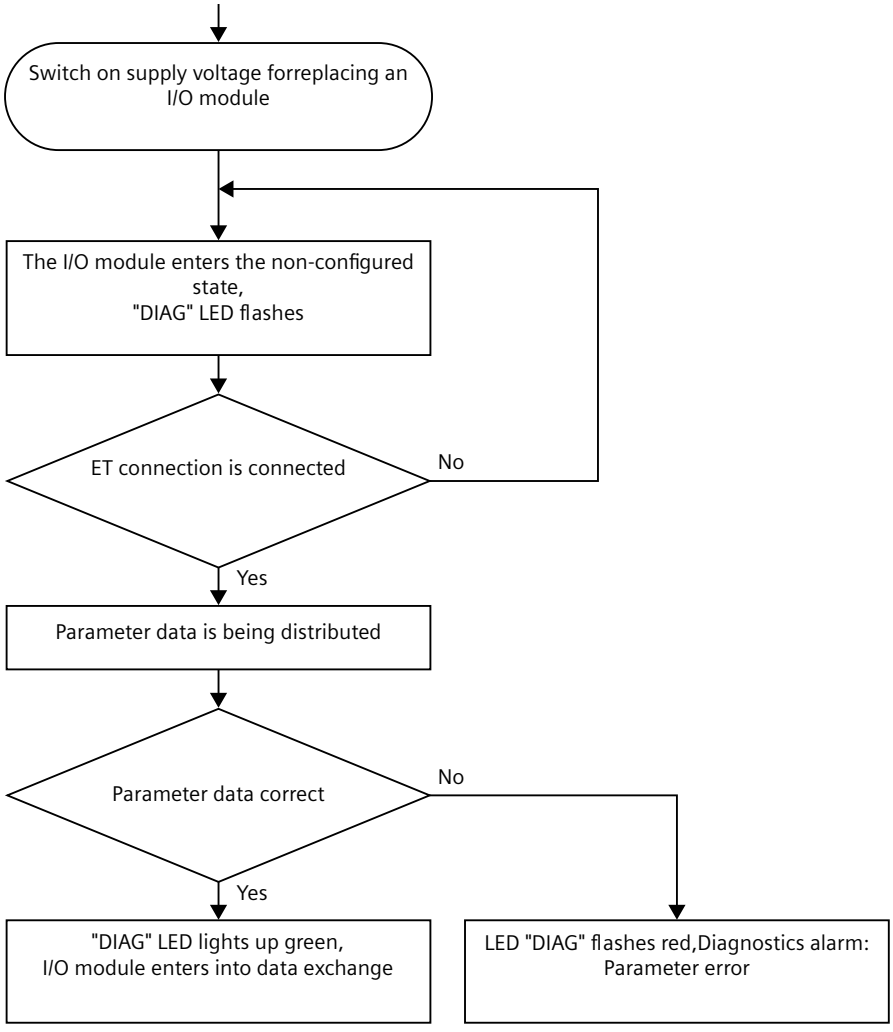


Figure 1-40 Startup of an ET 200AL I/O module

10.3 Modbus TCP

10.3.1 Commissioning the ET 200AL on Modbus TCP

Introduction

The commissioning of your distributed I/O system depends on the system configuration. The following procedure describes the commissioning of the ET 200AL distributed I/O system on a Modbus client.

Requirements for the ET 200AL distributed I/O system on Modbus TCP

NOTE

Performing tests

You must ensure the safety of your plant. You therefore need to perform a complete functional test and the necessary safety checks before the final commissioning of a plant. Also plan the tests to include any possible foreseeable errors. This will allow you to prevent people or plants from being placed in danger during operation.

Procedure

The following table shows the chapters/documents in which the required actions are described.

Table 1-17 Requirements for the ET 200AL distributed I/O system on Modbus TCP

Step	Procedure	See...
1	Mounting the ET 200AL interface module	Section Mounting (Page 36)
2	Wiring the ET 200AL interface module	Section Connecting (Page 41)
3	Configuring the ET 200AL interface module	Section Configuring (Page 69)
4	Turning on the supply voltage for the ET 200AL interface module	Equipment manual IM 157-1 MF interface module (https://support.industry.siemens.com/cs/ww/en/view/109824723)
5	ET 200AL interface module automatically switches to RUN mode	-

Reference

You can find additional information about configuring the parameters of Modbus TCP in the MultiFieldbus function manual (https://support.industry.siemens.com/cs/ww/en/view/109773209).

10.3.2 Startup on Modbus TCP

Principle of operation

The following figure shows as flow chart schematically the start-up of the ET 200AL distributed I/O system on Modbus TCP. The interface module is the Modbus TCP server in the network and communicates with the client.

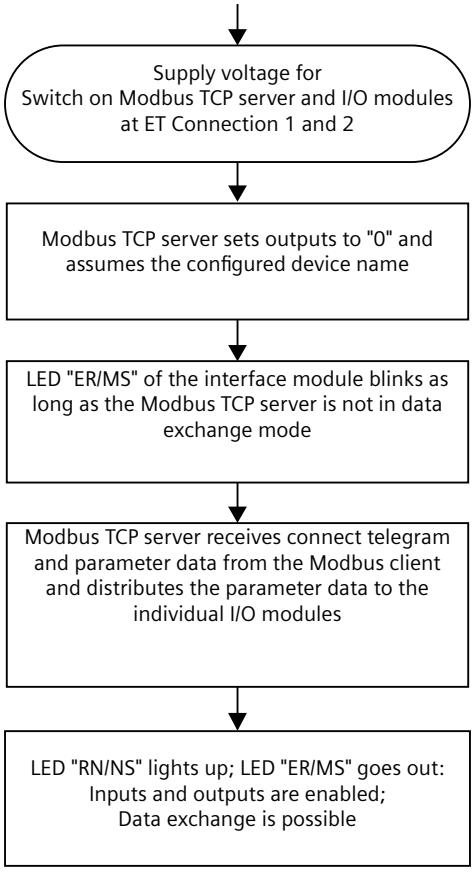


Figure 1-41 Startup of the ET 200AL distributed I/O system on Modubus TCP

The figure below schematically shows the startup of an ET 200AL I/O module after an ET 200AL Modubus TCP interface module as a flow chart.

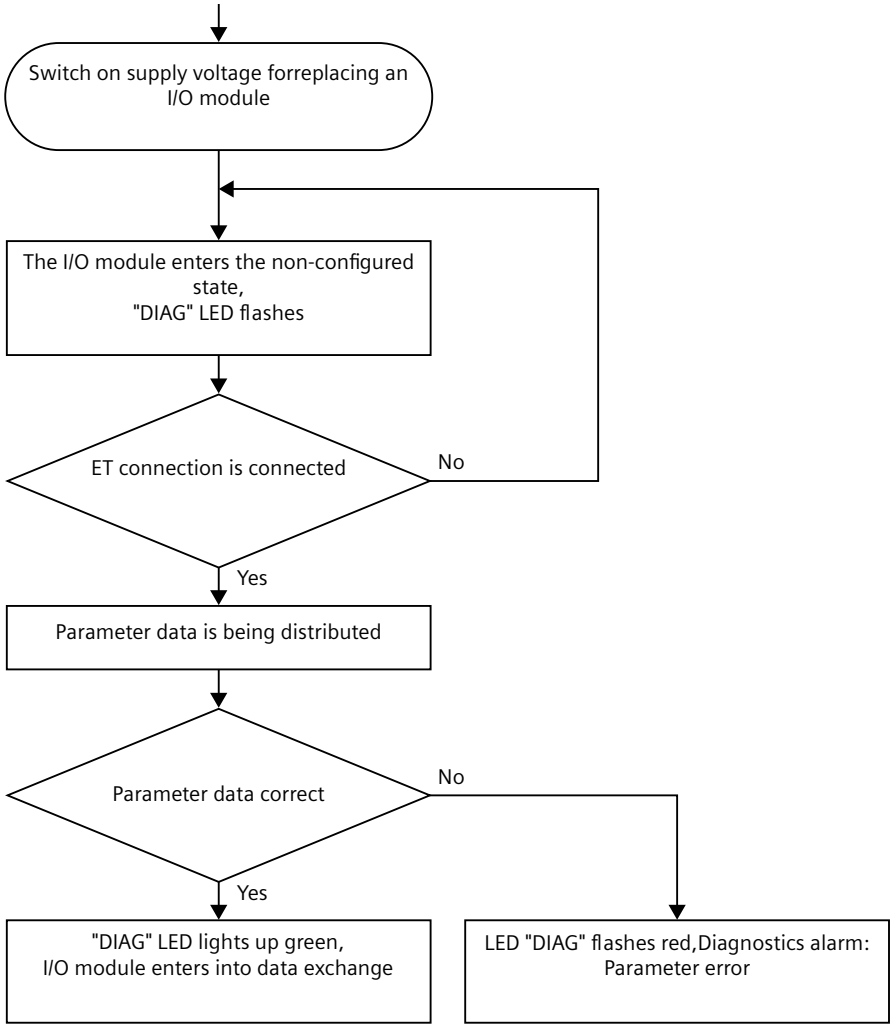


Figure 1-42 Startup of the ET 200AL I/O module

10.4 PROFIBUS DP

10.4.1 Commissioning ET 200AL on PROFIBUS DP

Introduction

The commissioning of your distributed I/O system depends on the system configuration. The following procedure describes the commissioning of the ET 200AL distributed I/O system on a DP master.

Requirements for the ET 200AL distributed I/O system on a PROFIBUS DP

NOTE

Performing tests

You must ensure the safety of your plant. You therefore need to perform a complete functional test and the necessary safety checks before the final commissioning of a plant. Also plan the tests to include any possible foreseeable errors. This helps to avoid endangering persons or equipment during operation.

Procedure

The following table shows the chapters/documents in which the required actions are described.

Table 1-18 Requirements for the ET 200AL distributed I/O system on a PROFIBUS DP

Step	Procedure	See...
1	Mounting the ET 200AL interface module	Section Mounting (Page 36)
2	Setting the PROFIBUS DP address on the ET 200AL PROFIBUS interface module	IM 157-1 DP interface module (https://support.industry.siemens.com/cs/ww/en/view/89255073) manual, section Setting the PROFIBUS DP address and terminating resistor
3	Wiring the ET 200AL interface module	Section Connecting (Page 41)
4	Configuring the ET 200AL interface module	Section Configuring (Page 69)
5	Switching on the supply voltage for the ET 200AL interface module	IM 157-1 DP interface module (https://support.industry.siemens.com/cs/ww/en/view/89255073) manual
6	ET 200AL interface module automatically switches to RUN mode	-

10.4.2 Startup on PROFIBUS DP

Principle of operation

The figure below schematically shows the startup of the ET 200AL distributed I/O system on the PROFIBUS DP (= DP slave) as a flow chart.

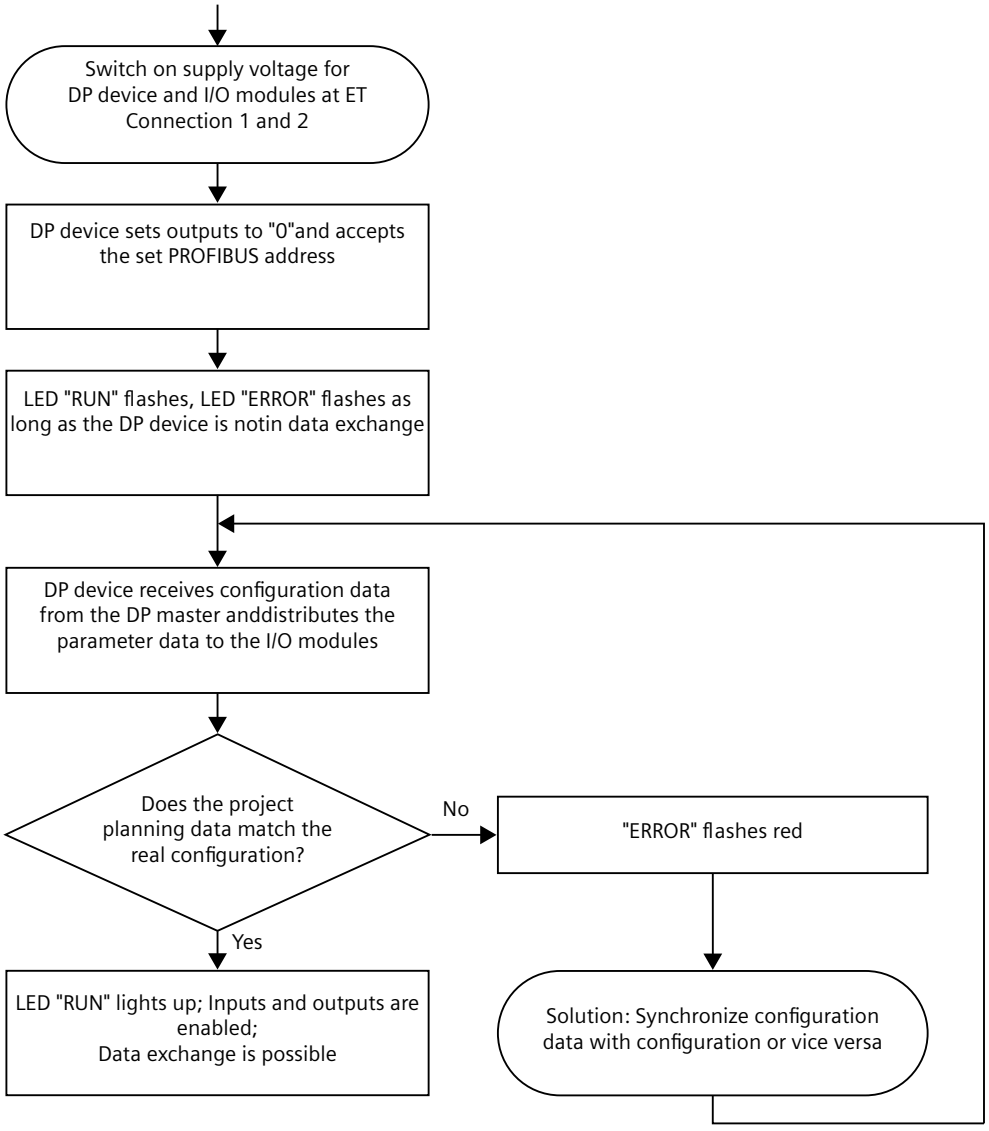


Figure 1-43 Startup of the ET 200AL distributed I/O system on PROFIBUS DP

The figure below schematically shows the startup of an ET 200AL I/O module after an ET 200AL PROFIBUS interface module as flow chart.

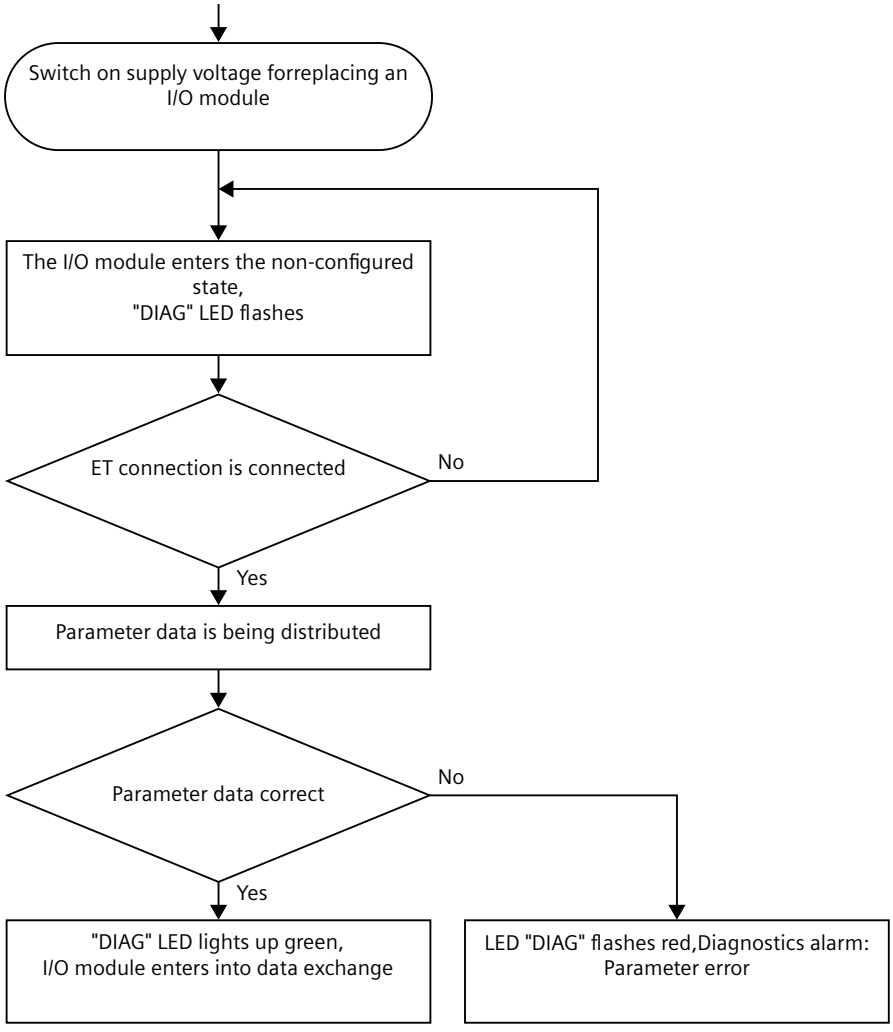


Figure 1-44 Startup of an ET 200AL I/O module

10.5 Identification and maintenance data

10.5.1 Reading out and entering I&M data

Introduction

Identification data I&M is information that is saved either as read-only (I data) or read/write (M data) on the interface module.

Identification data (I&M0): Manufacturer information on the module that is read-only and in some cases is also printed on the module housing, for example, article number, serial number and firmware version.

Maintenance data (I&M1, 2, 3): Plant-dependent information, e.g. installation location. Maintenance data is created during configuration and written to the module.

All modules of the ET 200AL distributed I/O system support identification data (I&M0 to I&M3).

The I&M identification data supports you in the following activities:

- Checking the plant configuration
- Locating hardware changes in a system
- Correcting errors in a system

With the I&M identification data, you have the option of clearly identifying modules online.

Maintenance data (I&M4): Storage of a CRC test value for interface modules IM 157-1 PN and IM 157-1 MF and to ensure data integrity of data used by the interface module.

In STEP 7, the identification data is displayed in the "Module status - IM 157" and "Properties..." tabs (see STEP 7 online help).

Options for reading out I&M data

You have the following options for reading the I&M data:

- Via the user program
- Via STEP 7 or HMI devices

Procedure for reading I&M data by means of the user program

To read the I&M data of the interface module in the user program, use the instruction "RDREC".

Procedure for reading the I&M data using STEP 7

Requirement: There must be an online connection to the interface module.

1. In the project navigation, under "Distributed I/O", select the I/O device or the DP slave, e.g. "IM 157-1 PN".
2. Select: **IO device/DP slave > Online & Diagnostics > Identification & Maintenance**.

Procedure for input of maintenance data using STEP 7

The default module name is assigned by STEP 7. You have the option to enter the following data:

- Plant designation (I&M1)
- Location identifier (I&M1)
- Installation date (I&M2)
- Additional information (I&M3)
- Signature (I&M4), only for PROFINET

To enter the data, follow these steps:

1. In the device view of the STEP 7 hardware network editor, select the interface module, for example.
2. In the properties under "General", select the "Identification & Maintenance" area and enter the data.

During the loading of the hardware configuration, the I&M data are also loaded.

Reference

You can find additional information on I&M data of the ET 200SP (mixed configuration) in the ET 200SP distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/58649293) system manual.

10.5.2 Data record structure for I&M data

Reading I&M data records (distributed via PROFINET IO)

You can directly access specific identification data by selecting **Read data record** ("RDREC" instruction). You obtain the corresponding part of the identification data under the associated data record index.

The following table shows the principle behind the structure of data records.

Table 1-19 Basic structure of data records with I&M identification data

Contents	Length (bytes)	Coding (hex)
Header information		
BlockType	2	I&M0: 0020_H I&M1: 0021_H I&M2: 0022_H I&M3: 0023_H I&M4: 0024_H
BlockLength	2	I&M0: 0038_H I&M1: 0038_H I&M2: 0012_H I&M3: 0038_H I&M4: 0038_H
BlockVersionHigh	1	01
BlockVersionLow	1	00
Identification data		
Identification data (see table below)	54 54 16 54 54	I&M0/Index $AFF0_H$ I&M1/Index $AFF1_H$ I&M2/Index $AFF2_H$ I&M3/Index $AFF3_H$ I&M4/Index $AFF4_H$

The following table shows the structure of data records for I&M identification data.

Table 1-20 Data record structure for I&M identification data

Identification data	Access	Default	Explanation
Identification data 0: (data record index AFF0 hex)			
VendorIDHigh	read (1 byte)	00_H	This is where the name of the manufacturer is stored (42_D = SIEMENS AG).
VendorIDLow	read (1 byte)	$2A_H$	
Order_ID	read (20 bytes)	6ES7157-1MA00-0AB0	Article number of module (e.g. IM 157-1 MF)
IM_SERIAL_NUMBER	read (16 bytes)	-	Serial number (device-specific)
IM_HARDWARE_REVISION	read (2 bytes)	1	Corresponding hardware version
IM_SOFTWARE_REVISION	read	Firmware version	Provides information about the firmware version of the module
• SWRevisionPrefix	(1 byte)	V	
• IM_SWRevision_Functional_Enhancement	(1 byte)	00 - FF_H	
• IM_SWRevision_Bug_Fix	(1 byte)	00 - FF_H	
• IM_SWRevision_Internal_Change	(1 byte)	00 - FF_H	
IM_REVISION_COUNTER	read (2 bytes)	0000_H	provides information about configured changes on the module (not used)
IM_PROFILE_ID	read (2 bytes)	0000_H	Generic device
IM_PROFILE_SPECIFIC_TYPE	read (2 bytes)	0005_H	Interface modules
IM_VERSION	read	0101_H	provides information about the version of the identification data (0101_H = Version 1.1)
• IM_Version_Major	(1 byte)		
• IM_Version_Minor	(1 byte)		
IM_SUPPORTED	read (2 bytes)	$001E_H$	provides information about the existing identification data (I&M1 though I&M4)
Maintenance data 1: (data record index AFF1 hex)			
IM_TAG_FUNCTION	Read/write (32 bytes)	-	Enter an identifier for the module here, that is unique plant-wide.
IM_TAG_LOCATION	Read/write (22 bytes)	-	Enter the installation location of the module here.
Maintenance data 2: (data record index AFF2 hex)			
IM_DATE	Read/write (16 bytes)	YYYY-MM-DD HH:MM	Enter the installation date of the module here.
Maintenance data 3: (data record index AFF3 hex)			
IM_DESCRIPTOR	Read/write (54 bytes)	-	Enter a comment describing the module.
Maintenance data 4: (data record index AFF4 hex)			
USI	Read (4 bytes)	0x63726331	UserstructureIdentifier: Internal, fixed value
CHK_OVERALL	Read (4 bytes)	-	Overall CRC via all individual CRCs
CHK_OVERALL_SUBS	Read (4 bytes)	0 or value*	Overall CRC via all assigned modules of the IM
CHK_STATIC_LOCAL	Read (4 bytes)	-	CRC via static data of the IM

* A value of 0 indicates that the IM firmware does not yet support the CRC calculation of the assigned modules.
If the value is ≠ 0, the IM supports this function, regardless of whether the associated modules support I&M4 data.

Identification data	Access	Default	Explanation
CHK_STATIC_SUBS	Read (4 bytes)	0 or value*	CRC via all static data of the modules of the IM
CHK_OVERALL_SETUP	Read (4 bytes)	-	Overall CRC via all setup data of the IM and modules of the IM
CHK_REMANENT_LOCAL	Read (4 bytes)	-	CRC via retentive data of the IM
CHK_REMANENT_SUBS	Read (4 bytes)	0 or value*	CRC via all retentive data of the modules of the IM
CHK_WORKING_LOCAL	Read (4 bytes)	-	CRC via the parameters in STEP 7 for the IM
CHK_WORKING_SUBS	Read (4 bytes)	0 or value*	CRC via all parameters in STEP 7 for the modules of the IM
NOT USED	Read (14 bytes)	0	14 reserved bytes

* A value of 0 indicates that the IM firmware does not yet support the CRC calculation of the assigned modules.
If the value is ≠ 0, the IM supports this function, regardless of whether the associated modules support I&M4 data.

Reading I&M data records with data record 255 (distributed via PROFIBUS DP)

The modules support standardized access to identification data using DR 255 (index 65000 to 65003). For additional information on the DR 255 data structure, refer to the specifications of the Profile Guideline - Order No. 3.502.

Maintenance 11

11.1 Replacing modules

Replacing modules

Replacing a module is not permitted during ongoing operation.

⚠ WARNING

Material damage can occur
If you remove/insert modules with the power connected, this can lead to undefined states in your system.
Material damage to the ET 200AL distributed I/O system may occur as a result.
Only remove or replace modules when the power is disconnected.
Always comply with the required standards and safety guidelines when configuring a system.

⚠ WARNING

Mixing up ET-Connection1 and ET-Connection2
When connecting the modules, always ensure that they are properly connected.
If you mix up the lines for ET-Connection1 and ET-Connection2 when connecting the modules, this can lead to undefined states in your system.

Behavior of ET-Connection

During ongoing operation, a module replacement may be necessary, e.g. because the module is defective. If an I/O module fails in an ET-Connection line, the line remains active up to the failed I/O module. After replacing the I/O module, the ET-Connection line starts up by itself.

Procedure

To replace a module, proceed as follows:

1. Disconnect the supply voltage to the module to be replaced.
2. Completely remove all cables connected to the module.
3. Completely remove the fixing screws of the module

4. Replace the module.

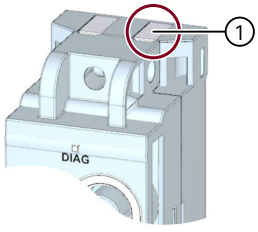
NOTE
"New" module
The removed module may only be replaced by a module of the same type.

5. Fasten the module with a torque of 1.2 Nm.
6. Connect all cables.
7. Turn the supply voltage on.

⚠ WARNING

Pay attention to the slot number of the module
If you mix up the ET 200AL I/O modules when connecting them, this can cause personal injury and damage to the machine.
The ET 200AL distributed I/O system cannot distinguish between modules of the same type during the actual/target comparison.
We recommend that you clearly label the ET 200AL I/O modules with the slot number.

The figure below shows a recommendation for labeling the ET 200AL I/O modules with the slot number.



① Recommendation for labeling the slot number

Figure 1-45 Slot number

Result

The disconnected I/O module and all downstream I/O modules start up again by themselves.

11.2 Firmware update

Introduction

During operation, it can become necessary to update the firmware (e.g. for function extensions).

Firmware updates are used to update the firmware of the interface module and I/O modules.

NOTE

Temporary bus interruption

When you perform a firmware update of an ET 200AL I/O module, then the ET-Connection is temporarily interrupted due to the restart of I/O module. All downstream ET 200AL I/O modules report a pull/plug interrupt.

Options for the firmware update

You have the following options to running a firmware update:

- Online via STEP 7, as of V5.5[1]
- Online with STEP 7, TIA Portal V13 or higher
- Embedded web server running on a SIMATIC CPU[1] or a SIMATIC F-CPU with fail-safe modules
- SIMATIC Automation Tool (SAT)
- Online via MultiFieldbus Configuration Tool (MFCT)

[1)] Not for use with fail-safe ET 200AL I/O modules

NOTE

MultiFieldbus interface module remains in configured fieldbus mode

After a firmware update, the MultiFieldbus interface module remains in the bus protocol in which the update was installed.

If there is an update via EtherNet/IP, for example, the MultiFieldbus interface module remains in EtherNet/IP mode.

Reference

More information about the procedure:

- FAQs on the Internet (https://support.industry.siemens.com/cs/ww/en/view/88778936)
- STEP 7 online help
- SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300) equipment manual (included in the SIMATIC Automation Tool).
- MultiFieldbus function manual (https://support.industry.siemens.com/cs/ww/en/view/109773209)

11.3 Resetting interface module to factory settings

This section applies to interface modules with one or more of these communication protocols:

- PROFINET
- EtherNet/IP
- Modbus TCP

Introduction

When you "Reset to factory settings", the interface module is reset to the delivery state settings. This means that all information that was saved internally on the interface module is deleted.

Result after resetting to factory settings

The following table shows an overview of the contents of the memory objects after resetting to factory settings.

Table 1-21 Result after resetting to factory settings

Memory object	Contents
IP address	• Deleted • Can be configured with TIA Portal for a reset: "Retain IP address"/"Delete IP address"
Device name	Deleted
MAC address	Is not deleted
Identification data (I&M0)	Is not deleted
Maintenance data (I&M1, 2, 3, 4)	Are deleted (optional)
Firmware version	Is not deleted

NOTE

Failure of downstream stations is possible
Resetting an interface module to factory settings can lead to failure of downstream stations in a line.

NOTE

Substitute value behavior of I/O modules when resetting to factory settings
When "Resetting to factory settings", the I/O modules in the station take on the non-configured state, which means input data are not entered and output data are not output.

Reset options

You have the following options to reset an interface module device to the factory settings:

- Online with STEP 7 (TIA Portal)
- Online with STEP 7, V5.5 or higher
- SIMATIC Automation Tool (SAT)
- Online via PRONETA
- Online via MultiFieldbus Configuration Tool (MFCT)

Requirement

You need an online connection to reset an interface module to factory settings.

Procedure with STEP 7 (TIA Portal)

Connect the PG/PC to the PROFINET IO interface of the ET 200AL distributed I/O system.

Make sure that there is an online connection to the interface module which is to be reset to factory settings.

1. Open the online and diagnostics view of the interface module.
2. In the "Functions" folder, select the "Reset to factory settings" group.
3. Select the "Retain IP address" option button if you want to retain the IP address, or the "Reset IP address" option button if you want to delete the IP address.
4. Click the "Reset" button.
5. Answer the security prompts with "OK".

Result: The interface module performs the "Reset to factory settings" while the RUN LED flashes yellow. When the RUN LED is lit yellow, the interface module has been reset to factory settings and is in the STOP operating mode. The event "Reset to factory settings" is entered in the diagnostics buffer.

Procedure with STEP 7 V5.5 or higher

Connect the PG/PC to the PROFINET IO interface of the ET 200AL distributed I/O system.

Make sure that there is an online connection to the interface module which is to be reset to factory settings.

1. Open the SIMATIC Manager.
2. Select accessible devices.
3. Select the interface module.
4. Navigate through "Menu > Options > Edit Ethernet devices > Reset to factor settings > Reset".

Result: The interface module performs the "Reset to factory settings" while the RUN LED flashes yellow. When the RUN LED is lit yellow, the interface module has been reset to factory settings and is in the STOP operating mode. The event "Reset to factory settings" is entered in the diagnostics buffer.

Procedure using the SIMATIC Automation Tool

The procedure is described in the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300) equipment manual (included in the SIMATIC Automation Tool).

Procedure using PRONETA

You can carry out these steps with PRONETA:

- Delete or reassign the device name and IP address
- Reset I&M data
- Remove module from the network and reintegrate

You can find information on this in the "PRONETA user manual (https://support.industry.siemens.com/cs/ww/en/view/109815137)"

Procedure using MFCT

You can find information on the procedure via MFCT under "MultiFieldbus function manual (https://support.industry.siemens.com/cs/ww/en/view/109773209)" in the "Resetting the MF device" section.

Reference

You will find more information on the procedure in the STEP 7 online help.

11.4 Reactions to errors of the F module

Safe state (safety concept)

The basic principle behind the safety concept is the presence of a safe state for all process tags.

NOTE

For digital F-modules, the safe state is "0". The safe state applies to sensors and actuators.

Error reactions and startup of the F-system

In the following situations, the values of the safe state must be connected to the fail-safe channel/channels instead of the process values (passivation of the fail-safe module) due to the safety function:

- When the F-system is started
- When errors are detected in the safety-related communication between the F-CPU and the F-module via the PROFIsafe safety protocol (communication error)
- When errors of the F-I/O or channel errors (e.g. wire break or discrepancy error) are detected

Detected errors are written to the diagnostic buffer of the F-CPU and reported to the safety program in the F-CPU.

F-modules cannot save errors as retentive data. If the system is switched off and then restarted, any pending errors are detected again at startup. However, you can save errors in your safety program.

⚠ WARNING

If channels are set to "disabled", there are no diagnostic or error handling reactions.
For channels that are set to "disabled" in STEP 7, no diagnostic message or error handling is triggered when a channel error occurs. Not even if this channel is indirectly affected by a channel group error ("Channel activated/deactivated" parameter).

Troubleshooting in the F-system

To correct errors in your F-system, proceed as described in IEC 61508-1: Section 7.15.2.4 and IEC 61508-2: Section 7.6.2.1 e.

Perform the following steps:

1. Rung diagnostics and correct the error
2. Revalidate the safety function
3. Record in the service report

Fail-safe values for F-modules

For F-modules with inputs, the F-system provides fail-safe values (0) for the safety program when passivated. The fail-safe values are used instead of the process data at the F-DI.

For F-modules with outputs, the F-system transfers the fail-safe values (0) to the fail-safe outputs during passivation. The fail-safe values are used instead of the output values of the safety program. The fail-safe outputs are de-energized. this process is performed even if the F-CPU goes to the STOP operating state.

It is not possible to set the parameters of fail-safe values.

The fail-safe values are used in the following dependencies for the channel involved or all channels of the I/O module involved:

- F-system used
- Type of error occurred
  - Error in the F-I/O
  - Channel fault
  - Communication error

Re-integration of a fail-safe module or channel

The F-system changes from fail-safe values to process values automatically or after acknowledgment in the safety program by the user. A detailed list of errors can be found in the device manual of the F-module or in the STEP 7 online help.

Procedure after re-integration:

- For an F-module with inputs, the process data pending at the F-DI is provided again to the safety program.
- For an F-module with outputs, the output values provided by the safety program are transferred again to the F-DQs.

Additional information on passivation and re-integration

For additional information on passivation and reintegration of F-I/O modules, refer to the SIMATIC Safety – Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126) manual.

Reaction of the F-module with inputs to communication errors

F-modules with inputs react differently to communication errors than to other errors.

When a communication error is detected, the current process values at the inputs of the F-module remain set. No channels are passivated. The current process values are passivated in the F-CPU.

11.5 Cleaning modules

When wired, ET 200AL modules comply with degree of protection IP65/IP67 and do not require any cleaning. If you do have to clean the modules, then use a dry or damp cloth. Please take care to comply with degree of protection IP65/67 when cleaning with liquids.

Technical specifications

12

12.1 Marks and approvals

Marks and approvals on the nameplate

The following overview provides information about the possible marks and approvals. Only the marks and approvals specified on the nameplate apply to the module.

You can find the associated certificates for download on the Internet. See also: ET 200AL approvals (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert)

CE marking

CE

The ET 200AL distributed I/O system fulfills the requirements and protection targets of the following directives and complies with the harmonized European standards (ES) which have been promulgated for programmable logic controllers in the official gazettes of the European Community:

- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)

  Directive of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the member states relating to electromagnetic compatibility; OJ L 96, 29.3.2014, p. 79–106
- 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment; OJ L 174, 1.7.2011, p. 88–110

The fail-safe modules of the ET 200AL distributed I/O system meet the safety requirements and safety objectives of the following EU directives and comply with the harmonized EU standards (EN) for programmable controllers as specified in the official journals of the European Union.

- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)

  Directive of the European Parliament and of the Council of February 26, 2014 on the harmonization of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, pages 79–106
- 2006/42/EC "Machinery Directive and Supplementary Directive 95/16/EC"

  Directive of the European Parliament and of the Council of 17 May, 2006 on machinery, and amending Directive 95/16/EC (revised); official journal of the EU, L157, 09/06/2006, pages 24–87
- 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, official journal of the EU L174, 01/07/2011, pages 88–110

The EC Declarations of Conformity are available for the responsible authorities and are kept at the following address:

Siemens Aktiengesellschaft
Digital Industries
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg, Germany

UKCA mark

The ET 200AL distributed I/O system complies with the designated British standards (BS) for programmable logic controllers published in the official consolidated list of the British Government. The ET 200ALdistributed I/O system meets the requirements and protection targets of the following regulations and associated supplements:

- Electromagnetic Compatibility Regulations 2016 (S.I. 2016 No. 1091), and related amendments
- Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (S.I. 2012 No. 3032), and related amendments
- Supply of Machinery (Safety) Regulations 2008 (S.I. 2008 No. 1597), and related amendments

UK Declarations of Conformity are available to the relevant authorities at the following address:

Siemens Aktiengesellschaft
Digital Industries
Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg, Germany

UL approval

Underwriters Laboratories Inc. according to

- UL 61010-1 and UL 61010-2-201
- CSA C22.2 No. 61010-1 and CSA C22.2 No. 61010-2-201

The following table shows the modules that are approved for UL50 Enclosure Type 4x Indoor use only, watertight.

Table 1-22 Modules approved according to UL50 Enclosure Type 4x, Indoor use only, watertight

Description	Article number
Interface modules	
IM 157-1 DP	6ES7157-1AA00-0AB0
IM 157-1 PN	6ES7157-1AB00-0AB0
Digital modules	
DI 8 x DC24V 8xM8	6ES7141-5BF00-0BA0
DI 8 x DC24V 4xM12	6ES7141-5AF00-0BA0
DI 16 x DC24V 8xM12	6ES7141-5AH00-0BA0
DIQ 4+DQ 4x24VDC/0.5A 8xM8	6ES7143-5BF00-0BA0

Description	Article number
DIQ 4+DQ 4x24VDC/0.5A 4xM12	6ES7143-5AF00-0BA0
DIQ 16x24VDC/0.5A 8xM12	6ES7143-5AH00-0BA0
DQ 8x24VDC/2A 8xM12	6ES7142-5AF00-0BA0
Analog modules	
AI 4xU/I/RTD 4xM12	6ES7144-5KD00-0BA0
AQ 4XU/I, 4XM12	6ES7145-5ND00-0BA0
Communications modules	
CM 4xIO-Link 4xM12	6ES7147-5JD00-0BA0

The following table shows the modules that are approved for UL50 Enclosure Type 1.

Table 1-23 Modules approved according to UL50 Enclosure Type 1

Description	Article number
Interface modules	
IM 157-1 MF	6ES7157-1MA00-0AB0
Digital modules	
DIQ 8x24VDC/0.5A 8xM8	6ES7143-5BF50-0BA0
Analog modules	
AI 4xRTD/TC 4xM12	6ES7144-5KD50-0BA0
Fail-safe modules	
F-DI 4+F-DQ 2x24VDC/2A, 4xM12	6ES7146-5FF00-0BA0
Communications modules	
CM 4xIO-Link 4xM12	6ES7147-5JD01-0BA0
CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12	6ES7147-5JJ00-0BA0
Voltage distributor	
PD 24VDC	6ES7194-2CA00-0AA0

RCM Australia/New Zealand

The ET 200AL distributed I/O system meets the requirements of EN 61000-6-4 Generic standards – Emission standard for industrial environments.

Korea Certificate

Please note that this device corresponds to limit value class A in terms of the emission of radio frequency interference. This device can be used in all areas, except residential areas.
이기기는업무용(A급) 전자파적합기기로서판매자또는사용자는이점을주의하시기바라며 가정외의지역에서사용하는것을목적으로합니다.

EAC (Eurasian Conformity)

The code EAC (Eurasian Conformity) confirms the conformity with the guidelines (TR) of the Eurasian Economic Union.

WEEE mark (European Union)



Disposal information, observe the local regulations and section "Secure decommissioning (Page 137)".

12.2 Certificates

Shipbuilding certificates

The following shipbuilding certificates are intended for the device:

- ABS (American Bureau of Shipping)
- Bureau Veritas (French marine classification society)
- CCS (China Classification Society)
- Class NK (Nippon Kaiji Kyokai)
- DNV (Det Norske Veritas)
- KR (Korean Register of Shipping)
- LRS (Lloyds Register of Shipping)
- RINA (Registro Italiano Navale)

After a successful approval you can find the certificates with the certified article numbers in the Internet. See also: ET 200AL Marine/Shipbuilding (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert?ct=446)

NOTE

The fail-safe module F DI 4+F DQ 2x24VDC/2A, 4xM12 of the ET 200AL distributed I/O system does not support the specified marine approvals due to the increased supply voltage requirements.

12.3 Standards and requirements

IEC 61131-2

The ET 200AL distributed I/O system fulfills the requirements and criteria of IEC 61131-2 (Programmable controllers, Part 2: Equipment requirements and tests) and the EMC requirements for use in Zone B.

IEC 61010-2-201

The ET 200AL distributed I/O system fulfills the requirements and criteria of standard IEC 61010-2-201.

PROFINET standard

The PROFINET interfaces of the ET 200AL distributed I/O system are based on the standard IEC 61158 Type 10.

PROFIBUS standard

The PROFIBUS interfaces of the ET 200AL distributed I/O system are based on IEC 61158 Type 3.

IO-Link standard

The IO-Link interfaces of the ET 200AL distributed I/O system are based on the standard IEC 61131-9.

Use in industrial environments

The ET 200AL distributed I/O devices are designed for the industrial field. It meets the following standards for this type of use:

- Requirements for interference emission EN IEC 61000-6-4
- Requirements for immunity EN IEC 61000-6-2

Use in residential areas

The ET 200AL distributed I/O system is not intended for use in residential areas. Using the ET 200AL distributed I/O system in residential areas can affect radio or television reception.

Use in mixed areas

Under certain circumstances, you can use the ET 200AL distributed I/O system in a mixed area. A mixed area is used for residential purposes and for commercial operations that do not significantly impact on residents.

If you want to use the ET 200AL distributed I/O system in mixed areas, you must ensure that its radio frequency interference emission complies with the limit classes of the EN 61000-6-3 generic standard. Suitable measures for observing these limits for use in a mixed area are, for example:

- Installation of the ET 200AL distributed I/O system in grounded control cabinets/control boxes
- Use of noise filters in the supply cables

An individual acceptance test is also required.

EtherNet/IP requirement

The EtherNet/IP interfaces of the ET 200AL distributed I/O system are based on the requirements of the CIP network library CIP Networks Library Volume 2 EtherNet/IP Adaptation of CIP.

Modbus TCP requirement

The Modbus TCP interfaces of the ET 200AL distributed I/O system are based on the requirements of the Modbus TCP application protocol specification V1.1b3.

Use in industrial burner and firing environments.

The fail-safe module F-DI 4+F-DQ 2x24VDC/2A, 4xM12 of the ET 200AL distributed I/O system meets the requirements and criteria of the following standards:

- EN 298 (Automatic burner control systems for burners and appliances burning gaseous or liquid fuels)
- EN 50156-1 (Electrical equipment for furnaces and ancillary equipment)
- EN 50156-2 (Electrical equipment for furnaces and ancillary equipment)

Importer addresses

The following table shows the importer addresses for specific countries:

Countries	Address
United Kingdom (UK)	Siemens plc. Manchester M20 2UR
Türkiye (TR)	Siemens San. ve Tic. A.Ş. Yakacık Cad. No:111 34870 Kartal/İstanbul

12.4 Electromagnetic compatibility

Definition

Electromagnetic compatibility is the ability of an electrical apparatus to function in a satisfactory manner in its electromagnetic environment without affecting this environment.

An I/O device of the ET 200AL distributed I/O system fulfills the requirements of the EMC law of the European Union. The requirement for this is that an I/O device of the ET 200AL distributed I/O system meets the specifications and guidelines for electrical configuration.

Pulse-shaped disturbance variables

The table below shows the electromagnetic compatibility of the distributed I/O systems compared to pulse-shaped disturbance variables.

Table 1-24 Pulse-shaped disturbance variables

Pulse-shaped disturbance variable	Tested with	Conforms to degree of severity
Electrostatic discharge according to IEC 61000-4-2.[1]	Air discharge: ±8 kV	3
	Contact discharge: ±4 kV	2
Burst pulses (fast transient disturbance variables) according to IEC 61000-4-4.[1]	±2 kV (power supply cable)	3
	±2 kV (PROFIBUS/PROFINET/MultiFieldbus line)	4
	±1 kV (signal line <30 m)	3
	±1 kV (ET-Connection)	3
High-energy single pulse (surge) to IEC 61000-4-5 [2] Signal line < 30 m and only installation within buildings		

Pulse-shaped disturbance variable	Tested with	Conforms to degree of severity
• Asymmetric coupling (phase-ground)[3]	±1 kV (24 V DC supply cable) without protective element	2
	±2 kV (PROFIBUS/PROFINET/MultiFieldbus line)	3
• Symmetric coupling (phase-phase)[3]	±0.5 kV (24 V DC supply cable) without protective element	2

[1] The maximum short-term influencing of analog devices during the duration of the EMC tests can amount to ±10 % of the full-scale value.
[2] Analog value deviation beyond the limits of the nominal range and diagnostics possible.
[3] If greater phase to ground or phase to phase values are required, you will need an additional external protective circuit (see function manual Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566)).

Sinusoidal disturbance variables

The following tables show the electromagnetic compatibility of the distributed I/O systems to sinusoidal disturbance variables.

Table 1-25 RF radiation

RF radiation according to IEC 61000-4-3 Electromagnetic RF field, amplitude modulated		Conforms to degree of severity
80 ... 1000 MHz	10 V/m	3
1.4 ... 6 GHz	3 V/m	2
80% AM (1 kHz)		

Table 1-26 RF coupling (signal and supply cables)

RF coupling according to IEC 61000-4-6.	Conforms to degree of severity
0.15 ... 80 MHz	3
10 V_{rms} unmodulated	
80% AM (1 kHz)	
150 Ω source impedance	

The maximum short-term influencing of analog modules during the duration of the EMC tests can amount to ±1% of the full-scale value.

Emission of radio frequency interference

The following table shows the interference emission of electromagnetic fields according to EN IEC 61000-6-4/EN 55016-2-3.

Table 1-27 Interference emission of electromagnetic fields

Frequency	Interference emission	Measuring distance
30 ... 230 MHz	<40 dB (µV/m) Q	10 m
230 ... 1000 MHz	<47 dB (µV/m) Q	10 m
1 ... 3 GHz	<76 dB (µV/m) P	3 m
3 ... 6 GHz	<80 dB (µV/m) P	3 m

Conducted emission

The following table shows the limit values for the power supply connections according to EN IEC 61000-6-4/EN 55016-2-1.

Table 1-28 Interference emission from the power supply

Frequency	Interference emission
0.15 ... 0.5 MHz	< 89 dB (µV) Q < 76 dB (µV) M
0.5 ... 30 MHz	< 83 dB (µV) Q < 70 dB (µV) M

12.5 Transport and storage conditions

Transport and storage conditions

The modules of the ET 200AL distributed I/O system exceed the specifications regarding transport and storage conditions pursuant to IEC 61131-2. The following table shows the conditions that apply to modules transported or stored in their original packaging.

- Transport condition class: TTH4
- Storage condition class: STH4

Table 1-29 Transport and storage conditions

Type of condition	Permitted range
Free fall	≤0.3 m
Temperature	-40 °C ... +70 °C
Temperature variation	20 K/h
Barometric pressure	1140 ... 540 hPa (Corresponds to an altitude of -1000 m to 5000 m)
Relative humidity	5... 95 %; no condensation

12.6 Mechanical and climatic ambient conditions

Operating conditions

The ET 200AL distributed I/O system is suitable for use in weather-proof, fixed locations.

- The conditions of use exceed the requirements pursuant to IEC 61131-2
  - Class OTH3

You can find the values for the operating conditions in the technical specifications of the manuals or on the Internet (https://support.industry.siemens.com/cs/de/en/view/109742718).

Tests of mechanical ambient conditions

The following table shows the type and scope of the tests on mechanical ambient conditions.

Table 1-30 Tests of mechanical ambient conditions

Condition tested	Test standard	Values
Vibrations	Vibration test according to IEC 60068-2-6.	Type of oscillation: Frequency sweeps with a rate of change of 1 octave/minute. 5 Hz to 12.9 Hz, constant amplitude 15 mm 12.9 Hz to 150 Hz, constant acceleration 10 g Duration of oscillation: 10 frequency sweeps per axis at each of three vertically aligned axes
Shock	Shock, tested according to IEC 60068-2-27	Type of shock: Half-sine Shock intensity: 30g peak value, 18 ms duration Direction of shock: 3 shocks each in ± direction in each of the 3 axes vertical to one another

Climatic ambient conditions

The following table shows the type and scope of the tests on climatic ambient conditions.

Table 1-31 Climatic ambient conditions

Ambient conditions	Fields of application	Comments
Temperature	-25 °C ... 55 °C	All installation positions
Temperature variation	10 K/h	-
Relative humidity	5 ... 100%	With condensation and sealing caps installed
Barometric pressure	1140 ... 540 hPa	Corresponds to an elevation of -1000 to 5000 m
Pollutant concentration	ANSI/ISA-71.04 severity level G1; G2; G3	-

The following table shows the modules with functional versions which are permitted to -30 °C.

Table 1-32 Extended temperature range to -30 °C

Description	Article number	As of functional version
Interface modules		
IM 157-1 DP	6ES7157-1AA00-0AB0	FS02
IM 157-1 MF	6ES7157-1MA00-0AB0	FS01
Digital modules		
DI 8 x DC24V 8xM8	6ES7141-5BF00-0BA0	FS03
DI 8 x DC24V 4xM12	6ES7141-5AF00-0BA0	FS03
DI 16 x DC24V 8xM12	6ES7141-5AH00-0BA0	FS03
DIQ 4+DQ 4x24VDC/0.5A 8xM8	6ES7143-5BF00-0BA0	FS03
DIQ 4+DQ 4x24VDC/0.5A 4xM12	6ES7143-5AF00-0BA0	FS03
DIQ 8x24VDC/0.5A 8xM8	6ES7143-5BF50-0BA0	FS01
DIQ 16x24VDC/0.5A 8xM12	6ES7143-5AH00-0BA0	FS03
DQ 8x24VDC/2A 8xM12	6ES7142-5AF00-0BA0	FS03
Analog modules		
AI 4xU/I/RTD 4xM12	6ES7144-5KD00-0BA0	FS04
AI 4xRTD/TC 4xM12	6ES7144-5KD50-0BA0	FS01
AQ 4XU/I, 4XM12	6ES7145-5ND00-0BA0	FS03
Communications modules		
CM 4xIO-Link 4xM12	6ES7147-5JD00-0BA0	FS05
CM 4xIO-Link 4xM12	6ES7147-5JD01-0BA0	FS01
CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12	6ES7147-5JJ00-0BA0	FS01
Fail-safe modules		
F-DI 4+F-DQ 2x24VDC/2A, 4xM12	6ES7146-5FF00-0BA0	FS01
Voltage distributor		
PD 24VDC	6ES7194-2CA00-0AA0	FS01

Use above 2000 m is possible.

The following constraints apply to the maximum specified ambient temperature:

Table 1-33 **Derating factor of installation altitude and ambient temperature**

Installation altitude	Derating factor for ambient temperature [1]
-1000 ... 2000 m	1.0
2000 ... 3000 m	0.9
3000 ... 4000 m	0.8
4000 ... 5000 m	0.7

[1] Base value for application of the derating factor is the maximum permissible ambient temperature in °C for 2000 m.

NOTE

- Linear interpolation between altitudes is permissible.
- The derating factors compensate for the decreasing cooling effect of air at higher elevations due to lower density.
- Make sure that the power supplies used are suitable for altitudes > 2000 m.

NOTE

All markings and certifications are currently based on an elevation of up to 2000 m.

12.7 Details on insulation, protection class, degree of protection and rated voltage

Insulation

The insulation is designed in compliance with the requirements of IEC 61010-2-201.

NOTE

Galvanic isolation with 707 V DC (Type Test) is tested for modules with 24 V DC supply voltage (SELV/PELV).

Pollution class according to IEC 61010-2-201

- Protection class III

Severity for voltage interruption

The I/O devices of the distributed I/O system ET 200AL meet and exceed the severity class PS1 for voltage interruptions with a value of 5 ms.

Pollution degree / overvoltage category pursuant to IEC 61010-2-201

Connected according to the specifications in the "Wiring (Page 62)" section:

- Pollution degree: 3 (macro environment)
- Overvoltage category: II

In delivery state, with one or more open connections:

- Pollution degree: 2 (micro environment)
- Overvoltage category: II

Degree of protection IP65 and IP67

Degree of protection IP65 and IP67 according to IEC 60529 for all modules of the ET 200AL distributed I/O system:

- 1. Code number: Dust-proof and complete protection from contact
- 2. Code number: Protection from water
  - IP65: Protection from water jets from any angle
    (The water may not have any damaging effect)
  - IP67: Protection against temporary submersion
    (The water must not enter the enclosure in harmful quantities)

Rated voltage for operation

The following table shows the nominal voltage and the corresponding tolerance with which the ET 200AL distributed I/O system operates.

Table 1-34 Rated voltage for operation

Rated voltage (SELV/PELV)	Tolerance range
24 V DC	20.4 ... 28.8 V DC

Industrial cybersecurity 13

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

In the first part of this section you will find basic information on the subject of industrial cybersecurity. Subsequent sections describe recommended measures for protecting the entire system and individual components from manipulation and unwanted access.

NOTE

Security-relevant changes to software or devices are documented in the section New properties/functions (Page 22).

13.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

13.2 Security update notification

Read the special information on maintaining the operational safety of your plant in the Introduction (Page 8) section.

Set up notification of security updates

To receive notifications about security updates, proceed as follows:

1. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home).
2. Enter the keyword "Security" in the search engine.
3. Choose the "Search in Knowledge base" option.
4. In the "Product tree" filter menu, select your product or your product group, for example "Automation Technology" > "Automation Systems" > "Industrial Automation Systems SIMATIC" > "I/O systems" > "SIMATIC ET 200 systems without control cabinet" > "ET 200AL".
5. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".
6. Select the document about which you want to receive notifications using the 3 points on the right "Add to my favorites".
7. In the following dialog, select the name, the storage location and the "Notify me" option for the favorite. Then click on the "+ Add to my favorites" button.

Result: You will be notified by email each time the document is changed.

Under "mySiePortal" > "Lists & notifications" > "My notifications", you can display your notifications and delete them if necessary.

13.3 Basic information on industrial cybersecurity

13.3.1 Definition of industrial cybersecurity

Industrial cybersecurity is generally understood to mean all measures to protect against the following threats:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability (e.g. due to the destruction of data or denial of service (DoS))

13.3.2 Objectives of industrial cybersecurity

The objectives of industrial cybersecurity are:

- Ensuring trouble-free operation of industrial systems and production processes
- Preventing threats to people and production from cybersecurity attacks
- Protection of industrial plants against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Provision of a practical and cost-effective concept for securing existing plants and devices without their own security functions

- Use of existing, open and proven industrial cybersecurity standards
- Compliance with legal requirements

An optimized and adapted security concept applies to automation and drive technology. The security measures must not impede or endanger production.

13.4 Integrated security concept and security strategies

13.4.1 Comprehensive security concept "Defense in Depth"

With Defense in Depth, Siemens provides a multi-layer security concept that offers industrial plants comprehensive and far-reaching protection in accordance with the recommendations of the IEC 62443 international standard.

Productivity and know-how are protected on 3 levels:

Plant security
Plant security uses various methods to secure the physical access of people to critical components. This starts with classic building access and extends to securing sensitive areas using access control (for example, code card, iris scan, fingerprint or access code).

Network security
Automation networks must be protected against unauthorized access. This is achieved through security measures on the product, but also those in the product-related environment.

System integrity
Targeted measures must be taken to protect existing know-how or to prevent unauthorized access to automation processes. The measures protect against unauthorized configuration changes and highlight attempts at manipulation.

You can find more information on the topics of Defense in Depth, plant security, network security, and system integrity on the SIEMENS Industrial cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) Web page.

You can also visit the download center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) to obtain more information on the topic of industrial cybersecurity. The "Operational Guidelines", for example, provide recommendations on basic security measures for secure machine and plant operation in an industrial environment.

13.4.2 Security management

The ISO 27001 and IEC 62443 standards call for a comprehensive approach in information technology (IT) and operational technology (OT) to protect against cyber attacks.

Responsibility for cybersecurity and IT security

Every operator of machinery and equipment is responsible for:

- Defining cybersecurity and IT security as an important criterion in the procurement and selection of machines and software applications.
- Use of suitable measures to protect production resources, data, and communication from manipulation and theft
- Providing all necessary resources and training to employees to fully support these goals

For this purpose, suitable measures must be selected after a risk assessment and a cost-benefit analysis in order to protect material and intellectual property and prevent damage from occurring. These measures should be integrated into corporate processes and procedures, evaluated regularly, and firmly anchored in the corporate culture. In addition to protecting intellectual property, the protection of personal data must be ensured at all organizational units and levels.

Siemens will provide you with information and support. Subscribe to the Security feeds (https://www.siemens.com/cert) for information on vulnerabilities. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home) and create filters to be notified when important information is published. The procedure is described in the section Notification of security updates (Page 129). Consider using Siemens Cybersecurity Services.

Responsibility in the digital supply chain

Cybersecurity should play a critical role in the evaluation and procurement process. The entire life cycle of a product should be considered to ensure protection against current and future risks. These include, for example, security updates throughout the product life cycle, including guidelines for secure disposal of the product.

Siemens plans and announces the provision of security updates, as well as total discontinuation of products, as part of product support.

Employee awareness

Regular training in cybersecurity and continuous testing of training success are essential so that cybersecurity measures are internalized in processes and work instructions. This involves general training in the use of software and IT hardware for company communication and as work equipment e.g.:

- Secure handling of USB devices
- Encrypted communication
- Use of VPN
- Rules for passwords and use of access
- Setting up two-factor authentication
- Educating employees about the dangers posed by malware, phishing, social engineering and other factors

Furthermore, if applicable, production equipment and software training should always include the topic of cybersecurity.

Maintaining the security concept through updates

Keeping software up-to-date is essential, for example, to benefit from the following measures:

- Implementation of new security strategies, protocols and techniques
- Closing of security vulnerabilities
- Elimination of security vulnerabilities

To this end, it is necessary to keep a constant eye on the further development of protective measures and, if necessary, the expansion of requirements.

Recommendations:

- Set up notifications for (security) updates
- Subscribe to information on vulnerabilities
- Monitor and implement the further development of the technology, especially in the area of cybersecurity

Always keep technology and knowledge up to date.

Consideration of the risks posed by cyber attacks in the Threat and Risk Assessment (TRA)

Make an inventory of all software, hardware, and infrastructure devices, in order to identify risks to the location or organization. Incident response procedures must be incorporated into all IT and manufacturing processes. The choice of risk mitigation measures should be based on a cost-benefit analysis and classification of risks. This is followed by the introduction of cybersecurity rules and procedures and the training of personnel.

Living the concept

Technical solutions alone are not sufficient to effectively counter threats.

Cybersecurity must be part of the corporate culture and process landscape and must be internalized and lived by all employees.

Continuously monitoring the security situation

You have the following options for continuously monitoring the cybersecurity situation:

- Setting anomaly references and creating allow and deny lists based on normal network communication and production machine behavior. The SINEC software family offers you reliable security tools (https://www.siemens.com/global/en/products/automation/industrial-communication/sinec-network-software/cybersecurity.html) to detect potential vulnerabilities in OT networks, quickly initiate suitable measures and effectively resolve security vulnerabilities.
- Establishment of an intrusion detection system (IDS) that generates alarms when unusual behavior occurs in the network

- Introduction of a Security Information and Event Management (SIEM) system to collect, analyze, and evaluate events in real time to enable early countermeasures
- Measures regarding network security: for example network segmentation, firewalls, VPN, DMZ (demilitarized zones)

13.5 Operational application environment and security assumptions

13.5.1 Intended use

SIMATIC products are intended for use in industry. If you plan to use the product in a different environment, check the conditions required for such use.

The product may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety information. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products.

Operational reliability and intended use

Read the "Special information" in the Introduction (Page 8) section.

Area of application

Refer to the "Application area" section in the System overview (Page 24) chapter.

13.5.2 Requirements for the operational application environment and security assumptions

Siemens recommends the following security measures:

- Threat and risk assessment (as part of security management)
- Network security concepts
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
- Access control concepts (utilizing access control systems)
  - Physical protection
  - Physical corporate security
  - Physical product security

Threat and Risk Assessment

Vulnerabilities and risks are identified, and countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) on the Industrial Cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) website.

Access control concepts

Physical protection
In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security
You can ensure the physical security of the company by taking the following measures:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security
You can ensure physical production safety by taking the following measures, among others:

- Separate access control for critical areas, such as production zones.
- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.
- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).
- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsafe on systems.

13.6 Security properties of the devices

The security properties of the individual devices are listed in the Equipment Manuals.

13.7 Secure operation of the system

This section describes measures recommended by Siemens to protect your system from manipulation and unauthorized access.

13.7.1 Hardening measures

System hardening, simplify referred to as hardening, is the secure configuration of products or systems. The aim is to close security gaps and take various measures to reduce the attack surfaces for cyberattacks.

Measures for system hardening include, for example:

- Secure configuration in which only necessary software components and services are installed or activated for proper operation.
- Access control, by which restrictive user and rights management system is implemented.

13.7.2 Secure configuration

Secure configuration involves control over all software components, along with their interfaces, ports, and services.

Activated services and ports pose a risk, e.g. of unauthorized access to the network and programs.

To minimize risks, only activate the necessary services for all automation components. Take all activated services (especially Web servers, FTP, remote maintenance etc.) into account in the security concept. Consider the default states of ports and services in your security concept.

You can find an overview of all ports and services used in the Communication function manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

13.7.3 Handling of sensitive data

Data protection information

Siemens Aktiengesellschaft observes the applicable data protection laws, including the General Data Protection Regulation (GDPR), in particular the rules of data minimization and data protection-friendly default settings (privacy by design, privacy by default).

The products do not store any personal data.

If you establish a reference to an identifiable person by linking this functional data with other data (such as shift schedules) or if you store personal data on the same medium (such as a hard disk), you are responsible for ensuring that the data protection regulations are observed.

Information on the secure removal of data is provided in the section Secure decommissioning (Page 137).

Storage of security-related data

When storing your security-relevant data on your PC, independently ensure secure data storage.

13.7.4 Regular firmware updates

NOTE

Outdated firmware versions might not be monitored for security vulnerabilities.

- Always keep your plant/products up to date to benefit from troubleshooting and to minimize potential risks.
- Use email notifications to be automatically informed about firmware updates.

You can find more information in:

- Section Firmware update (Page 110)
- Section Notification of security updates (Page 129)

13.7.5 Notifications about security vulnerabilities (Siemens Security Advisories)

A vulnerability is a security vulnerability in information security. It can pose a threat as it provides intruders with the opportunity to access system resources and manipulate or steal data. Many vulnerabilities allow availability to be impaired.

Siemens ProductCERT

If Siemens identifies or fixes security gaps (Vulnerabilities) in the products, this will be published in the Security Advisories.

You can find the documents for SIMATIC on the following Siemens Aktiengesellschaft web page: Siemens ProductCERT and Siemens CERT (https://www.siemens.com/global/en/products/services/cert.html?s=SIMATIC&_originalHost=new.siemens.com#SecurityPublications)

"SIMATIC" is preset in the "Search Security Advisories" search field. You can also enter other product names or other terms in the search field and search for them.

On this page, you will also find all the required information on how to deal with vulnerabilities:

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities
- Notifications are also possible in CSAF format
- Option to subscribe to RSS feeds and newsletters
- List of all current vulnerabilities and detailed information such as:
  - Description
  - Classification according to Common Vulnerability Scoring System (CVSS)
  - Measures
  - Availability
  - Etc.

Set up Security feeds (https://www.siemens.com/cert) to receive notifications about security-related topics.

If you suspect or have discovered a vulnerability in a Siemens product, please inform us immediately. To do this, press the "Contact" button on the CERT Services page (https://www.siemens.com/cert) and follow the instructions.

13.7.6 Data backup

Secure your configuration and parameter settings so that you can quickly restore this data if needed.

13.7.7 Security checks

Security checks for data, files, and archives serve to ensure data integrity at the storage location and during file transmission, protecting against manipulation and transmission errors. This is often achieved using digital checksums that are provided alongside the data. Tools (such as SHA-256 or SHA-512) for calculating and verifying these checksums are provided in many systems and named according to their respective calculation methods.

File Integrity Guidelines describe the prescribed procedure for integrity checks

Integrity protection is a protection function for engineering data and firmware files

Communication integrity means protecting communication against unauthorized manipulations to ensure high system availability. A central element in this regard is, for example, the use of digital checksums when accessing controllers. (Source: Industrial Cybersecurity website (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html))

13.7.8 Secure decommissioning

In the following section, you will find information on how to properly decommission individual components of your automation system. Decommissioning is necessary when the component has reached the end of its service life.

Decommissioning includes environmentally sound disposal and secure removal of all digital data of electronic components with storage medium.

13.7.8.1 Securely removing data

Before disposing of components of your automation system, you should securely delete all data from the storage media of these components. How to securely delete data from the devices so that it cannot be recovered is described below.

NOTICE
Data misuse resulting from non-secure deletion of data Incomplete or non-secure deletion of data from data memories can result in data misuse by third parties. For this reason, ensure secure deletion of data from all storage media used before disposing of the product.

Secure erasure of data from the interface module

With the following tools, you can securely erase the data from the interface module:

- STEP 7 < V19
- SIMATIC Automation Tool
- MultiFieldbus Configuration Tool (MFCT)
- PRONETA

Follow these steps in the order given:

1. Establish an online connection.
2. Open the Online and Diagnostics view of the IM (either from the project context or via "Accessible devices").
3. In the dialog box "Functions > Reset to factory settings", select the option "Delete I&M data" and then the "Reset" button.

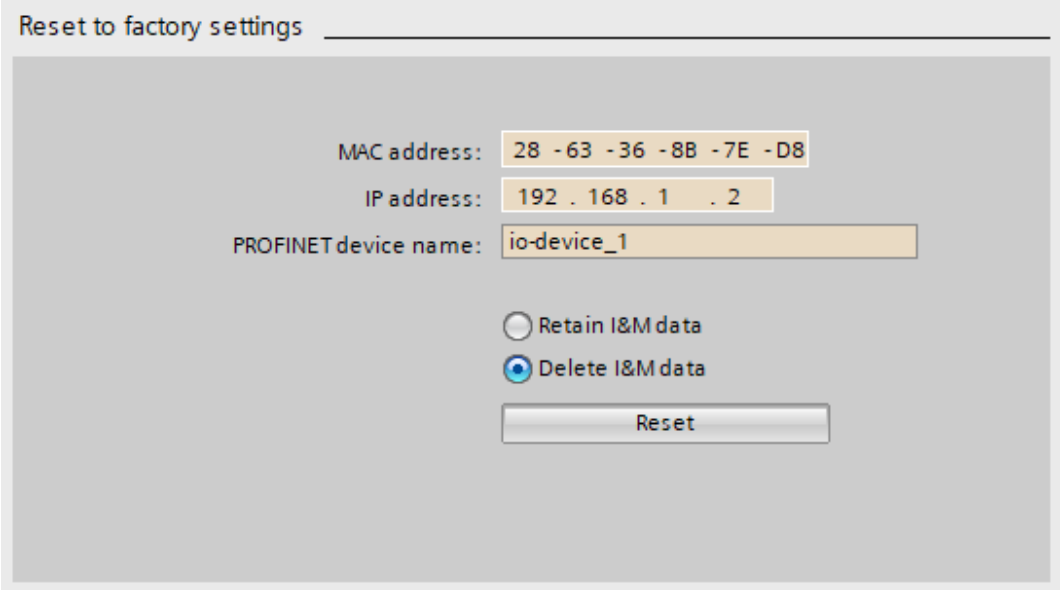


Figure 1-46 Resetting an interface module to factory settings

Result: All the data that was still in the data memories of the interface module was deleted. You can now dispose of the components.

For more information on resetting the interface module to factory settings, refer to the section Resetting an interface module to factory settings (Page 111).

NOTE

STEP 7 ≥ V19

Only the communication parameters will be securely deleted on "Reset to factory settings" with the "Delete I&M data" option enabled when you use STEP 7 ≥ V19.

Deleted communication parameters:

- IP address
- Device name
- PROFINET configuration data

If you want to securely remove all data, use one of the tools listed above for this purpose.

13.7.8.2 Recycling and disposal

For environmentally sustainable recycling and disposal of your old equipment, contact a certified electronic waste disposal service and dispose of the equipment according to the applicable regulations in your country.

13.8 Secure operation of the engineering software

For more information on secure operation of the engineering software, refer to the TIA Portal online help.

13.9 Secure operation of interface modules

Device-specific security information and instructions for interface modules can be found in the respective Equipment Manual.

13.9.1 Data integrity for interface modules

Data integrity refers to the completeness and correctness (integrity) of data, which is an essential prerequisite for the proper functioning of systems.

Measures for data privacy, data consistency, and data security ensure that data used within devices cannot be damaged, altered (manipulated), or deleted during processing or transmission, and at the very least, any changes to the data are detected.

Data integrity for interface modules

To detect intentional or accidental changes to data within an interface module and its associated modules, the possibility of dynamic integrity checking is introduced for PROFINET interface modules.

The ability to detect integrity breaches enhances the resilience of the distributed I/O system.

Data integrity within a distributed I/O system is entirely covered within the interface module and does not pertain to other components of the automation system.

Principle

The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as parameter settings, IP address, device name, MAC address and I&M data. The interface module stores the checksums in the I&M4 data area.

A CRC (Cyclic Redundancy Check) is always the same for a specific, unchanged memory content. When the memory content changes, the interface module (IM) calculates a different checksum for this content by reading and comparing the I&M4 data. By comparing with the initial CRC, you can determine whether the data in the memory has been modified or not:

- CRC stayed the same: No change in the data within this memory area of the interface module IM
- CRC changed: The data within this memory area of the IM was modified

Only you, as the user, know whether changes to the data of an interface module were intentional or not. If changes were not intentional, you can detect that the data of the interface module has been compromised through changed CRCs and respond accordingly.

I&M data

PROFINET devices provide Identification and Maintenance data (I&M data), which is a set of predefined data structures containing the internal module status. With this data, a module can be identified, its serial number can be determined, etc.

The CRC checksums are mapped in the maintenance data **I&M4** of the interface module.

NOTE

Requirements for calculating the CRCs

The CRCs via the memory contents of the interface module are calculated only when you request to read the I&M4 data.

The CRCs cover not only the interface module itself but can also take into consideration combined checksums from associated modules (refer to the section on the structure of the data record for I&M data). Process data is not included in the calculation of CRCs.

Example:

- You put your distributed I/O system into operation and read the CRC CHK_OVERALL with the value "0x55AAA678" ("16#55AAA678") from the interface module via the I&M4 data.
- As long as no changes have been made to the data of the interface module or the associated modules, each subsequent read will give the value "0x55AAA678" or "16#55AAA678".
- Once you read a different CRC CHK_OVERALL, for example, "0xCC9876FF", you will realize that there must have been changes to the data of the interface module or the associated modules.

The quality of the statement regarding the data integrity of the distributed I/O system improves with each module associated with the interface module that supports I&M4 data. Refer to the Equipment Manual of the respective module to find out if and from which firmware version the module supports I&M4 data.

You can find the structure of I&M data 0 to 4 in the section Record structure for I&M data (Page 105).

Spare parts scenario

The spare parts scenario is still ensured. This means that you can replace interface modules with the same article number. For the "new" interface module, the static data such as the serial number and MAC addresses will change. Note that this is why the replacement will be reflected in the changed identification data CHK_STATIC_LOCAL and consequently also in CHK_OVERALL.

More information on the spare parts scenario and compatibility can be found in the Equipment Manual of the interface module.

13.9.2 Signed firmware update for interface modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect internet source

Information on whether your interface module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

Principle of the signed firmware update for interface modules

Firmware updates for interface modules starting with article number 6ES7157-1MA00-0AB0 may include a digital signature. The digitally signed firmware update files are available for download on the Siemens Support Web page.

The interface module verifies the authenticity and integrity of the firmware update file before installation using the digital signature with standardized asymmetric cryptography methods. As a result, the interface module can detect a manipulated or corrupted firmware update file and reject it.

Note that the interface module performs the verification only after the complete firmware download has taken place.

Subsequently, a notification is sent to the firmware update tool regarding the success or failure of the signature verification.

You still have all the options for firmware updates, as described in the Firmware update (Page 110) section, when performing signed firmware updates for modules. If the firmware update was not successful, the module will continue to run with the previous firmware.

Diagnostics alarms and remedy

When performing a firmware update for a module with an established connection between the IM and CPU, the following options for notifications are available in the CPU's diagnostic buffer:

- Successful integrity check of the firmware for the module
- Rejection of non-secure firmware for the module

You can find more information in the section on diagnostics alarms in the equipment manual for the respective module.

In case of firmware update rejection, proceed as follows:

1. Check whether the firmware update file you are using originates from a secure source and was downloaded unchanged. As a check, calculate the hash value of the downloaded firmware update file and compare it with the value specified on the download page.
2. Download the firmware again from the Siemens Support website.
3. Repeat the firmware update.

Information on the procedure for calculating and comparing hash values is available on the Internet (https://support.industry.siemens.com/cs/de/de/view/109483101/en).

13.9.3 Secure Boot

Secure Boot

Secure Boot verifies, before the boot process, whether firmware has been falsified, for example through manipulation or accidental falsification.
Secure Boot ensures the authenticity and integrity of the firmware executed by the device.

Information on whether your interface module supports Secure Boot is available in the Technical specifications section of the corresponding Equipment Manual.

Principle of "Secure Boot" for interface modules

Interface modules verify the authenticity and integrity of the firmware to be executed using "Secure Boot" before being executed.

The verification is carried out using standardized asymmetric cryptography methods.

In addition to signed firmware updates for interface modules, Secure Boot also prevents manipulation of the firmware through physical intervention in the interface module.

Secure Boot is integrated into the interface module and cannot be deactivated for security reasons.

NOTE

Longer startup duration of the interface module
The signature verification of Secure Boot significantly extends the startup time of the interface module. You can find time specifications in the Equipment Manual of the interface module, in the Technical specifications section.

LED display on the interface module

If the Secure Boot verification results in an invalid signature, the LEDs RUN, ERROR, and MAINT on the interface module will flash. In this case, you need to replace the interface module.

13.10 Safe operation of I/O modules

Device-specific security information and instructions for I/O modules can be found in the respective Equipment Manual.

13.10.1 Data integrity for I/O modules

Data integrity for I/O modules

In order to detect intentional or accidental changes to the data of an interface module and the assigned modules, the dynamic integrity check for I/O modules is introduced as of firmware version V2.0. You can also find out whether your I/O module supports the data integrity check in the Technical specifications section of the corresponding equipment manual.

Principle

The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as serial numbers, parameter settings, calibration data and I&M data of I/O modules. The interface module stores the checksums in the I&M4 data area.

You can find more information on the principle of data integrity and I&M4 data in the section Data integrity for interface modules (Page 139).

Spare parts scenario

The spare parts scenario is still ensured. This means that you can replace I/O modules with the same article number. For the "new" I/O module, the static data such as the serial number will change. Note that the replacement is therefore reflected in the following modified I&M4 data of the interface module:

- CHK_STATIC_SUBS
- CHK_OVERALL_SUBS
- CHK_OVERALL

You can find the structure of I&M data in the section Record structure for I&M data (Page 105).

13.10.2 Signed firmware update for I/O modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect internet source

Signed firmware update for I/O modules

Firmware updates for I/O modules as of firmware version V2.0 contain a digital signature. The digitally signed firmware update files are available for download on the Siemens Support Web page.

Principle, diagnostics alarms and remedies as for interface modules

The principle and diagnostics of the signed firmware update are the same for interface modules and I/O modules. The information in the section Signed firmware update for interface modules (Page 141) applies.

Safety-related shutdown of ET200AL standard modules

A

Introduction

The diagram below illustrates the fail-safe shutdown of ET 200AL standard modules.

In the configuration shown in the diagram below, all digital outputs that are operated with the 2L+ and 2M supply of the ET 200AL standard modules are switched to the safe OFF state. This step achieves the safety class SIL2/category 3/PLd.

Principle of operation

The higher-level safety relay (for example: 3SK1) disconnects the 2L+ and 2M supply. This switches all digital outputs operated with the 2L+ and 2M (switched) supply to the safe state. The digital outputs connected to the 1L+ and 1M (non-switched) supply are not intended for functional switching and therefore cannot be shut down safely.

There is no interaction between the outputs supplied by 1L+ and 2L+.

You can also integrate I/O modules that are operated solely at the supply 1L+ and 1M (non-switched) in the structure of your distributed I/O system. These I/O devices must be enabled as reaction-free modules. These I/O modules are not affected by a disconnection, they pass on the supply 2L+ and 2M (switched). The following figure shows this as an example using the DI, AI and AQ modules.

Schematic circuit diagram with 3SK1

The following figure shows a schematic circuit diagram with safety relay 3SK1.

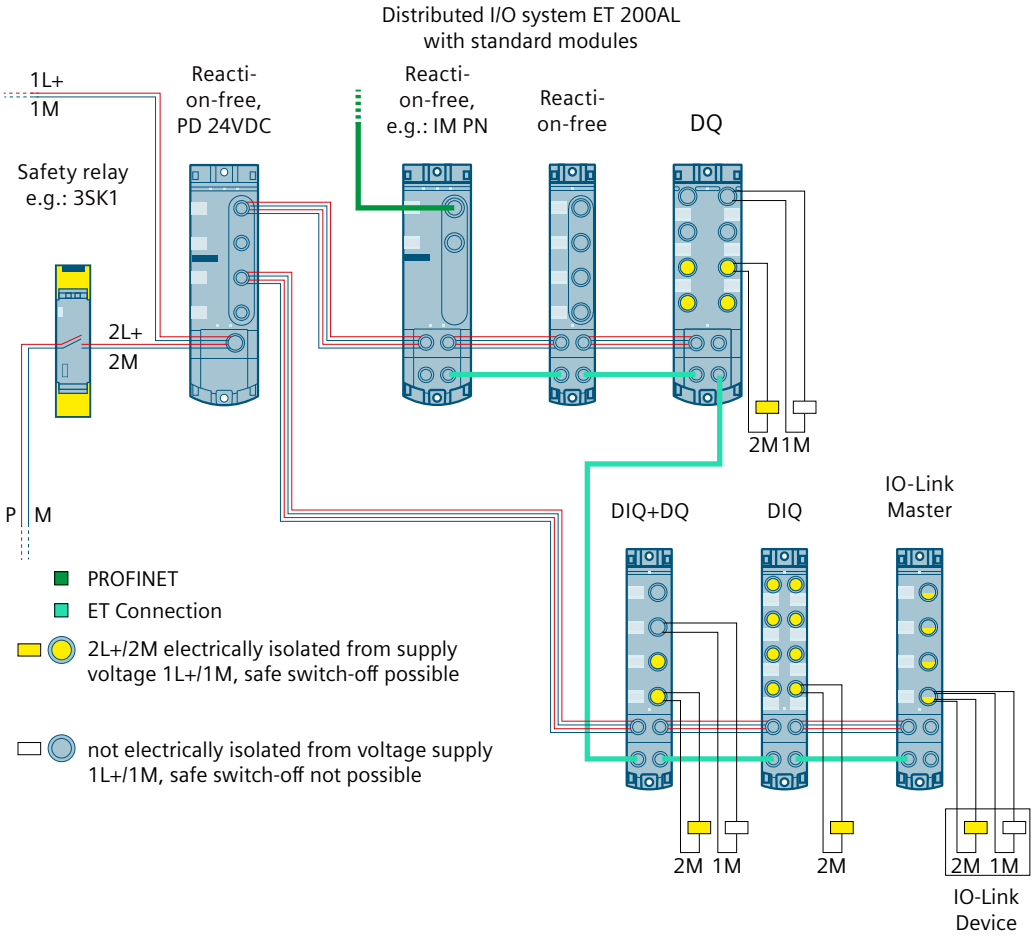


Figure 1-47 Higher-level safety circuit with safety relay

You can find an overview table with the article numbers of the I/O modules and other information in the FAQ on safety-related shutdown (https://support.industry.siemens.com/cs/us/en/view/39198632).

Planning

Note the following points when planning safety circuits.

WARNING

Note potential groups for safety-related shutdown
When a digital output is connected to a digital input, pay attention to the potential groups. Depending on the configuration, 1M and 2M can then be connected, which leads to elimination of the electrical isolation between 1L+ and 2L+.
The safety-related shutdown is not permitted if the electrical isolation is eliminated.

NOTE

Safe electrical isolation

Maintain safe galvanic isolation for voltages higher than SELV/PELV.

NOTE

Safety-related shutdown for the IO-Link master

For an IO-Link master with IO-Link Port Class B, safety-related shutdown is available for the additional supply (PIN 2 and PIN 5).

The other signals at the port are reaction-free.

Please note that the IO-Link device must have corresponding safety characteristics in order to use safety-oriented tripping.

Limits of the higher-level safety circuit

The ET 200AL standard modules do not fulfill any safety functions. The safety functions are executed by the safety relay in order to bring the system into a safe state.

Adjust the operation inspection interval of the safety switching device with a relay output to the safety class.

Take the following measures if energy that is not provided by the higher-level safety circuit is used to control the safety function.

Cover critical errors in the safety function that are not detected by the higher-level safety circuit (e.g. 3SK1) with suitable safety measures. The "diagnostics" must be performed indirectly via the controlled process.

Specifications for safety-relevant process data:

- Functionally safe
- Read via fail-safe inputs (e.g. F-DI)
- Fail-safe processing unit (e.g. F-CPU) for issuing commands
- Output through fail-safe outputs (e.g. F-DQ) to control the safety function

Requirements on the power supply

Operation requires a SELV/PELV power supply to limit overvoltages to L+ and M (24 V). This measure prevents possible errors from the power supply side at the same time.

Select the power supply according to the requirements of the respective operating instructions for the shutdown device and for the ET 200AL system.

You can find more information on safe SELV/PELV in the data sheets of the power supplies used.

FAQ

The information on the safety-related shutdown of standard modules refers to the status of the issue date. Read the up-to-date information on safety-related shutdown in this FAQ (https://support.industry.siemens.com/cs/us/en/view/39198632).

This FAQ specifies the SIMATIC standard modules that are suitable for a safety-related shutdown and a file with wiring examples.

Request German Technical Inspectorate report (Report no. SN89858T)

You can request copies of the German Technical Inspectorate report at the following address:

Siemens Aktiengesellschaft
Digital Industries
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg, Germany

Dimension drawings

B

2 module widths are available with the distributed I/O system.

The figure below shows the height and width of the modules. The depth of the modules ranges from 40 mm to 46 mm. Detailed information on the dimensions of the individual modules can be found in the manuals for the Interface modules (https://support.industry.siemens.com/cs/ww/en/ps/14246/man) and I/O modules (https://support.industry.siemens.com/cs/ww/en/ps/14247/man) in the section "Dimension drawing".

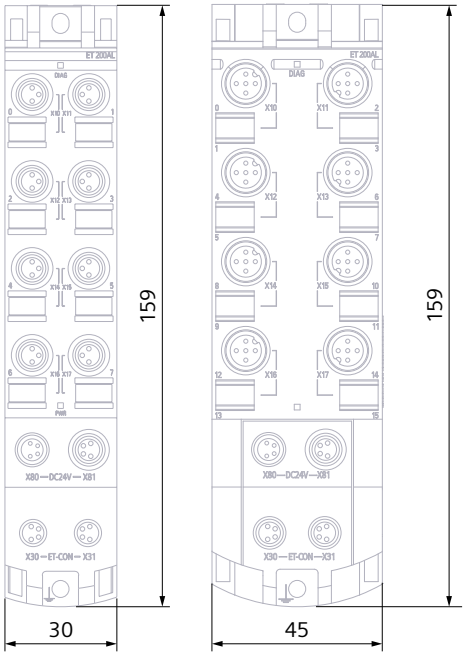


Figure 1-48 Module dimension drawings (front view)

Accessories/spare parts

C

C.1 Accessories/spare parts

Accessories for the ET 200AL distributed I/O system

Table 1-35 Accessories for ET-Connection

Designation	Length	Article number	
Cable		**Standard**	**PUR**
Bus cable for ET-Connection M8, pre-assembled on both sides with 2 x M8 connectors, 4-pin, shielded	0.19 m	6ES7194-2LH02-0AA0	6ES7194-2MH02-0AA0
	0.3 m	6ES7194-2LH03-0AA0	6ES7194-2MH03-0AA0
	1.0 m	6ES7194-2LH10-0AA0	6ES7194-2MH10-0AA0
	2.0 m	6ES7194-2LH20-0AA0	6ES7194-2MH20-0AA0
	5.0 m	6ES7194-2LH50-0AA0	6ES7194-2MH50-0AA0
	10.0 m	6ES7194-2LN10-0AA0	6ES7194-2MN10-0AA0
	15.0 m	6ES7194-2LN15-0AA0	6ES7194-2MN15-0AA0
Bus cable for ET-Connection M8, pre-assembled on both sides with 2 x M8 connectors, angled, 4-pin, shielded	0.3 m	6ES7194-2LH03-0AB0	6ES7194-2MH03-0AB0
	1.0 m	6ES7194-2LH10-0AB0	6ES7194-2MH10-0AB0
	2.0 m	6ES7194-2LH20-0AB0	6ES7194-2MH20-0AB0
	5.0 m	6ES7194-2LH50-0AB0	6ES7194-2MH50-0AB0
	10.0 m	6ES7194-2LN10-0AB0	6ES7194-2MN10-0AB0
	15.0 m	6ES7194-2LN15-0AB0	6ES7194-2MN15-0AB0
Bus cable for ET-Connection M8, pre-assembled on one side with 1 x M8 connector, 4-pin, shielded	2.0 m	6ES7194-2LH20-0AC0	6ES7194-2MH20-0AC0
	5.0 m	6ES7194-2LH50-0AC0	6ES7194-2MH50-0AC0
	10.0 m	6ES7194-2LN10-0AC0	6ES7194-2MN10-0AC0
	15.0 m	6ES7194-2LN15-0AC0	6ES7194-2MN15-0AC0
Connecting cable for bus cable ET-Connection M8, both ends assembled with 2x M8 socket, 4-pin, shielded	0.2 m	6ES7194-2LH02-0AD0	6ES7194-2MH02-0AD0
Connector			
M8 connector for ET-Connection, 4-pin, shielded		6ES7194-2AB00-0AA0	

Table 1-36 Accessories for power supply M8

Designation	Length	Article number	
Cable		**Standard**	**PUR**
Power cable M8, pre-assembled on both sides with M8 connector and M8 socket, 4-pin	0.19 m	6ES7194-2LH02-1AA0	6ES7194-2MH02-1AA0
	0.3 m	6ES7194-2LH03-1AA0	6ES7194-2MH03-1AA0
	1.0 m	6ES7194-2LH10-1AA0	6ES7194-2MH10-1AA0
	2.0 m	6ES7194-2LH20-1AA0	6ES7194-2MH20-1AA0
	5.0 m	6ES7194-2LH50-1AA0	6ES7194-2MH50-1AA0
	10.0 m	6ES7194-2LN10-1AA0	6ES7194-2MN10-1AA0
	15.0 m	6ES7194-2LN15-1AA0	6ES7194-2MN15-1AA0
Power cable M8, pre-assembled on both sides with	0.3 m	6ES7194-2LH03-1AB0	6ES7194-2MH03-1AB0

Designation	Length	Article number	
angled M8 connector and angled M8 socket, 4-pin	1.0 m	6ES7194-2LH10-1AB0	6ES7194-2MH10-1AB0
	2.0 m	6ES7194-2LH20-1AB0	6ES7194-2MH20-1AB0
	5.0 m	6ES7194-2LH50-1AB0	6ES7194-2MH50-1AB0
	10.0 m	6ES7194-2LN10-1AB0	6ES7194-2MN10-1AB0
	15.0 m	6ES7194-2LN15-1AB0	6ES7194-2MN15-1AB0
Power cable M8, pre-assembled on one side with M8 socket, 4-pin	2.0 m	6ES7194-2LH20-1AC0	6ES7194-2MH20-1AC0
	5.0 m	6ES7194-2LH50-1AC0	6ES7194-2MH50-1AC0
	10.0 m	6ES7194-2LN10-1AC0	6ES7194-2MN10-1AC0
	15.0 m	6ES7194-2LN15-1AC0	6ES7194-2MN15-1AC0
Connector			
M8 power connector, pin insert, 4-pin		6ES7194-2AA00-0AA0	
M8 power connector, socket insert, 4-pin		6ES7194-2AC00-0AA0	

Table 1-37 Accessories for power supply M12-L

Designation	Length	Article number
Cable		
M12 CONNECTING CABLE, L-CODED M12 L-cod 4-pol+FE st/st f/m PVC M12 L-cod 4+FE PVC 2,5 mm² Connection cable, straight socket on straight pin, 16 A	1.5 m	Company Harting: 21 33 A7A 8524 015
	5.0 m	Company Harting: 21 33 A7A 8524 050
	10.0 m	Company Harting: 21 33 A7A 8524 100
M12 CONNECTING CABLE, L-CODED M12 L-cod 4-pol+FE st/- f/- PVC M12 L-cod 4+FE PVC 2,5 mm² Connection cable, straight socket on open end, 16 A	1.5 m	Company Harting: 21 33 A70 0524 015
	5.0 m	Company Harting: 21 33 A70 0524 050
	10.0 m	Company Harting: 21 33 A70 0524 100

Table 1-38 M12 connector

Designation		Article number
Non-preassembled connectors for X1 DP1 (pin)		
PROFIBUS M12 plug connector 180° with female insert		6GK1905-0EB00
PROFIBUS M12 plug connector FastConnect 180° with female insert		6GK1905-0EB10
PROFIBUS M12 plug connector, angled with female insert		3RK1902-1DA00
Non-preassembled connectors for X1 DP2 (socket)		
PROFIBUS M12 plug connector 180° with pin insert		6GK1905-0EA00
PROFIBUS M12 plug connector FastConnect 180° with pin insert		6GK1905-0EA10
PROFIBUS M12 plug connector angled with pin insert		3RK1902-1BA00
Non-preassembled connectors for X1 P1R PN (LAN) and X1 P2R PN (LAN) socket		
PROFINET M12 plug connector d-coded with FastConnect connection technology, 180	1 unit/ pack	6GK1901-0DB10-6AA0
	8 units/ pack	6GK1901-0DB10-6AA8
PROFINET M12 plug connector, D-coded with fast connect technology 180°	1 unit/ pack	6GK1901-0DB20-6AA0
	8 units/ pack	6GK1901-0DB20-6AA8
PROFINET M12 plug connector, D-coded, angled		3RK1902-2DA00

Table 1-39 Non-preassembled cable M12

Designation	Article number
Non-preassembled cable for X1 DP1 and X1 DP2	
PROFIBUS FC Cable	
FC Standard Cable	6XV1830-0EH10
FC Trailing Cable	6XV1830-3EH10
FC Food Cable (PE sheath)	6XV1830-0GH10
FC Robust Cable (PUR sheath)	6XV1830-0JH10
FC FRNC Cable (FRNC sheath)	6XV1830-0LH10
FC Underground Cable	6XV1830-3FH10
Festoon Cable GP (PVC sheath)	6XV1830-3GH10
FC Flexible Cable GP (PUR sheath)	6XV1831-2K
Non-preassembled connectors for X1 P1R PN (LAN) and X1 P2R PN (LAN)	
PROFIBUS FC Cable	
FC Standard Cable	6XV1840-2AH10
FC TP Trailing Cable	6XV1840-3AH10
FC TP Trailing Cable GP	6XV1870-2D
FC TP Marine Cable	6XV1840-4AH10
FC TP Torsion Cable	6XV1870-2F
FC TP Flexible Cable GP (PVC sheath)	6XV1870-2B
FC TP FRNC Cable (FRNC sheath)	6XV1871-2F
FC TP Food Cable (PE sheath)	6XV1871-2L
FC TP Festoon Cable GP (PVC sheath)	6XV1871-2S

Table 1-40 Pre-assembled cable M12

Designation		Article number
Pre-assembled cable for X1 DP1 and X1 DP2		
PROFIBUS M12 connecting cable, trailing cable, pre-assembled on both sides with PROFIBUS M12 connectors, 180° (one end with socket, one end with pin)	0.3 m	6XV1830-3DE30
	0.5 m	6XV1830-3DE50
	1.0 m	6XV1830-3DH10
	1.5 m	6XV1830-3DH15
	2.0 m	6XV1830-3DH20
	3.0 m	6XV1830-3DH30
	5.0 m	6XV1830-3DH50
	10.0 m	6XV1830-3DN10
	15.0 m	6XV1830-3DN15
PROFIBUS M12 connecting cable, trailing cable, pre-assembled on both sides with PROFIBUS M12 connectors, angled (one end with socket, one end with pin)	1.5 m	6XV1830-3DH15-0SB0
	2.0 m	6XV1830-3DH20-0SB0
	3.0 m	3RK1902-1NB30
	5.0 m	3RK1902-1NB50
	10.0 m	3RK1902-1NC10
	15.0 m	6XV1830-3DN15-0SB0
Pre-assembled cable for X1 P1R PN (LAN) and X1 P2R PN (LAN)		
PROFINET M12 connecting cable, trailing cable, pre-assembled on both ends with M12 connectors 180° (pin)	0.3 m	6XV1870-8AE30
	0.5 m	6XV1870-8AE50
	1.0 m	6XV1870-8AH10

Designation		Article number
PROFINET M12 connecting cable, trailing cable, pre-assembled on both ends with M12 connectors 180° (pin)	1.5 m	6XV1870-8AH15
	2.0 m	6XV1870-8AH20
	3.0 m	6XV1870-8AH30
	5.0 m	6XV1870-8AH50
	10.0 m	6XV1870-8AN10
	15.0 m	6XV1870-8AN15
PROFINET M12 connecting cable, trailing cable, pre-assembled on both ends with M12 connectors, angled (pin)	0.3 m	6XV1870-8AE30-0SB0
	0.5 m	6XV1870-8AE50-0SB0
	1.0 m	6XV1870-8AH10-0SB0
	1.5 m	6XV1870-8AH15-0SB0
	2.0 m	6XV1870-8AH20-0SB0
	3.0 m	3RK1902-2NB30
	5.0 m	3RK1902-2NB50
	10.0 m	3RK1902-2NC10
	15.0 m	6XV1870-8AN15-0SB0
PROFINET M12 connecting cable, trailing cable, pre-assembled on both sides with PROFIBUS M12 connectors, angled (one end with pin, one end open)	3.0 m	3RK1902-2HB30
	5.0 m	3RK1902-2HB50
	10.0 m	3RK1902-2HC10
PROFINET M12 connecting cable, trailing cable, pre-assembled on one end with M12 connectors 180° (pin), other end with RJ45 plug 145°	2.0 m	6XV1871-5TH20
	3.0 m	6XV1871-5TH30
	5.0 m	6XV1871-5TH50
	10.0 m	6XV1871-5TN10
	15.0 m	6XV1871-5TN15

Table 1-41 Y cable

Designation		Article number
SIMATIC DP, Y-cable for distributed I/Os for double connection of I/Os using single cable, 5-pin, M12	0.2 m	6ES7194-6KA00-0XA0
SIMATIC DP, Y-cable, for fail-safe ET 200 distributed I/O, IP 65/67, for connection of single-channel sensors (1oo1 evaluation) 5-pin M12	0.2 m	6ES7194-6KB00-0XA0
SIMATIC DP, Y-cable, for fail-safe distributed I/O ET 200, IP 65/67, for common connection of an F-DQ and F-DI channel by means of 8-pin M12 socket	0.2 m	6ES7194-6KC00-0XA0

Table 1-42 Additional accessories

Designation	Article number
Identification labels 10 x 5 mm RAL9016, composed of 200 labels on frames, per frame 40 labels	6ES7194-2BA00-0AA0
Identification labels 10 x 5 mm RAL1018, yellow, consisting of 200 labels on frames, 40 labels per frame	6ES7194-2BB00-0AA0
Identification labels 10 x 7 mm, yellow, consisting of 816 labels on frames, 48 labels per frame (for eCoding plug connectors)	6ES7194-6HA00-0AA0
Sealing cap M8 for modules IP67	3RK1901-1PN00
Sealing cap M12 for modules IP67	3RX9802-0AA00
Bus connection plug PROFIBUS M12, pin insert, 5 units	6GK1905-0EC00
Stripping Tool for ET-Connection	6ES7194-2KA00-0AA0

Designation	Article number
Stripping Tool for PROFINET	6GK1901-1GA00
Stripping Tool for PROFIBUS	6GK1905-6AA00
eCoding plug connector, stores the F-destination addresses and F-source addresses for F-modules	6ES7194-6KB01-0AA0

Online catalog

Other article numbers for the ET 200AL distributed I/O system can be found on the Internet (https://mall.industry.siemens.com) in the online catalog and the online order system.

C.2 UL-approved cables

In combination with the UL-approved cables for the power supply and the connection of inputs/outputs, the SIMATIC ET 200AL distributed I/O devices meet UL approval. Siemens has UL-approved cables for these applications in the product portfolio.

C.3 Cables

Cables for ET-Connection PVC cable and PUR cable

The cables for ET-Connection are available in the following versions and lengths:

- Bus cable (4-wire), pre-assembled on both sides with 2 M8 connectors, 4-pole, shielded
  - available lengths: 0.19 m, 0.3 m, 1 m, 2 m, 5 m, 10 m, 15 m
- Bus cable (4-wire), pre-assembled on both sides with 2 M8 connectors, angled, 4-pole, shielded
  - available lengths: 0.3 m, 1 m, 2 m, 5 m, 10 m, 15 m
- Bus cable (4-wire), pre-assembled on one side 1x M8 connector, 4-pole, shielded
  - available lengths: 2 m, 5 m, 10 m, 15 m

The following table shows the technical properties of the bus cable ET-Connection PVC cable.

Table 1-43 Cables for ET-Connection, PVC cable

General information	
Product type designation	BUS CABLE ET-CONNECTION
Function	To connect ET-CONNECTION devices with degree of protection IP65/IP67
Degree of protection and protection class	
IP65	Yes
IP67	Yes
Ambient conditions	
Ambient temperature during mounting	
minimum	-30 °C
maximum	80 °C

* = Applies to cable lengths up to 10 m.

General information	
Storage/transport temperature	
Ambient temperature during transport and storage	
minimum	-40 °C
maximum	80 °C
Cables	
Cable designation	2Y(ST)CY 1x4x0.5/1.0-100-GN
Number of electrical wires	4
Design of shielding	Overlapped aluminum-lined sheet, coated with shielding made of tin plated copper wires
Outside diameter of the inner conductor	0.5 mm
Outside diameter of the wire insulation	1.0 mm
Outside diameter of the cable sheath	5 mm
Number of bending cycles	1000000; Trailing-chain suitable for 1 million bending cycles with a bending radius of 100 mm, a velocity of 4 m/s and an acceleration of 4 m/s²
Permissible bending radius	
One time bending, min.	20 mm
Multiple bending, min.	40 mm
Constant bending	100 mm
Color of the cable sheath	Green
Color of the wire insulation of the data wires	White, yellow, blue, orange
Weight per length	34 kg/km
Mechanics/material	
Type of cable outlet	180° cable outlet 90° cable outlet (with angled connectors)
Number of connectors	1 or 2
Connector housing material	Metal/plastic
Wire insulation material	PE
Cable sheath material	PVC
Material property halogen free	No
Material property silicon free	Yes

* = Applies to cable lengths up to 10 m.

The following table shows the technical properties of the bus cable ET-Connection, PUR cable.

Table 1-44 Cables for ET-Connection, PUR cable

General information	
Product type designation	BUS CABLE ET-CONNECTION, PUR CABLE
Function	To connect ET-CONNECTION devices with degree of protection IP65/IP67
Degree of protection and protection class	
IP65	Yes
IP67	Yes
Ambient conditions	
Ambient temperature during mounting	
minimum	-30 °C

* = Applies to cable lengths up to 10 m.

General information	
maximum	80 °C
Storage/transport temperature	
Ambient temperature during transport and storage	
minimum	-40 °C
maximum	80 °C
Cables	
Cable designation	2Y(ST)C11Y 2x2x0.5/1.0-100-GN
Number of electrical wires	4
Design of shielding	Overlapped aluminum-lined sheet, coated with shielding made of tin plated copper wires
Outside diameter of the inner conductor	0.5 mm
Outside diameter of the wire insulation	1.0 mm
Outside diameter of the cable sheath	5 mm
Number of bending cycles	1000000*; trailing-chain suitable for 1 million bending cycles with a bending radius of 100 mm, a velocity of 4 m/s and an acceleration of 4 m/s²
Permissible bending radius	
One time bending, min.	20 mm
Multiple bending, min.	40 mm
Constant bending	100 mm
Color of the cable sheath	Green
Color of the wire insulation of the data wires	White, yellow, blue, orange
Weight per length	34 kg/km
Mechanics/material	
Type of cable outlet	180° cable outlet 90° cable outlet (with angled connectors)
Number of connectors	1 or 2
Connector housing material	Metal/plastic
Wire insulation material	PE
Cable sheath material	PUR
Material property halogen free	Yes
Material property silicon free	Yes

* = Applies to cable lengths up to 10 m.

Connection cable for ET-Connection PVC cable and PUR cable

You can use the connection cable between two cables for ET-Connection.

Typical applications for using connection cable for ET-Connection are:

- Combination of individual cable lengths by joining multiple pre-assembled cables for ET-Connection.
- Selective installation of disconnection points of cables for ET-Connection (for simple changing of cables and cable sections, e.g. with trailing-cable applications).

You can use a maximum of two connection cables between the two modules.
The length of the cables for ET-Connection is limited to maximum 10 m when connection cables are used.

The connection cable for ET-Connection is available in the following design:

- Connection cable for bus cable ET-Connection M8, both ends assembled with 2x M8 socket, 4-pole, shielded, length 0.2 m

The following table shows the technical properties of the connection cable for ET-Connection PVC cable.

Table 1-45 Connection cables for ET-Connection, PVC cable

General information	
Product type designation	Connection cable for bus cable ET-CONNECTION, cable 0.2 M
Function	To connect two bus cables ET-CONNECTION
Degree of protection and protection class	
IP65	Yes
IP67	Yes
Ambient conditions	
Ambient temperature during mounting	
minimum	-30 °C
maximum	80 °C
Storage/transport temperature	
Ambient temperature during transport and storage	
minimum	-40 °C
maximum	80 °C
Cables	
Cable designation	2Y(ST)CY 1x4x0.5/1.0-100-GN
Number of electrical wires	4
Design of shielding	Overlapped aluminum-lined sheet, coated with shielding made of tin plated copper wires
Cable length	0.2 m
Outside diameter of the inner conductor	0.5 mm
Outside diameter of the wire insulation	1.0 mm
Outside diameter of the cable sheath	5 mm
Permissible bending radius	
One time bending, min.	20 mm
Multiple bending, min.	40 mm
Constant bending	100 mm
Color of the cable sheath	Green
Color of the wire insulation of the data wires	White, yellow, blue, orange
Weight per length	34 kg/km
Mechanics/material	
Type of cable outlet	180° cable outlet
Connector housing material	Metal/plastic
Wire insulation material	PE
Cable sheath material	PVC
Material property halogen free	No
Material property silicon free	Yes

The following table shows the technical properties of the connection cable for ET-Connection, PUR cable.

Table 1-46 Connection cables for ET-Connection, PUR cable

General information	
Product type designation	Connection cable for bus cable ET-CONNECTION, PUR cable 0.2 M
Function	To connect two bus cables ET-CONNECTION
Degree of protection and protection class	
IP65	Yes
IP67	Yes
Ambient conditions	
Ambient temperature during mounting	
minimum	-30 °C
maximum	80 °C
Storage/transport temperature	
Ambient temperature during transport and storage	
minimum	-40 °C
maximum	80 °C
Cables	
Cable designation	2Y(ST)C11Y 2x2x0.5/1.0-100-GN
Number of electrical wires	4
Design of shielding	Overlapped aluminum-lined sheet, coated with shielding made of tin plated copper wires
Cable length	0.2 m
Outside diameter of the inner conductor	0.5 mm
Outside diameter of the wire insulation	1.0 mm
Outside diameter of the cable sheath	5 mm
Permissible bending radius	
One time bending, min.	20 mm
Multiple bending, min.	40 mm
Constant bending	100 mm
Color of the cable sheath	Green
Color of the wire insulation of the data wires	White, yellow, blue, orange
Weight per length	34 kg/km
Mechanics/material	
Type of cable outlet	180° cable outlet
Connector housing material	Metal/plastic
Wire insulation material	PE
Cable sheath material	PUR
Material property halogen free	Yes
Material property silicon free	Yes

Cables for voltage supply PVC cable and PUR cable

The cables for the power supply are available in the following versions and lengths:

- Power cable (4-wire), pre-assembled on both sides with a 4-pole M8 pin connector/socket connector
  - available lengths: 0.19 m, 0.3 m, 1 m, 2 m, 5 m, 10 m, 15 m
- Power cable (4-wire), pre-assembled on both sides with a 4-pole M8 pin connector/socket connector, angled
  - available lengths: 0.3 m, 1 m, 2 m, 5 m, 10 m, 15 m
- Power cable (4-wire), pre-assembled on one side with 1x M8 socket connector
  - available lengths: 2 m, 5 m, 10 m, 15 m

The following table shows the technical properties of the power supply line PVC cable

Table 1-47 Cables for power supply, PVC cable

General information	
Product type designation	POWER CABLE M8
Function	For connection of ET 200AL for 24 V DC power supply
Degree of protection and protection class	
IP65	Yes
IP67	Yes
Ambient conditions	
Ambient temperature during mounting	
minimum	-30 °C
maximum	80 °C
Storage/transport temperature	
Ambient temperature during transport and storage	
minimum	-40 °C
maximum	80 °C
Cables	
Cable designation	4 Li9Y 0.50 mm² Y
Number of electrical wires	4
Outside diameter of the inner conductor	0.8 mm
Outside diameter of the wire insulation	1.46 mm
Outside diameter of the cable sheath	5.2 mm
Number of bending cycles	2500000; Trailing-chain suitable for 2.5 million bending cycles with a bending radius of 52 mm, a speed of 3 m/s² and an acceleration of 10 m/s²
Permissible bending radius	
One time bending, min.	26 mm
Multiple bending, min.	52 mm
Constant bending	52 mm
Color of the cable sheath	Gray
Color of the wire insulation of the power wires	White, brown, blue black
Weight per length	44 kg/km
Mechanics/material	

General information	
Type of cable outlet	180° cable outlet 90° cable outlet (with angled connectors)
Number of connectors	1 or 2
Connector housing material	Plastic
Wire insulation material	PP
Cable sheath material	PVC
Material property halogen free	No
Material property silicon free	Yes

The following table shows the technical properties of the power supply, PUR cable

Table 1-48 Cables for power supply, PUR cable

General information	
Product type designation	POWER CABLE M8, PUR CABLE
Function	For connection of ET 200AL for 24 V DC power supply
Degree of protection and protection class	
IP65	Yes
IP67	Yes
Ambient conditions	
Ambient temperature during mounting	
minimum	-30 °C
maximum	80 °C
Storage/transport temperature	
Ambient temperature during transport and storage	
minimum	-40 °C
maximum	80 °C
Cables	
Cable designation	LIF9Y11YFHF 4x0.50 mm²
Number of electrical wires	4
Outside diameter of the inner conductor	1 mm
Outside diameter of the wire insulation	1.46 mm
Outside diameter of the cable sheath	5.1 mm
Number of bending cycles	2000000; trailing-chain suitable for 2 million bending cycles with a bending radius of 51 mm, a velocity of 5 m/s and an acceleration of 5 m/s²
Permissible bending radius	
One time bending, min.	26 mm
Multiple bending, min.	51 mm
Constant bending	51 mm
Color of the cable sheath	Gray
Color of the wire insulation of the power wires	White, brown, blue black
Weight per length	44 kg/km
Mechanics/material	
Type of cable outlet	180° cable outlet 90° cable outlet (with angled connectors)
Number of connectors	1 or 2

General information	
Connector housing material	Plastic
Wire insulation material	PP
Cable sheath material	PE-PUR
Material property halogen free	Yes
Material property silicon free	Yes

C.4 Connectors

The following table shows the technical specifications of the user-configurable connectors.

The following table shows the technical specifications of the connection plug for the ET-CONNECTION connection.

Article number	6ES7194-2AB00-0AA0
General information	
Product type designation	Connection plug
Product description	M8 plug connector with high degree of protection, 4-pin, metal version
Suitability for use	for connecting ET-CONNECTION nodes (e.g. SIMATIC ET 200AL) in degree of protection IP65 / 67
Degree and class of protection	
IP degree of protection	IP65/67
Ambient conditions	
Ambient temperature during assembly, min.	-30 °C
Ambient temperature during assembly, max.	80 °C
Ambient temperature during storage/transportation	
• min.	-40 °C
• max.	80 °C
Mechanics/material	
Outgoing feeder type	180° cable outlet
Material of housing	metal
Dimensions	
Width	14 mm
Depth	47 mm

The following table shows the technical specifications of the power connector with female contact insert for the 24 V DC power supply.

Article number	6ES7194-2AC00-0AA0
General information	
Product type designation	Power connector
Product description	M8 plug connector with high degree of protection, socket insert, 4-pin, plastic version
Suitability for use	For connection to ET 200AL for 24 V DC power supply
Degree and class of protection	
IP degree of protection	IP65/67
Ambient conditions	
Ambient temperature during assembly, min.	-30 °C
Ambient temperature during assembly, max.	85 °C
Ambient temperature during storage/transportation	
• min.	-40 °C
• max.	85 °C

Article number	6ES7194-2AC00-0AA0
connection method / header	
Connector type	M8, 4-pole
Type of electrical connection for mains supply line	Screw terminals
• connectable cable cross-section for mains supply line, min.	0.14 mm²
• connectable cable cross-section for mains supply line, max.	0.5 mm²
• Connectable conductor cross-section for AWG cables, min.	26
• Connectable conductor cross-section for AWG cables, max.	20
Suitable for cable diameter, min.	4 mm
usable for cable diameter, max.	5.5 mm
Mechanics/material	
Outgoing feeder type	180° cable outlet
Material of housing	plastic
Dimensions	
Width	14 mm
Depth	47 mm

The following table shows the technical specifications of the power connector with male contact insert for the 24 V DC power supply.

Article number	6ES7194-2AA00-0AA0
General information	
Product type designation	Power connector
Product description	M8 plug connector with high degree of protection, 4-pin, plastic version
Suitability for use	For connection to ET 200AL for 24 V DC power supply
Degree and class of protection	
IP degree of protection	IP65/67
Ambient conditions	
Ambient temperature during assembly, min.	-30 °C
Ambient temperature during assembly, max.	85 °C
Ambient temperature during storage/transportation	
• min.	-40 °C
• max.	85 °C
connection method / header	
Connector type	M8, 4-pole
Type of electrical connection for mains supply line	Screw terminals
• connectable cable cross-section for mains supply line, min.	0.14 mm²
• connectable cable cross-section for mains supply line, max.	0.5 mm²
• Connectable conductor cross-section for AWG cables, min.	26

Article number	6ES7194-2AA00-0AA0
• Connectable conductor cross-section for AWG cables, max.	20
Suitable for cable diameter, min.	4 mm
usable for cable diameter, max.	5.5 mm
Mechanics/material	
Outgoing feeder type	180° cable outlet
Material of housing	plastic
Dimensions	
Width	14 mm
Depth	47 mm

C.5 Pin assignment and core color

Pin assignment of the sockets for ET-Connection

The tables below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

Table 1-49 Pin assignment for ET-Connection (interface modules)

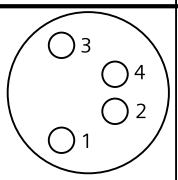
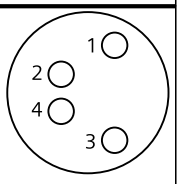
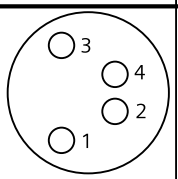
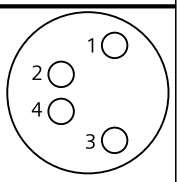
Pin	Assignment		Assignment of the core color of the bus cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection1)	X31 socket (ET-Connection2)		X30	X31
1	RXP	RXP	yellow		
2	TXP	TXP	white		
3	TXN	TXN	blue		
4	RXN	RXN	orange		
Shield-ing	Functional earth FE		-		

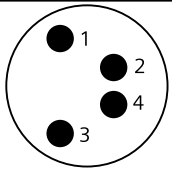
Table 1-50 Pin assignment for ET-Connection (I/O modules)

Pin	Assignment		Assignment of the core color of the bus cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	yellow		
2	RXP	TXP	white		
3	RXN	TXN	blue		
4	TXN	RXN	orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment for infeed of the supply voltage.

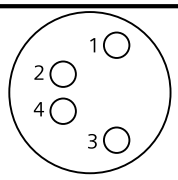
Table 1-51 Pin assignment of the supply voltage connector

Pin	Assignment **X80 connector (power input)**	Assignment of the core color of the power cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	brown	
2	Ground 2M (switched)	white	
3	Ground 1M (non-switched)	blue	
4	Load voltage 2L+ (switched)	black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment for loop-through of the supply voltage.

Table 1-52 Pin assignment of the supply voltage socket

Pin	Assignment **X81 Socket (power output)**	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	brown	
2	Ground 2M (switched)	white	
3	Ground 1M (non-switched)	blue	
4	Load voltage 2L+ (switched)	black	

SIMATIC ET 200AL data

D

The EU Data Act, a key component of the European data strategy, entered into force on 11 January 2024.

The following information provides an overview of the data that is generated by the SIMATIC ET 200AL automation system and accessible to you.

D.1 Data of the interface and I/O modules

Type, format, and estimated scope of data that the product is capable of generating

Type of data	Formats	Estimated scope
Process data (input and output data, states, alarms)	Numeric formats, binary formats	Cyclic processing Depending on application
Configuration and parameter data (upload to PG/PC)	Binary formats, string formats	Depending on application
Diagnostics data, service data	Binary formats	Depending on application Less than 100 bytes per diagnostic event; several kilobytes of service data
Fieldbus* metadata: I&M data, log data, statistics data	Binary formats, string formats	Approximately 100 bytes per read-out data record

* PROFIBUS, PROFINET, EtherNet/IP, Modbus TCP (only for interface modules as MultiFieldbus devices)

Continuous and real-time data generation

The interface and I/O modules are able to generate data continuously and in real time. Data acquisition takes place continuously throughout the entire operation. The cycle time is specified by the higher-level CPU.

Data storage and storage duration

Local data storage

The interface and I/O modules store data in integrated memory areas.

Local data storage	Storage capacity	Storage duration
Retentive memory (for I&M data, configuration and parameter data*, service data)	Up to 16 MB for interface modules 1 to 2 MB for I/O modules	Permanent
Work memory (for process data, diagnostics data, fieldbus metadata, configuration and parameter data, service data)	Up to 1 MB for interface modules Several 100 KB for I/O modules	During operation of the module

* only interface modules as MultiFieldbus devices and IO-Link masters

Data access/retrieval, terms of use, and quality of service

Type of data	Access/retrieval via	Terms of use	Quality of service*
Process data (input and output data, states, alarms)	CPU TIA Portal SIMATIC Automation Tool PRONETA S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Via fieldbus without authentication Via CPU (https://support.industry.siemens.com/cs/de/de/view/59193101-/en)	Prioritization of control tasks over data access Standard fieldbus transmission mechanisms Data throughput rates up to 1 Gbps via PROFINET
Configuration and parameter data (upload to PG/PC)	TIA Portal (via CPU) S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Via fieldbus without authentication Via CPU (https://support.industry.siemens.com/cs/de/de/view/59193101-/en)	Standard fieldbus transmission mechanisms
Diagnostics data, service data	CPU TIA Portal SIMATIC Automation Tool PRONETA S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Via fieldbus without authentication Via CPU (https://support.industry.siemens.com/cs/de/de/view/59193101-/en)	Standard fieldbus transmission mechanisms
Fieldbus metadata: I&M data, log data, statistics data	CPU TIA Portal SIMATIC Automation Tool PRONETA S7-PCT (for IO-Link masters) MFCT (for interface modules as MultiFieldbus devices)	Via fieldbus without authentication Via CPU (https://support.industry.siemens.com/cs/de/de/view/59193101-/en)	Standard fieldbus transmission mechanisms

* "Quality of service" refers to the ability of the interface, power supply, and I/O modules to manage network resources efficiently and to ensure that specific performance requirements for data transmission are met.

Deletion of data from interface and I/O modules

Interface modules

To delete all data from the data memories of the interface module, the "Reset to factory settings" function is available.

The IM can be reset to factory settings using any of the following:

- TIA Portal
- SIMATIC Automation Tool
- MultiFieldbus Configuration Tool (MFCT)
- PRONETA

I/O modules

The data of an IO-Link master can be deleted using S7-PCT by executing the "Reset to factory settings" function.

For all other I/O modules, no delete function is available.

More information

You can find more information on deleting data in the "Securely removing data (Page 137)" and "Restoring the factory settings (Page 111)" sections.

SIEMENS

SIMATIC

ET 200AL
IO-Link I/O modules

System Manual

08/2025
A5E48755395-AD

Introduction 1
Safety instructions 2
New features/functions 3
System overview 4
Application planning 5
Mounting 6
Connecting 7
Configuring 8
Commissioning 9
Maintenance 10
Technical specifications 11
Industrial cybersecurity 12
Safety-related shutdown of ET 200AL IO-Link modules A
Dimension drawings B
Accessories/spare parts C
SIMATIC ET 200AL IO-Link I/O modules data D

Table of contents

1 Introduction 5

1.1 SiePortal 7

1.2 Information classes ET 200AL IO-Link I/O Module 7

1.3 Basic tools 8

1.4 S7 Port Configuration Tool (S7-PCT) 10

1.5 SIMATIC Technical Documentation 11

2 Safety instructions 13

2.1 Warnings in this document 13

2.2 Safety-related symbols for IP65/IP67 modules 13

2.3 Intended use 14

2.4 Changes to the device and spare parts 14

2.5 Target group and personnel qualifications 14

2.6 Personal protective equipment 15

2.7 Working on electrical parts 15

2.8 Residual risks 15

2.8.1 Live parts 15

2.8.2 Conductive pollution 16

2.8.3 Overheating 16

2.8.4 Uncontrolled movements 17

2.8.5 Unsafe operating states 17

2.9 Behavior in case of emergency 17

2.10 Material damage 17

2.10.1 Transport and storage 17

2.10.2 Installation and connection 18

3 New features/functions 19

4 System overview 20

4.1 System overview 20

4.2 What are ET 200AL IO-Link I/O modules? 20

4.3 Components 22

5 Application planning 23

5.1 Hardware configuration 23

5.2 Configuration of IO-Link I/O modules 23

6 Mounting 26
6.1 Basics 26
6.2 Mounting modules 27

7 Connecting 30
7.1 Rules and regulations for operation 30
7.2 Operation of the IO-Link I/O modules on a grounded/ungrounded infeed 32
7.3 Electrical configuration of the IO-Link I/O modules 37
7.4 Connecting IO-Link I/O modules to functional ground 39
7.4.1 Mounting IO-Link I/O modules on a conductive surface 39
7.4.2 Mounting IO-Link I/O modules on a non-conductive surface 40
7.5 Wiring 41
7.6 Marking of IO-Link I/O modules 44
7.6.1 Factory markings 44
7.6.2 Optional markings 45
7.6.3 Mounting identification labels 46

8 Configuring 47
8.1 Requirements 47
8.2 IODD and Port Configuration Tool - S7-PCT 47

9 Commissioning 50
9.1 Startup of the IO-Link I/O module 50

10 Maintenance 51
10.1 Replacing modules 51
10.2 Firmware update 52
10.3 Resetting a module 53
10.4 Maintaining/cleaning the modules 54

11 Technical specifications 56
11.1 Markings and approvals 56
11.2 Certificates 58
11.3 Standards and requirements 58
11.4 Electromagnetic compatibility 59
11.5 Transport and storage conditions 61
11.6 Mechanical and climatic ambient conditions 61
11.7 Details on insulation, protection class, degree of protection and rated voltage 62

12 Industrial cybersecurity 64
12.1 Cybersecurity information 64
12.2 Security update notification 65
12.3 Basic information on industrial cybersecurity 65
12.3.1 Definition of industrial cybersecurity 65
12.3.2 Objectives of industrial cybersecurity 65
12.4 Integrated security concept and security strategies 66
12.4.1 Comprehensive security concept "Defense in Depth" 66
12.4.2 Security management 67
12.5 Operational application environment and security assumptions 69
12.5.1 Intended use 69
12.5.2 Requirements for the operational application environment and security assumptions 69
12.6 Security properties of the devices 71
12.7 Secure operation of the system 71
12.7.1 Hardening measures 71
12.7.2 Secure configuration 71
12.7.3 Handling of sensitive data 71
12.7.4 Regular firmware updates 72
12.7.5 Notifications about security vulnerabilities (Siemens Security Advisories) 72
12.7.6 Data backup 73
12.7.7 Security checks 73
12.7.8 Secure decommissioning 73
12.7.8.1 Securely removing data 73
12.7.8.2 Recycling and disposal 74
12.8 Secure operation of the engineering software 74
12.9 Safe operation of I/O modules 74
12.9.1 Data integrity for I/O modules 74
12.9.2 Signed firmware update for I/O modules 75

A Safety-related shutdown of ET 200AL IO-Link modules 76

B Dimension drawings 80

C Accessories/spare parts 81
C.1 Accessories/spare parts 81
C.2 UL-approved cables 82

D SIMATIC ET 200AL IO-Link I/O modules data 85

1 Introduction

Purpose of the documentation

This documentation provides you with important information on how to configure, install, wire and commission the IO-Link I/O modules of the SIMATIC ET 200AL distributed I/O system.

Basic knowledge required

A basic knowledge of automation technology is required to understand the documentation.

Validity of the documentation

This documentation applies to the IO-Link I/O modules of the SIMATIC ET 200AL distributed I/O system.

Conventions

Observe the notes labeled as follows:

NOTE

A note contains important information on the product described in the documentation and on the handling of the product to which particular attention should be paid.

Standards

You can find a dated reference to the respective standards or the EU Declaration of Conformity on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert?ct=444&ci=526).

Special information

NOTE

Important note for maintaining the operational safety of your plant

Plants with safety-related features are subject to special operational safety requirements on the part of the operator. The supplier is also obliged to comply with special product monitoring measures. For this reason, we inform you in personal notifications about product developments and features that are (or could be) relevant to the operation of plants from a safety perspective.

You should subscribe to the corresponding notifications in order to obtain the latest information and to allow you to make any necessary modifications to your system.

Log into SiePortal. Follow the links below and click on "Email on update" on the right-hand side in each case:

- SIMATIC S7-300/S7-300F (https://support.industry.siemens.com/cs/ww/en/ps/13751)
- SIMATIC S7-400/S7-400H/S7-400F/FH (https://support.industry.siemens.com/cs/ww/en/ps/13828)
- SIMATIC WinAC RTX (F) (https://support.industry.siemens.com/cs/ww/en/ps/13915)
- SIMATIC S7-1500/SIMATIC S7-1500F (https://support.industry.siemens.com/cs/ww/en/ps/13716)
- SIMATIC S7-1200/SIMATIC S7-1200F (https://support.industry.siemens.com/cs/ww/en/ps/13683)
- Distributed I/O (https://support.industry.siemens.com/cs/ww/en/ps/14029)
- STEP 7 (TIA Portal) (https://support.industry.siemens.com/cs/ww/en/ps/14667)

NOTE

When using F-CPUs in safety mode and fail-safe modules, note the description of the fail-safe system SIMATIC Safety Programming and Operating Manual SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/de/view/54110126/en).

ID Link for the digital nameplate



Figure 1-49 ID Link example IO-Link DI 16x24VDC 8xM12

The ID Link is a globally unique identifier according to IEC 61406, which you will find in the future as a QR code on your product.

The figure shows an example of an ID Link for the I/O device digital inputs DI 16x24VDC 8xM12.

You can recognize the ID link by the frame with a black corner at the bottom right. The ID Link takes you to the digital nameplate of your product.

Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner or reader app. Call the ID link.

In the digital nameplate, you will find product data, manuals, Declarations of Conformity, certificates, and other helpful information about your product.

1.1 SiePortal

You can find current information on the following topics quickly and easily here:

- **Catalog and ordering system**
  Ordering system for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).
- **Product support**
  All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.
- **Application examples**
  Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.
- **Services**
  Information about Industry Services, Field Services, Technical Support, spare parts and training offers.
- **Forums**
  For answers and solutions concerning automation technology.
- **mySiePortal**
  Your personal work area in the SiePortal for notifications, support requests, and configurable documents.

This information is provided by SiePortal on the Internet (https://sieportal.siemens.com/).

1.2 Information classes ET 200AL IO-Link I/O Module



The documentation for the SIMATIC ET 200AL IO-Link I/O modules is divided into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL IO-Link distributed I/O system.

- ET 200AL IO-Link I/O Modules System Manual

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

- IO-Link I/O Modules Equipment Manual

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC IO-Link system.

- IO-Link System Function Manual

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.3 Basic tools

Tools

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities on various SIMATIC S7 stations as bulk operations independent of TIA Portal.

The SIMATIC Automation Tool offers a wide range of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Assignment of addresses (IP, subnet, Gateway) and device name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization through LED flashing
- Reading out of CPU error information
- Reading the CPU diagnostic buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/98161300)

PRONETA

SIEMENS PRONETA (PROFINET network analysis) is a commissioning and diagnostic tool for PROFINET networks. PRONETA Basic has two core functions:

- In the network analysis, you get an overview of the PROFINET topology. Compare a real configuration with a reference installation or make simple parameter changes, e.g. to the names and IP addresses of the devices.
- The "IO test" is a simple and rapid test of the wiring and the module configuration of a plant, including documentation of the test results.

You can find SIEMENS PRONETA Basic on the Internet:
(https://support.industry.siemens.com/cs/ww/en/view/67460624)

SIEMENS PRONETA Professional is a licensed product that offers you additional functions. It offers you simple asset management in PROFINET networks and supports operators of automation systems in automatic data collection/acquisition of the components used through various functions:

- The user interface (API) offers an access point to the automation cell to automate the scan functions using MQTT or a command line.
- With PROFIenergy diagnostics, you can quickly detect the current pause mode or the readiness for operation of devices that support PROFIenergy and change these as needed.
- The data record wizard supports PROFINET developers in reading and writing acyclic PROFINET data records quickly and easily without PLC and engineering.

You can find SIEMENS PRONETA Professional on the Internet.
(https://www.siemens.com/proneta-professional)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

1.4 S7 Port Configuration Tool (S7-PCT)

SIMATIC S7-PCT

The Port Configuration Tool (PCT) is a PC-based software for the parameter assignment of Siemens IO-Link Master modules and IO-Link devices from any manufacturer.

You integrate IO-Link-devices using the standardized device description "IODD", which you get from the respective device manufacturer. S7-PCT supports version 1.0 and V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link Master from STEP 7. When STEP 7 is not used or the IO-Link Master is not operated on a SIMATIC controller, "standalone"-operation is also possible.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

1.5 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Safety instructions

2

2.1 Warnings in this document

You can find explanations of the warnings used in this document in the "Legal information" section.

2.2 Safety-related symbols for IP65/IP67 modules

The following table contains an explanation of the symbols located on your IP65/IP67 modules, their packaging or in the accompanying documentation.

Symbol	Meaning
	General warning sign **Caution/Notice** You must read the product documentation. The product documentation contains information about the type of potential hazard and enables you to recognize risks and implement countermeasures.
	The assigned safety symbols apply to devices **with Ex approval**. You must read the product documentation. The product documentation contains information about the type of potential hazard and enables you to recognize risks and implement countermeasures.
	Read the information provided by the product documentation. ISO 7010 M002
	Ensure the device is only installed by an electrically skilled person. IEC 60417 No. 6182
	Note that connected mains lines must be designed according to the expected minimum and maximum ambient temperature.
	Note that the device must be constructed and connected in accordance with EMC regulations.

Symbol	Meaning
 230V MODULES	Note that a 230 V device can be exposed to electrical voltages which can be dangerous. ANSI Z535.2
 24V MODULES	Note that a device of Protection Class III may only be supplied with a protective low voltage according to the standard SELV/PELV. IEC 60417-DB Symbol 5180 "Class III equipment"
 INDOOR USE ONLY INDUSTRIAL USE ONLY	Be aware that the device is only approved for the industrial field and only for indoor use.

2.3 Intended use

The system is used to control machines and plants.

Intended use also includes observance of this documentation, in particular the safety instructions and conditions of use. See section Technical specifications (Page 56).

2.4 Changes to the device and spare parts

Modifications to the module may affect the safety and the function of the module:

- Do not make any changes or attachments to the module.
- Do not remove or paste over safety instructions on the module.
- Only use original spare parts and accessories.

2.5 Target group and personnel qualifications

All persons working with this module require the following knowledge:

- Contents of this document as well as contents of the enclosed documents.
- Handling the module (after instruction)
- Relevant standards and regulations
- Accident prevention regulations

The following activities are reserved for specially qualified personnel:

Working on electrical parts
Work on electrical parts may only be performed by the following persons:

- Qualified electricians
- Persons trained in electrical engineering under the direction and supervision of qualified personnel.

Commissioning and configuration
Commissioning and configuration requires general knowledge in the field of automation technology.

2.6 Personal protective equipment

The personal protective equipment depends on the activity and is determined by the operator. To avoid material damage during packing, unpacking and installation activities we recommend:

- ESD wrist strap
- ESD shoes

2.7 Working on electrical parts

Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualifications (Page 14)).

- Always observe the country-specific safety rules.
- Notify all those who will be affected by the procedure.
- Follow the 5 safety rules according to DIN EN 50110-1 (VDE 0105-1):

1. Disconnect
2. Secure to prevent reconnection
3. Verify safe isolation from the supply (all poles)
4. Ground and short-circuit
5. Erect barriers around or cover adjacent live parts

After completing work:

- Restore operational readiness in reverse order.

2.8 Residual risks

Despite all the technical and procedural risk reductions that have been carried out, not all dangers can be avoided. The following sections describe these residual risks and measures to avoid them.

2.8.1 Live parts

Electrocution on contact with live parts leads to life-threatening injuries (death).

Operation

- Do not open the module.
- Do not use damaged modules.
- Pull the plug and not the cable.

Installation and connection

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualifications (Page 14)).
- Adhere to the protective measures for safe working on electrical parts (see section Working on electrical parts (Page 15))
- Fuse the connection cables according to the current-carrying capacity of the cable used, taking into account the applicable standards.
- Ground the module according to regulations.
- For the 24 V DC supply (SELV/PELV), only use power supply units that provide safe electrical extra-low voltage in accordance with IEC 61131-2 or IEC 61010-2-201.

Maintenance

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualifications (Page 14)).
- Adhere to the protective measures for safe working on electrical parts (see section Working on electrical parts (Page 15)).

2.8.2 Conductive pollution

Electrocution during transmission of electrical energy via conductive contamination to the body leads to life-threatening injuries (death).

- Seal unused connections with a suitable and approved sealing cap.
- Keep the module free from conductive pollution.

2.8.3 Overheating

Smoke development and fire due to overheating of module and cables result in burns and life-threatening injuries (death).

To avoid overheating:

- Ensure the correct installation position.
- Ensure sufficient air supply (e.g. maintain mounting clearances).
- Only use undamaged cables.

Installation and connection

- Follow the instructions for the mounting position.
- Adhere to the specified ventilation clearances.
- Fuse the connecting cables according to the cable cross-section.

Maintenance

- Check plug-in connections and cables regularly for damage.

2.8.4 Uncontrolled movements

Uncontrolled movements of driven machine or system parts during commissioning, operation, maintenance and repair.

- Follow the safety instructions described in the function manuals.

2.8.5 Unsafe operating states

Unsafe operating states may result in personal injury of unknown extent.
The following factors can be triggers:

- Manipulation of the software, e.g. viruses, trojans or worms.

Manipulation of the software, e.g. viruses, trojans or worms.

- Adhere to the protective measures against tampering with the software (see section Industrial cybersecurity (Page 64)).
- Perform available updates in a timely manner.
- Protect files stored on removable media from malware with appropriate protective measures, e.g. virus scanner.
- Set up access protection for the CPU.

2.9 Behavior in case of emergency

- Force EMERGENCY OFF

When the safe operating state has been restored:

- Unlock the EMERGENCY OFF mechanism.
- The person responsible for the system ensures that the system starts up in a controlled and defined manner.

2.10 Material damage

2.10.1 Transport and storage

- Only pack, store, transport and ship electronic components, modules or devices in the original product packaging or in other suitable materials, e.g. conductive foam rubber or aluminum foil.
- Observe the limits during transport and storage. See Technical specifications (Page 56) section.

2.10.2 Installation and connection

- We recommend touching components, modules and devices only if they are grounded by one of the following measures:
  - With an ESD wrist strap.
  - With ESD shoes or ESD grounding strips in ESD areas with conductive flooring.
- Place electronic components, modules and devices only on conductive surfaces (e.g. tables with ESD coating, conductive ESD plastic foam, ESD packing bags, ESD transport containers).
- Ensure that there is sufficient overvoltage protection.

Installation/disassembly with voltage switched on

- Refer to section Mounting (Page 26)
- Refer to section Replacing modules (Page 51)

New features/functions

3

What's new in Edition 08/2025 of the ET 200AL system manual compared with Edition 12/2022?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	ID link	Here you will find a description of the ID link	Section Introduction (Page 5)
	General security instructions	The section contains a compilation of general security instructions for the ET 200AL distributed I/O system.	Section Safety instructions (Page 13)
	Importer addresses	You can find the importer addresses for specific countries here.	Section Standards and requirements (Page 58)
	"Industrial Cybersecurity" section	Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities. The section contains the following information: • Basic information on the subject of industrial cybersecurity • Measures to protect individual components and the entire system against manipulation and unwanted access.	Section Industrial cybersecurity (Page 64)
	SIMATIC ET 200AL data	The following information provides an overview of the data that is generated by the SIMATIC ET 200AL automation system and accessible to you.	Section SIMATIC ET 200AL IO-Link I/O modules data (Page 85)
Changed contents	Technical specifications	Various specifications have been adapted in the "Technical specifications" section	Section Technical specifications (Page 56)

System overview

4

4.1 System overview

Introduction

A continuous communication down to the lowest field level ensures enhanced use of the functions and performance capability of sensors and actuators. Enhanced use of sensors and actuators allows you to operate your machines and plants more productively.

No data other than the actual process value can be exchanged via the standard interfaces (digital, analog) used at the sensor/actuator level. Sensors and actuators with integrated intelligence are now used for increasingly complex functions and require a communication interface tailored to these requirements.

Definition

IO-Link is an innovative, point-to-point communication interface for the sensor/actuator area that is specified in IEC 61131-9.

IO-Link consists of the following system components:

- IO-Link master
- IO-Link device
- Unshielded 3-wire or 5-wire standard cable
- Engineering tool for configuring and assigning parameters of IO-Link

4.2 What are ET 200AL IO-Link I/O modules?

SIMATIC ET 200AL IO-Link I/O modules

SIMATIC ET 200AL IO-Link I/O modules belong to the SIMATIC ET 200AL distributed I/O system.

You can operate the IO-Link I/O modules on any IO-Link master with IP20 or IP67 degree of protection.

Customer benefits

Easy to use

- IO modules can be connected to any IO-Link master
- CAx-compliant labeling of all interfaces
- Communication and power supply via a single cable
- Standardized IO-Link Connector technology (M12)

Compact design

- 30 mm housing width for tight spaces or 45 mm housing width for a large number of channels
- High degree of protection IP65/IP67
- Adequate for temperatures from -30 °C to +55 °C and accelerations up to 10 g



Communication standards

- IO-Link according to specification V1.1
- Supports the "General profile" of IO-Link

Flexible mounting

- Easy mounting in all mounting positions - even in small spaces
- Point-to-point connection of spatially separated modules using an IO-Link cable
- Addition of a line topology (PROFIBUS, PROFINET IO, ET-Connection) via the IO-Link star topology
- Connection of sensors and actuators with M8 and M12 connection technology

Figure 1-50 Benefits of the ET 200AL IO-Link

Area of application

The SIMATIC ET 200AL distributed I/O system is especially well-suited for the following application areas:

- Where space is limited
- Moving applications
- Assembly and handling technology

Thanks to its scalable construction, you have the option to precisely customize its configuration to your on site needs.

The SIMATIC ET 200AL distributed I/O system is designed in IP65/IP67 degree of protection. The I/O modules are suited for distributed use indoors on a machine or assembly line.

You can adapt the cable routing optimally to the machine requirements. The combination of a line topology, such as PROFINET IO and ET connection, and the star topology of IO-Link make this easy to implement.

Configuration

The IO-Link I/O modules of the SIMATIC ET 200AL distributed I/O system are operated on any IO-Link master.

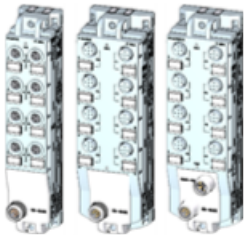
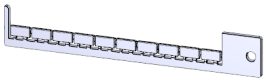
A cable with M12 plug-in connection is used for the communication and power supply.

4.3 Components

Components of the IO-Link I/O modules

The following table shows and explains the function of the components of the IO-Link I/O modules of the ET 200AL distributed I/O system.

Table 1-53 Components of the IO-Link I/O modules

Component	Function	View
IO-Link I/O modules	• The I/O modules form the interface to the process • Recording and controlling the current process status via the connected sensors and actuators	
Identification labels	• The identification labels come with the module and can be machine printed • Can be ordered separately	
M12-A connecting cable	• Connection of IO-Link I/O module to the master • Connection to sensors and actuators	
Power connecting cable M12-L	• Connection of additional load voltage	
Sealing cap M8 and M12	• Seal for unused connections • IP degree of protection is maintained through use	
Y-cable	• Double connection of actuators or sensors to one socket • IP degree of protection class is maintained when two actuators or sensors are connected to one socket	

Application planning

5

5.1 Hardware configuration

Basic configuration with IO-Link I/O modules

Connect the IO-Link I/O module to an IO-Link port of the master with an M12-A coded plug.

The maximum cable length between an IO-Link device and an IO-Link master is 20 m.

Power is supplied to the IO-Link I/O modules via the IO-Link master.

You can connect one IO-Link I/O module per IO-Link port to an IO-Link master.

For I/O modules with high power demand, an M12-L power connector is available for an additional supply voltage.

You can find information on the maximum infeed current in the technical specifications of the modules in the respective equipment manuals or on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

5.2 Configuration of IO-Link I/O modules

Each ET 200AL IO-Link I/O module has an M12 A-coded plug for connection to an IO-Link master.

When connecting the IO-Link I/O modules to an IP65/67 IO-Link master, pay attention to the required port class (Type A or Type B). You can find the technical specifications in the respective equipment manuals or on the Internet.

PROFINET IO

The figure shows an IO-Link configuration in combination with a PROFINET IO network. The line topology of PROFINET IO is supplemented with a star topology of IO-Link.

NOTE

Configuration variants

You can also use the IO-Link I/O modules on IO-Link masters with other fieldbuses.

Connection examples

The following figure shows a connection example using an S7-1500 IO-Link master with IP20 degree of protection.

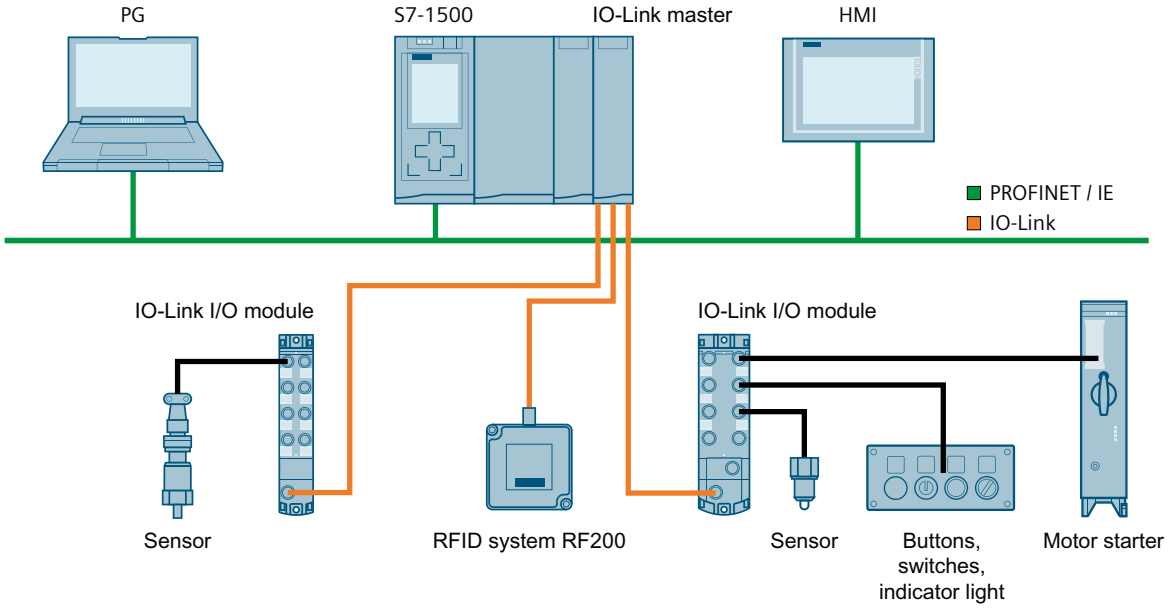


Figure 1-51 Configuration with IP20 IO-Link master

The following figure shows a connection example on an ET 200eco PN M12-L IO-Link master with IP65/67 degree of protection.

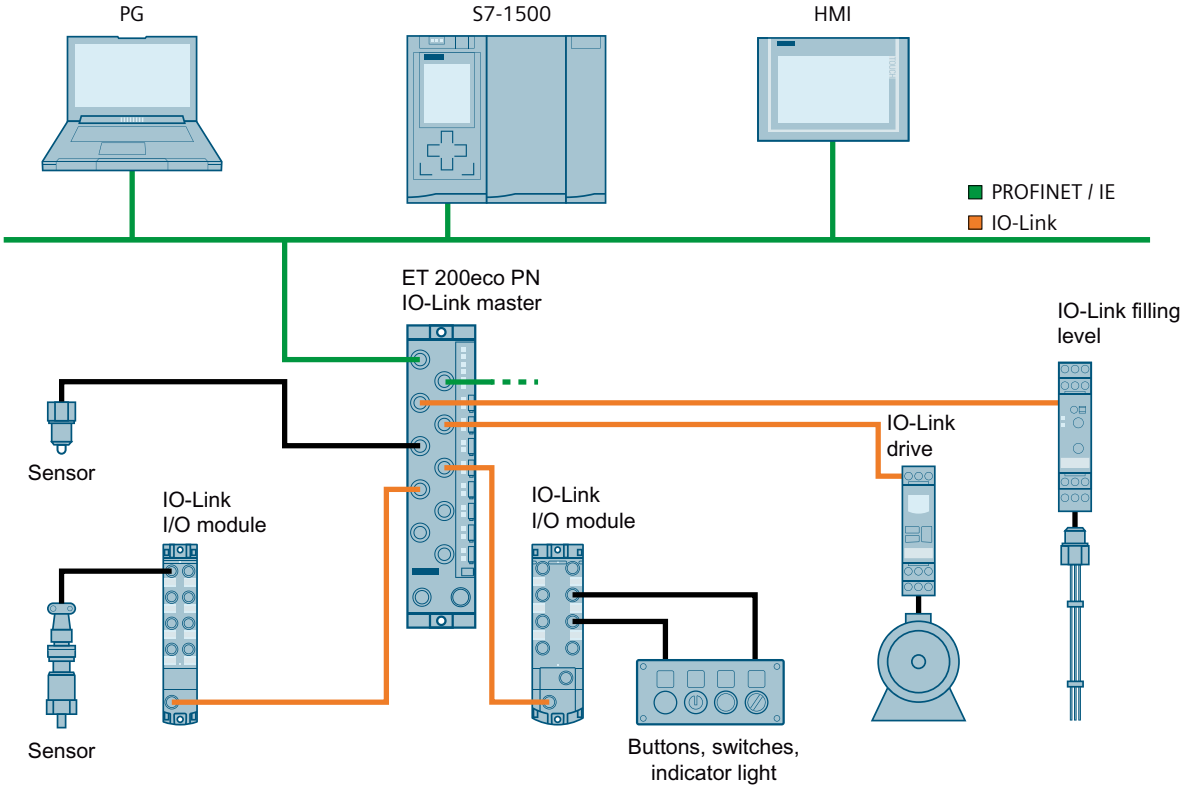


Figure 1-52 Configuration with IP65/67 IO-Link master

Mounting

6

6.1 Basics

Introduction

The IO-Link I/O modules are designed for IP65/IP67 degree of protection. This means that you can mount the modules directly in your plant.

Mounting position

You can mount the IO-Link I/O modules in any mounting position.

Minimum clearances

Maintain a minimum clearance of 2 cm from adjacent modules or other devices when mounting. The minimum clearance makes it easier to install the connectors.

Mounting rules

When mounting the modules, you do not need to following any special rules.

NOTE

Mounting of the modules

Only mount the IO-Link I/O module when the supply voltages are disconnected.

6.2 Mounting modules

Introduction

The IO-Link I/O modules are designed for mounting on a level, stable surface.

Thanks to the axisymmetrical drill holes in the modules, you have the option to fasten the modules on an aluminum profile using tee nuts.

The following images shows the aluminum profile on which you can mount the modules.

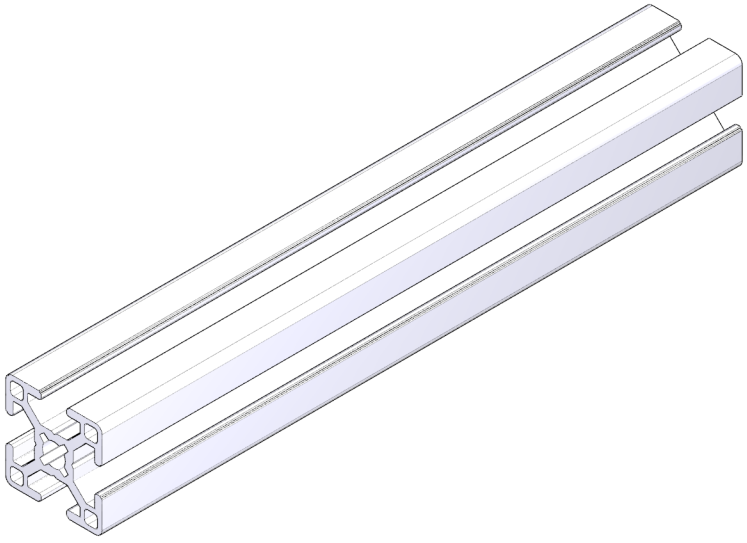


Figure 1-53 Aluminum profile

Required tool

For installation, you need a screwdriver or an Allen wrench.

Required screws

The following table shows and explains the screw types required to mount the modules.

Table 1-54 Recommended screws

Screw type	Explanation
Socket head cap screw M4 according to DIN EN ISO 1207 / DIN EN ISO 1580	The screw length must be at least 30 mm. If you need washers, use DIN EN ISO 7089/DIN EN ISO 7090 washers.
Hexagon socket head cap screw M4 according to DIN EN ISO 4762	

Drill holes of the modules

All IO-Link I/O modules have a uniform drill pattern.

- All module housings are axisymmetrical.
- The distance between the top and bottom drill hole is identical for all modules.

Mounting 30 mm wide I/O modules (front or side)

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/95886672)

The 30 mm I/O modules have a fastening point at the top and bottom. The 30 mm wide I/O modules can also be side-fastened. When fastening them at the side, you must use the supplied spacers.

Follow the steps below to mount a 30 mm wide I/O module:

1. Drill two fastening holes with 4.5 mm diameter spaced 149.6 mm apart.
2. Use the supplied spacers for side fastening of the I/O module on the top and bottom (on one side adjacent to the fastening surface).
3. Fasten the I/O module with the screws to both fastening points (tightening torque 1.2 Nm).

The figure below shows the dimensions for fastening the 30 mm wide I/O modules using the example of the IO-Link I/O module DIQ 4+DQ 4x24VDC/0.5A 8xM8.

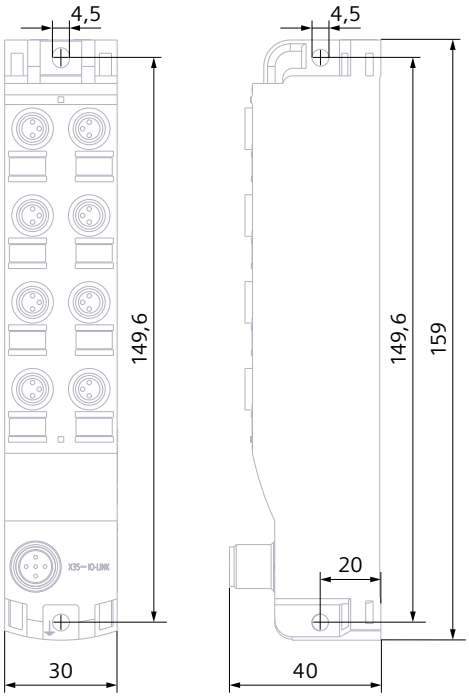


Figure 1-54 Dimensions for mounting 30 mm wide I/O modules

Mounting 45 mm I/O modules (front mounting)

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/95886672)

The 45 mm wide I/O modules have a fastening point at the top and bottom.

Follow the steps below to mount a 45 mm wide I/O module:

1. Drill two fastening holes with 4.5 mm diameter spaced 149.6 mm apart.
2. Fasten the I/O module with the screws to both fastening points (tightening torque 1.2 Nm).

The figure below shows the dimensions for fastening using the example of the IO-Link I/O module DI 8x24VDC M12-L 8xM12.

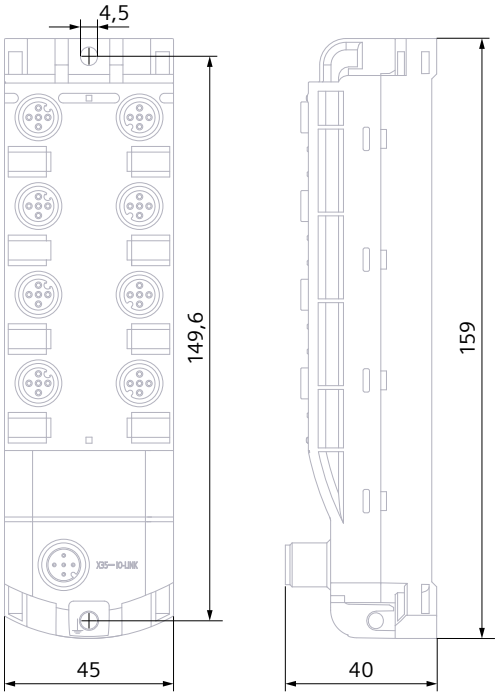


Figure 1-55 Dimensions for mounting 45 mm I/O modules

Fastening for cable ties

All IO-Link I/O modules have integrated fastening points for cable ties. The fastening points are found on all four corners of the modules.

The figure below shows the top left fastening point for 2.5 mm cable ties for fastening the cables.

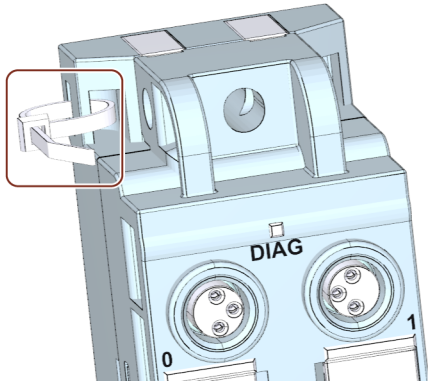


Figure 1-56 Top left fastening point for cable ties

Connecting

7

7.1 Rules and regulations for operation

Introduction

Depending on the area of application, the IO-Link I/O modules, as an integral component of a system, must adhere to special rules.

This section gives an overview of the most important rules you must follow when integrating the IO-Link I/O modules in a plant or system.

Specific application

Observe the safety and accident prevention regulations that are applicable to specific applications, for example, the Machinery Directive.

EMERGENCY-STOP device

Emergency Stop devices according to IEC 60204-1 (corresponds to DIN VDE 0113-1) must remain effective in all operating modes of the system.

Excluding hazardous system conditions

Hazardous operating states must not occur in any situation, but especially:

- When the system restarts after a voltage dip or power outage
- When the IO-Link I/O modules start up after interruption of the IO-Link communication

If necessary, force an EMERGENCY STOP.

An uncontrolled or undefined startup is not permitted after the "EMERGENCY STOP" is unlocked.

Cables and wires

Note that the utilized cables (including plugs) are approved for a continuous operating temperature of 30 °C above the operation temperature of the IO-Link I/O modules.

The cables and wires used must be rated for at least the supply voltage used.

External fuses/switches

External fuses and switches must be installed so that they meet the standards for cable and device protection applicable to your application.

Line voltage

For the line voltage, note the following:

- For stationary plants or systems without an all-pole line disconnector, there must be a disconnector unit (all-pole) fitted in the building installation.
- For load current supplies, the configured rated voltage range must correspond to the local line voltage.
- For all electric circuits of the IO-Link I/O modules, the fluctuation/deviation of the supply voltage and load voltage from the rated value must be within the permitted tolerance.

You can find more information in the section Specifications for insulation, protection class, degree of protection and rated voltage (Page 62).

24 V supply

For the 24 V supply, note the following:

- For buildings:
  If there is a danger due to overvoltages, you must take lightning protection measures for external lightning protection (e.g. lighting protection elements).
- With 24 V DC supply lines and signal lines:
  If there is a danger due to overvoltages, you must take lightning protection measures for internal lightning protection (e.g. lightning protection elements. You will find additional information in the Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566) function manual).
- For 24 V DC supply:
  Ensure that there is an electrical protective separation of extra-low voltage (SELV/PELV) according to IEC 61010-2-201 or IEC 60950-1.
  1L+ is supplied via the IO-Link master. Observe the requirements of the IO-Link master used.
  2L+ is connected via port Type B or the M12-L power connector. Protect 2L+ with a UL- or IEC-approved fuse (tripping characteristic type B or C). This fuse must conform to the cable cross-section and must not exceed the maximum total current of the IO-Link I/O module. Module-specific specifications can be found in the equipment manuals and on the Internet.

NOTE

Wet environment

If you use IO-Link I/O modules in a wet environment, other limits apply for SELV/PELV.

Protection against outside electrical influences

Below is a description of what you must pay attention to in terms of protection against electrical impacts and/or faults:

- To protect against electromagnetic interference, connect the I/O devices to functional ground.
- Ensure correct installation and routing of the supply, signal and IO-Link cables.
- Configure the plant/system in such a way that an error does not result in undefined states.
  - Line/wire break
  - Cross-circuit in the cable

Reference

Additional information can be found in the function manual Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566).

7.2 Operation of the IO-Link I/O modules on a grounded/ungrounded infeed

Introduction

Information on the overall configuration of the IO-Link I/O modules on a grounded infeed (TN-S system) is provided below. Statements regarding the TN-S system relate to the upstream 24 V DC power supply that is connected to the TN-S system.

Together, the IO-Link I/O modules and the IO-Link master form a unit. The following items must be noted for the configuration.

- IO-Link voltage supply via IO-Link master port class A
- IO-Link voltage supply via IO-Link master port class B
- Voltage supply for modules with high power demand via the M12-L power connector

The specific subjects discussed are:

- Disconnecting devices, short-circuit and overload protection to IEC 60364 (corresponding to DIN VDE 0100) and IEC 60204 (corresponding to DIN VDE 0113)
- Load current supplies and load circuits
- Supply voltages of the IO-Link I/O modules

Grounded infeed

In grounded incoming supplies, the neutral conductor of the supply system is grounded. A ground fault between a live conductor and ground or a grounded system component causes the protective devices to trip.

Supply voltages

Provide the IO-Link master with an SELV/PELV 1L+ supply voltage.
The SELV/PELV 2L+ load voltage is supplied via the M12-A connector with port class B or via the M12-L power connector. The SELV/PELV 2L+ load voltage can be switched depending on the application.

- IO-Link 1L+ supply voltage (non-switched) via M12-A connector port class A.
- IO-Link 2L+ load voltage (switched) via M12-A connector port class B or M12-L power connector.

Safe electrical isolation (SELV/PELV)

Power packs/power supply modules with safe electrical isolation SELV/PELV are required for operation of the IO-Link I/O modules. These power packs/power supply modules must comply with IEC 61010-2-201.

The wiring of SELV/PELV circuits must be separated from the wiring of non-SELV/PELV circuits. Or the insulation of all conductors must be rated for the higher voltage.

NOTICE
Operation in damp / wet environments When operating in a damp / wet environment, different voltage limits apply for SELV/PELV according to IEC 61010-2-201.

Configuring IO-Link I/O modules with grounded reference potential

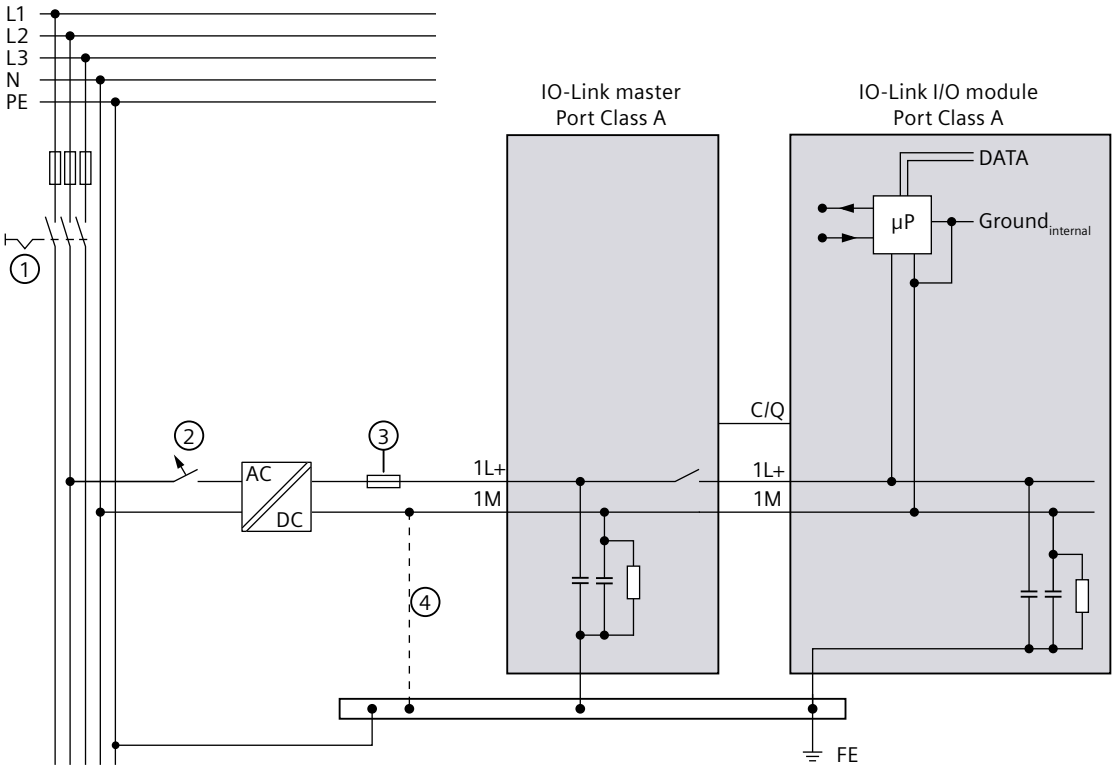
In the configuration of IO-Link I/O modules with grounded reference potential, any interference currents that occur are discharged to functional ground. The connections must be externally connected. Establish a connection between 1M or 2M and functional ground.

Configuring IO-Link I/O modules with ungrounded reference potential

In the configuration of IO-Link I/O modules with ungrounded reference potential, any interference currents that occur are discharged to functional ground via an internal RC network. You do not need an external connection between 1M, 2M and functional ground.

Overall configuration of IO-Link I/O modules

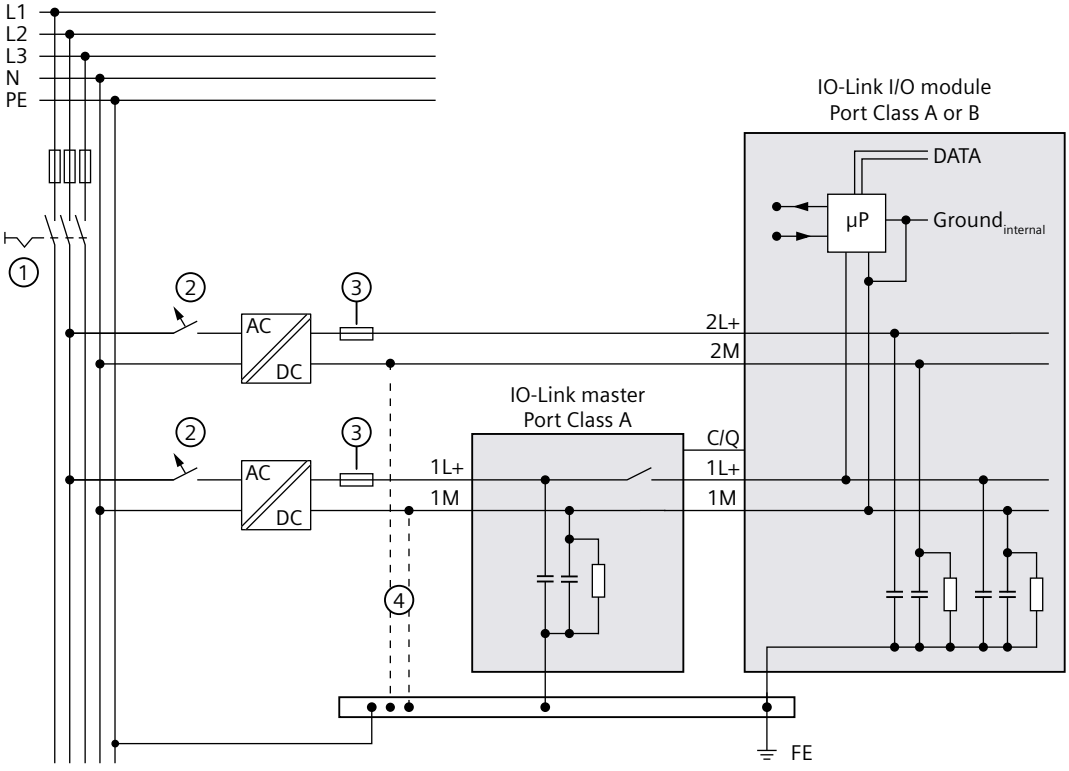
The figure below shows the overall electrical configuration using the example of an IO-Link I/O module with port class A on an IO-Link master with port class A.



① Main switch
② Short-circuit and overvoltage protection
③ Fuses for cable protection
④ In the configuration of the IO-Link system with ungrounded reference potential, the connection between 1M and functional ground is omitted.

Figure 1-57 Electrical configuration of IO-Link I/O module with port class A

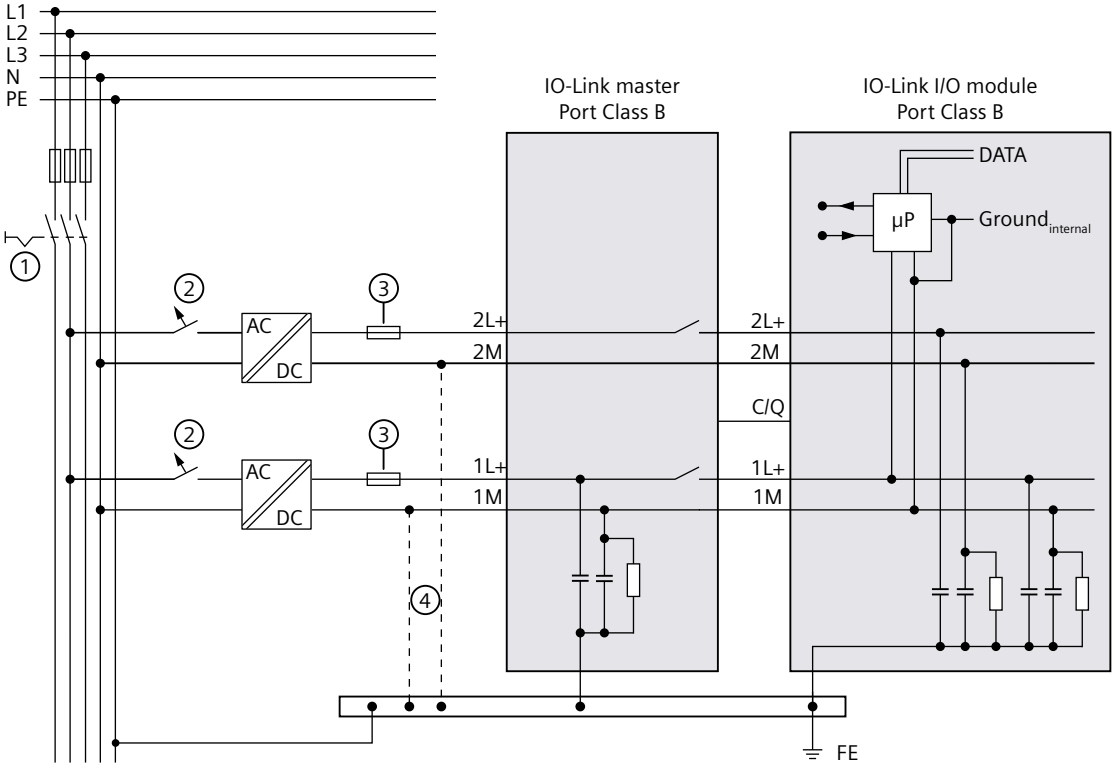
The figure below shows the overall electrical configuration using the example of an IO-Link I/O module with port class A or B on an IO-Link master with port class A.



① Main switch
② Short-circuit and overvoltage protection
③ Fuses for cable protection
④ In the configuration of the IO-Link system with ungrounded reference potential, the connection between 1M, 2M and functional ground is omitted.

Figure 1-58 Electrical configuration of an IO-Link I/O module with port class A or B on an IO-Link master with port class A.

The figure below shows the overall electrical configuration using the example of an IO-Link I/O module with port class B on an IO-Link master with port class B.



① Main switch
② Short-circuit and overvoltage protection
③ Fuses for cable protection
④ In the configuration of the IO-Link system with ungrounded reference potential, the connection between 1M, 2M and functional ground is omitted.

Figure 1-59 Electrical configuration of an IO-Link I/O module with port class B on an IO-Link master with port class B.

Components and protective measures

Various components and protective measures are stipulated for setting up a complete plant. The types of components and the degree to which the protective measures are mandatory depend on the IEC regulation that applies to your plant setup.

The following table shows the components of the electrical configuration with reference to the previous figure and compares the IEC regulations.

Table 1-55 Components of electrical configuration

	Reference to illustration	IEC 60364 (DIN VDE 0100)	IEC 60204 (DIN VDE 0113)
Disconnection element for controller, sensors, and actuators	①	... Part 460: Main switch	... Part 1: Disconnectors
Short-circuit / overload protection	②	.... Part 725: Single-pole protection of circuits	... Part 1: Single-pole protection of grounded secondary circuit
Cable protection	③	... Part 430: Protection of cables and wires against overcurrent Protect all incoming supply cables with a circuit breaker.	... Part 1: Overcurrent protection

Insulation monitoring

You must provide insulation monitoring in the following cases:

- In the configuration of the IO-Link system with ungrounded reference potential
- When hazardous system conditions may occur due to errors

7.3 Electrical configuration of the IO-Link I/O modules

Electrical isolation

In the electrical configuration of the IO-Link I/O modules, there is electrical isolation between:

- IO-Link 1L+: Non-switched supply voltage (electronics/sensor/load supply):
  Electrically isolated from 2L+ (load voltage supply)
- 2L+ port class B or M12-L power connector: Switched supply voltage (load voltage supply):
  Electrically isolated from all other circuit components
  Can be switched off without affecting the IO-Link 1L+

Connection of a digital output with a digital input

NOTICE

Pay attention to the potential group
When a digital output is connected to a digital input, pay attention to the potential groups. Depending on the configuration, 1M and 2M may then be connected, resulting in elimination of the electrical isolation between 1L+ and 2L+. The possible compensating currents can destroy the digital module.

⚠ WARNING

Note potential groups for safety-related shutdown
When a digital output is connected to a digital input, pay attention to the potential groups. Depending on the configuration, 1M and 2M can be connected through this, which leads to cancellation of the electrical isolation between 1L+ and 2L+.
The safety-related shutdown is not permitted if the electrical isolation is canceled.

Cable protection

According to DIN VDE 0100, cable protection is required. Therefore, you must always protect the supply lines externally.

Protect the 24 V DC supply lines against short-circuits and overloads.

Select a protective device that meets the following criteria:

- Suitable for 24 V DC supply voltage
- Suitable for cable cross-section and type of installation
- Suitable for other conditions, such as temperature

Power supply of the configuration

Up to two voltage groups are available for the ET 200AL distributed I/O system.

- 1L+ via IO-Link (supply voltage / non-switched)
- 2L+ via port class B or M12-L power connector (load voltage / switched)

NOTE

Connecting and disconnecting of 1L+ IO-Link, 2L+ via port class B or M12-L power connector
Unlike the load voltage 2L+ via port class B or the M12-L power connector, the connection and disconnection of the supply voltage 1L+ during operation results in a module restart.

7.4 Connecting IO-Link I/O modules to functional ground

Introduction

You must connect the IO-Link I/O modules to functional ground.

What is functional ground?

All IO-Link I/O modules have a functional ground connection. This connection is used to suppress interference sensitivity, but not for protection purposes. With the functional ground connection, you establish an electrical connection to a point of your system or a shield. Electromagnetic interferences are discharged directly to ground via this connection. By discharging the electromagnetic interference, the interference immunity of the entire module is increased.

The figure below shows the symbol that is used to mark the functional ground connection on the IO-Link I/O modules.

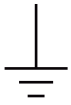


Figure 1-60 Functional ground

7.4.1 Mounting IO-Link I/O modules on a conductive surface

Requirement

Conductive surface for mounting of the module

Required tool

To connect to functional ground, you need the following tool:

- Screwdriver or hexagon socket size 3

Required accessories:

To connect to functional ground, you need the following accessories:

- 2 x M4 fastening screws

Mounting

To connect the IO-Link I/O modules to functional ground in the case of a conductive mounting surface, proceed as follows:

1. Drill two fastening holes. The dimensions of the module can be found in the section Dimension drawings (Page 80).
2. Screw the module with the M4 fastening screws using a torque of 1.2 Nm.

NOTE

Grounding in the case of a conductive mounting surface

When you mount an IO-Link I/O module on a conductive, grounded surface, the lower fastening screw establishes a conductive connection to the ground potential.

Ensure that there is a low-impedance connection between the module and conductive surface as well as between the conductive surface and functional ground.

Reference

You will find more information on installing the modules in the section Mounting modules (Page 27).

7.4.2 Mounting IO-Link I/O modules on a non-conductive surface

Requirement

Non-conductive surface for mounting of the module

Required tool

To connect to functional ground, you need the following tool:

- Screwdriver or hexagon socket size 3
- Stripping tool
- Crimp tool

Required accessories:

To connect to functional ground in the case of a non-conductive mounting surface, you need the following accessories:

- 2 x 4 mm fixing screws
- Cable lug, suitable for 4 mm screws
- Grounding cable (braided copper cable) with a minimum cross section of 4 mm^2

Mounting

To connect IO-Link I/O modules to functional ground, proceed as follows:

1. Drill two fastening holes.
2. Strip the grounding cable.
3. Fasten the cable lug to the grounding cable.
4. Screw the module and the cable lug with the 4 mm fastening screws using a torque of 1.2 Nm.

The figure below shows how to connect the functional ground.

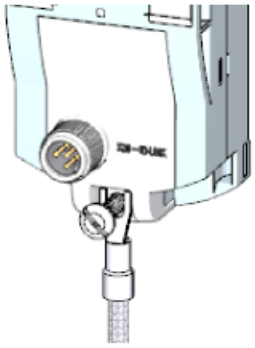


Figure 1-61 Connecting the functional ground

NOTE

Grounding in the case of a non-conductive mounting surface
Make sure there is a low-impedance connection between the module and functional ground.

Reference

You will find more information on installing the modules in the section Mounting modules (Page 27).

7.5 Wiring

Connection

Connect all cables to the front side of the modules:

- IO-Link to the 5-pole M12 connector (A-coded)
- Signal lines to the 3-pole M8 sockets or 4/5-pole M12 sockets (A-coded)
- Additional load voltage to the 5-pole M12 plug (L-coded)

Requirement

Wire the modules with the supply voltage off.

Required tool

If you are not using pre-assembled cables, you need the following tool:

- Stripping tool
- Screwdriver to wire the connection plugs

Accessories required for the connection of IO-Link

You need the following accessories:

- Cables
  - Pre-assembled cable M12, 4-pole or 5-pole, or
  - Flexible 3, 4 or 5-core copper cable (core cross-section: 0.25 to 0.5 mm^2)
- 5-pole M12-A coded connecting socket

Accessories required for the connection of additional load voltage

You need the following accessories:

- Pre-assembled power cable M12-L coded, 4-pole or 5-pole
- Flexible 4-core or 5-core copper cable (core cross-section: 0.5 to 2.5 mm^2)
- 4-pole or 5-pole M12-L coded socket

Connecting M8 connectors

To connect M8 connectors, proceed as follows:

1. Insert the plug into the respective round socket on the module.
   Ensure the correct alignment between plug and socket.
2. Tighten the connector using the knurled screw with a torque of 0.4 Nm.

The figure below shows the connection of the M8 plugs, using the example of the IO-Link digital input module DI 8x24VDC 8xM8..

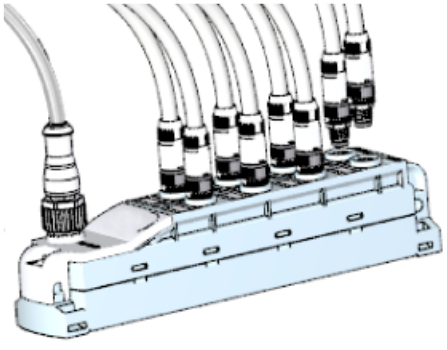


Figure 1-62 Connecting M8 connectors

Connecting M12 connectors

To connect M12 connectors, proceed as follows:

1. Insert the plug into the respective round socket on the module.
   Ensure the correct alignment between plug and socket (groove and spring).
2. Tighten the connector using the knurled screw with a torque of 1 Nm.

The figure below shows the connection of the M12 plugs, using the example of the IO-Link digital input module DI 16x24VDC 8xM12..

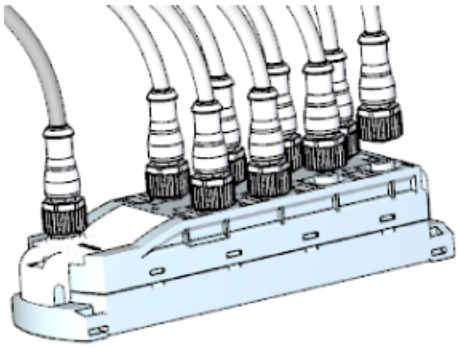


Figure 1-63 Connecting M12 connectors

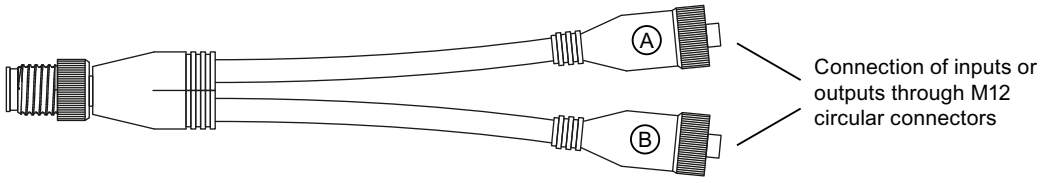
Pin assignment of the sockets

The pin assignment of the sockets can be found in the equipment manuals of the I/O modules (https://support.industry.siemens.com/cs/ww/en/ps/14247/man) in the section on pin assignment and on the side surface of the module.

Y-cable

The Y-cable allows you to connect two actuators or sensors to the inputs or outputs.

The use of a Y-cable is recommended in particular if two channels are occupied per socket of an I/O module. The Y-cable distributes the channels to two circular connectors.



The figure below shows the wiring of the Y-cable.

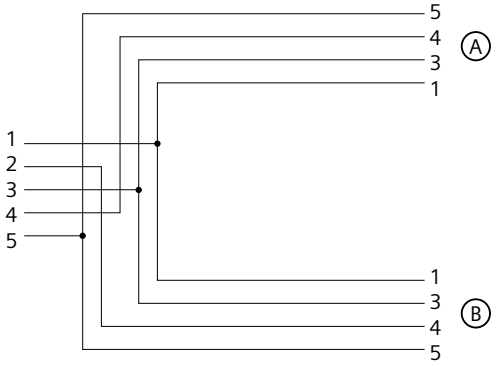


Figure 1-64 Wiring of the Y-cable

Sealing of unused sockets

To ensure IP65 or IP67 degree of protection, seal off all unused sockets with sealing caps.

Article numbers for accessories/spare parts.

You will find the article numbers in the Appendix in section Accessories/spare parts (Page 81).

See also

Interface modules (https://support.industry.siemens.com/cs/ww/en/ps/14246/man)

7.6 Marking of IO-Link I/O modules

7.6.1 Factory markings

Introduction

For better orientation, the IO-Link I/O modules are furnished with various markings that support you when configuring and connecting the modules.

Marking of the interfaces

The interfaces of the modules are factory-labeled.

The table below shows the labeling of the interfaces.

Table 1-56 Interface labeling

interface	Labeling
IO-Link	X35 (IO-Link)
I/O input and output interfaces	X10 ... X17
Additional power supply	X80 (DC24V)

Pin assignment

The pin assignments of the various interfaces are lasered at the factory, on the side of every module.

7.6.2 Optional markings

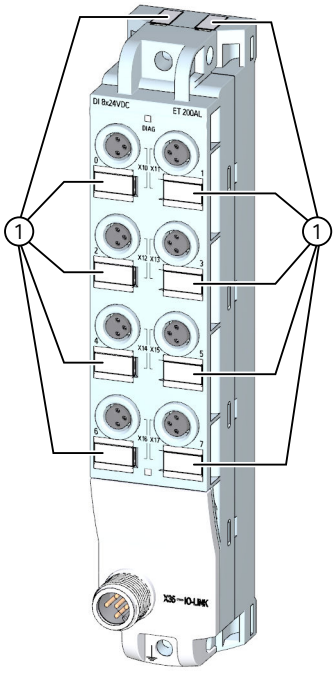
Introduction

In addition to the factory markings, there are also optional possibilities for labeling or marking interfaces and modules on the IO-Link I/O modules.

Identification label

The identification labels come with each IO-Link I/O module as strips and can be machine-printed. A strip has 10 identification labels measuring 10 x 5 mm in the color RAL9016. The identification labels can be inserted into every module at the points provided. The identification labels are used for channel and module labeling.

The figure below shows all points where you can use the identification labels using the example of the IO-Link digital input module module DI 8x24VDC 8xM8.



① Identification labels

Figure 1-65 Optional marking

7.6.3 Mounting identification labels

Introduction

This section describes how to mount or remove identification labels.

Required tools

You need a screwdriver with 3 mm blade width (only to remove identification labels).

Mounting procedure

To mount an identification label, proceed as follows:

1. Print the identification label using commercially available marking systems.
2. Press the identification label out of its holder.
3. Stick the identification labels into the cutouts provided, as shown in the figure Optional marking (Page 45).

Mounting the identification labels is the same for all modules.

Removal procedure

To remove an identification label, proceed as follows:

1. Carefully use a screwdriver to pull out the identification label.

Removing identification labels is the same for all modules.

Configuring

8

8.1 Requirements

Introduction

Configuration and parameter assignment of the IO-Link I/O modules is carried out with:

- STEP 7 (TIA Portal)
- S7-PCT
- IO-Link configuration software of the IO-Link master manufacturer

Requirements

Observe the software requirements of the configuration software of the utilized IO-Link master.

Table 1-57 Hardware requirements

Hardware	Requirements
IO-Link master	As of IO-Link V1.1

8.2 IODD and Port Configuration Tool - S7-PCT

Device description IODD

An electronic device description, the IODD file (IO Device Description), is available for each device. The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the same manner by the IO-Link configuration tools of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODD finder is available on the Internet (https://ioddfinder.io-link.com).

IO-Link configuration tool

Configuration tools are required to configure the entire IO-Link system. The IO-Link configuration tools of the master manufacturers are able to read IODDs.

The main tasks of the IO-Link configuration tool include:

- Assignment of devices to the master ports
- Address assignment of the ports within the address area of the master
- Parameter assignment of the IO-Link devices

Diagnostics can also be carried out on the connected devices.

This means the IO-Link configuration tool supports the transparent representation of the IO-Link system down to field level.

Siemens provides S7-PCT for engineering of the IO-Link system.

You can find the relevant device description file, software and function manuals in SIOS. (https://support.industry.siemens.com/cs/ww/en/view/109737170)

S7-PCT with IODD of an IO-Link I/O module

The following figure shows a section from S7-PCT with IODD of an IO-Link I/O module and the device information contained therein.

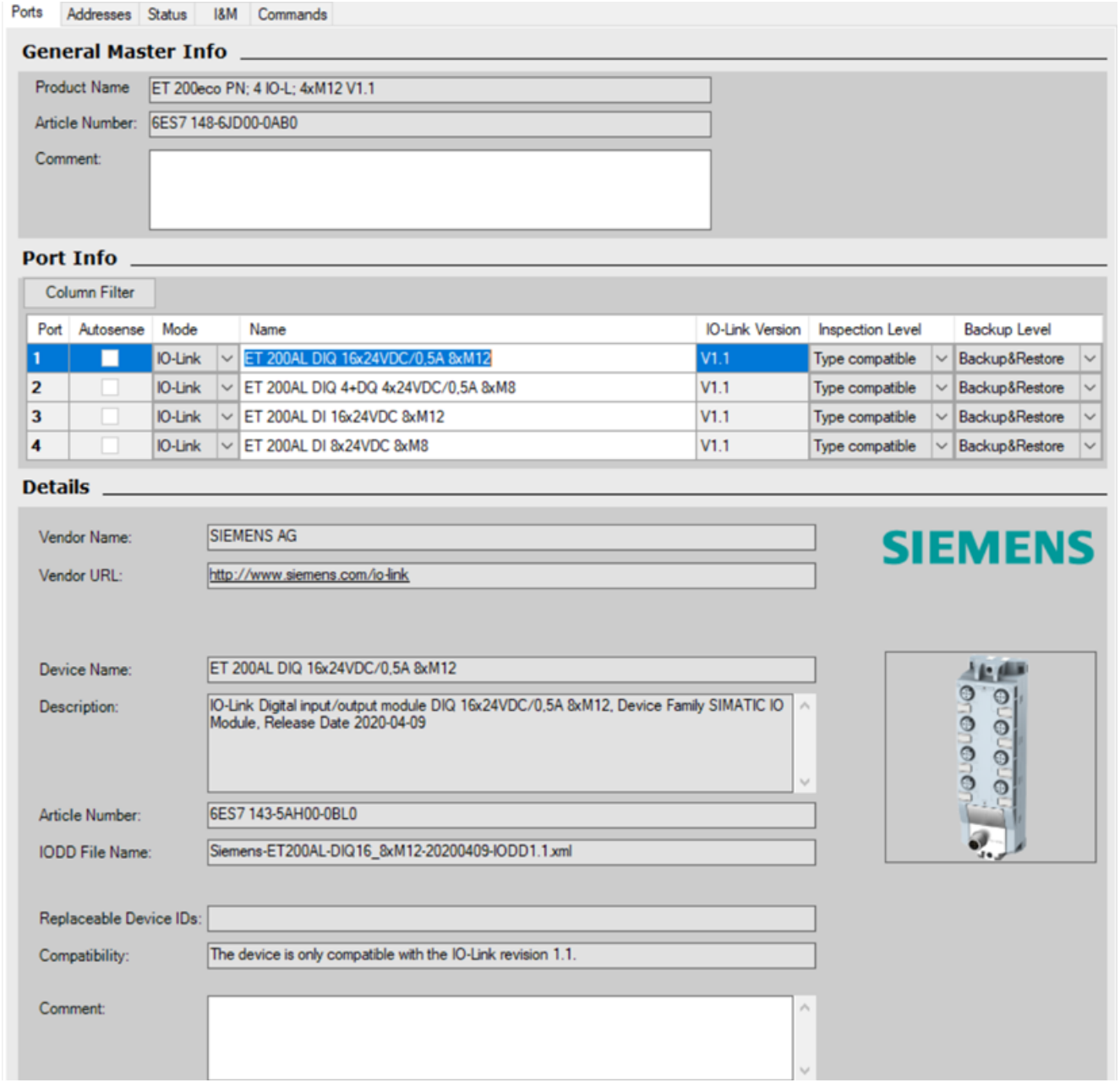


Figure 1-66 S7-PCT with IODD of a device and the device information contained therein

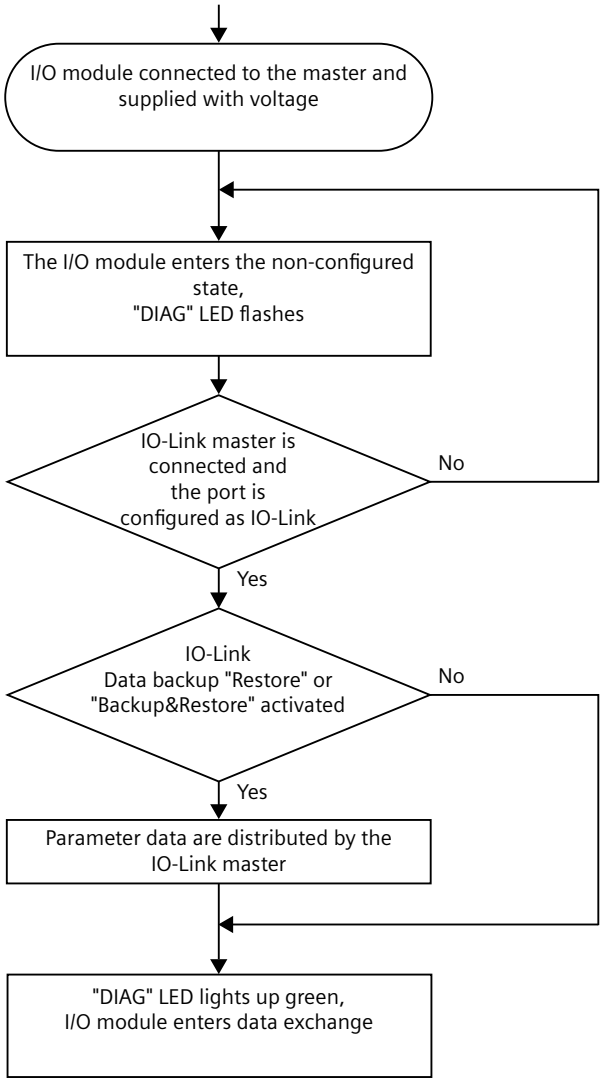
Commissioning

9

9.1 Startup of the IO-Link I/O module

Principle of operation

The figure below shows the startup of an IO-Link I/O module on an IO-Link Master schematically as a flow chart.



The "PWR" LED lights up green when the 2L+ voltage is applied.

Figure 1-67 Startup of an ET 200AL IO-Link I/O module

Maintenance 10

10.1 Replacing modules

Replacing IO-Link I/O modules

The replacement of a module is not permitted during ongoing operation.

⚠ WARNING

Property damage can occur
If you remove/insert modules while the power is connected, this can lead to undefined states in your system.
The IO-Link I/O module may be damaged as a result.
Only remove or replace modules when the power is disconnected.
Always comply with the required standards and safety guidelines when configuring a system.

If you use the restore function of the master, the master automatically provides the saved parameters to the new module after module replacement. You have the following setting options for module replacement:

- "Backup&Restore"
  You have set the master port to "Backup&Restore". The new module behaves like the replaced module because the master has saved the last parameter change using the backup function.
- "Restore"
  You have set the master port to "Restore". The new module applies the parameter settings that were saved in the master at the time of the last back-up.

Procedure

To replace an IO-Link I/O module, follow these steps:

1. Ensure that no current is flowing via the outputs.
2. Completely disconnect all cables connected to the IO-Link I/O module.
3. Completely remove the fixing screws of the module
4. Replace the IO-Link I/O module.

NOTE
"New" IO-Link I/O module
The removed IO-Link I/O module may only be replaced by a module of the same type.

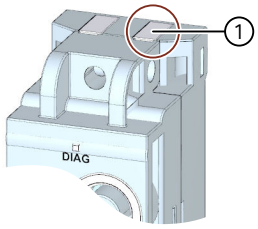
5. Fasten the IO-Link I/O module with the screws with a torque of 1.2 Nm.

6. Connect all cables.
7. Turn the supply voltage on.

⚠ WARNING

Observe the device number of the modules
If you mix up the IO-Link I/O modules when connecting them, this can cause personal injury and property damage.
We recommend that you clearly label the IO-Link I/O modules with the device number.

The figure below shows a recommendation for the marking of the IO-Link I/O modules with the device number.



① Recommendation for the marking of device numbers

Figure 1-68 Device number

Result

The IO-Link I/O module that was out of service starts up again automatically. When data backup is set, the IO-Link master loads the parameter settings to the module.

10.2 Firmware update

Introduction

During operation, it can become necessary to update the firmware (e.g. for function extensions).

You use a firmware update to update the module firmware.

NOTE

STOP state during the update
When you perform a firmware update for an IO-Link I/O module, the module goes to STOP state during the update.

Requirement

To perform a FW update, you need an IO-Link master that supports the IO-Link FW update transfer mechanism.

Option for the firmware update

You have the option of performing a firmware update online via S7-PCT.

Reference

You will find additional information on the procedure in the "Help" > "Help topics" tab in S7-PCT. Enter "Firmware" in the search field and confirm with Enter.

10.3 Resetting a module

Introduction

With "Restore Factory Setting", the IO-Link I/O module is set to the delivery condition. All information that was saved internally on the IO-Link I/O module is deleted.

Options for resetting

You can reset the IO-Link I/O module in S7-PCT.
You have two different possibilities for this.

- "Application Reset"
- "Restore Factory Setting"

Result after "Application Reset"

The "Application Reset" command resets the application-specific parameters to the default values. The identification parameters of the module remain unchanged.

The command is not followed by a module restart or a communication interruption.

Result after "Restore Factory Setting"

The "Restore Factory Setting" command causes three different actions. The actions are dependent on the data backup setting on the IO-Link master.

- "None":
  The default parameters of the IO-Link I/O module are loaded. The IO-Link I/O module performs a restart.
- "Restore":
  The saved parameters at the time of the backup are loaded. The IO-Link I/O module performs a restart.
- "Backup&Restore":
  The parameters that were in the IO-Link I/O module before the "Restore Factory Setting" command are loaded. The IO-Link I/O module performs a restart.

Requirement

An online connection must exist to reset an IO-Link I/O device.

Procedure using S7-PCT

Connect the PG/PC to the PROFINET IO or PROFIBUS DP interface of the IO-Link master or to your system.

Make sure that an online connection to the IO-Link I/O module exists.

1. Select an IO-Link I/O module in the project tree.
2. Select the "Parameters" tab in the work area.
3. Under "Parameters" > "Parameter Data" > "System command", click on the desired button:

- "Application Reset"
- "Restore Factory Setting"

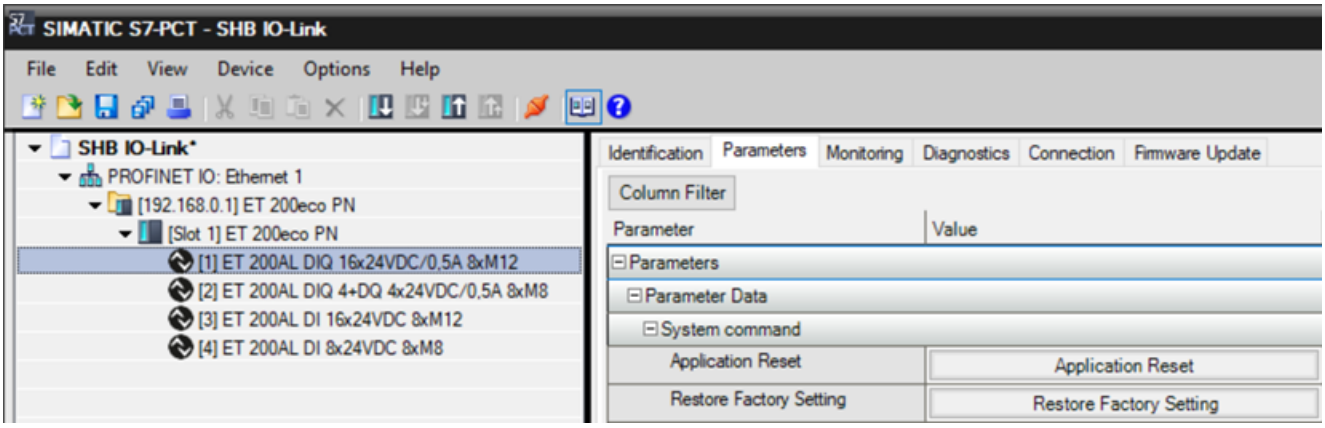


Figure 1-69 Resetting a module

Result: The IO-Link I/O module is reset.

Reference

You can find more information on the procedure in the S7-PCT online help.

10.4 Maintaining/cleaning the modules

Maintenance

The IO-Link I/O modules are maintenance-free.

NOTE

Repairs

Repairs to an IO-Link I/O module may only be carried out by the manufacturer.

Cleaning

When wired, the IO-Link I/O modules comply with degree of protection IP65/IP67 and do not require any cleaning.
If you want to clean the modules, use a dry or damp cloth. Please take care to comply with degree of protection IP65/67 when cleaning with liquids.

Technical specifications

11

11.1 Markings and approvals

Marks and approvals on the nameplate

The following overview provides information about the possible marks and approvals. Only the marks and approvals specified on the nameplate apply to the module.

You can find the associated certificates for download on the Internet. See also: ET 200AL approvals (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert)

CE marking

CE

The ET 200AL IO-Link I/O modules meet the requirements and protection targets of the following Directives and complies with the harmonized European standards (EN) for programmable logic controllers published in the official gazettes of the European Community:

- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)

  Directive of the European Parliament and of the Council of February 26, 2014 on the harmonization of the laws of the Member States relating to electromagnetic compatibility; OJ L 96, 29/3/2014, pp. 79–106
- 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)

  Directive of the European Parliament and of the Council of June 8, 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment; OJ L 174, 1/7/2011, pp. 88–110

The EC Declarations of Conformity are available for the responsible authorities and are kept at the following address:

Siemens Aktiengesellschaft
Digital Industries
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg, Germany

UKCA mark

The ET 200AL IO-Link I/O modules comply with the designated British Standards (BS) for programmable logic controllers published in the official consolidated list of the British government. The ET 200AL IO-Link I/O modules fulfill the requirements and protection targets of the following regulations and related supplements:

- Electromagnetic Compatibility Regulations 2016 (S.I. 2016 No. 1091), and related amendments
- Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (S.I. 2012 No. 3032), and related amendments

UK Declarations of Conformity are available to the relevant authorities at the following address:

Siemens Aktiengesellschaft
Digital Industries
Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg, Germany

UL approval

Underwriters Laboratories Inc. according to

- UL 61010-1 and UL 61010-2-201
- CSA C22.2 No. 61010-1 and CSA C22.2 No. 61010-2-201

RCM Australia/New Zealand

The ET 200AL IO-Link I/O modules meet the requirements of EN 61000-6-4 Generic standards – Emission standard for industrial environments.

Korea Certificate

Note that this device corresponds to limit class A in terms of the emission of radio frequency interference. This device can be used in all areas, except residential areas.
이기기는업무용(A급) 전자파적합기기로서판매자또는사용자는이점을주의하시기바라며 가정외의지역에서사용하는것을목적으로합니다.

EAC (Eurasian Conformity)

The code EAC (Eurasian Conformity) confirms the conformity with the guidelines (TR) of the Eurasian Economic Union.

WEEE mark (European Union)



Disposal information, observe the local regulations and section "Secure decommissioning (Page 73)".

11.2 Certificates

Shipbuilding certificates

The following shipbuilding certificates are intended for the device:

- ABS (American Bureau of Shipping)
- Bureau Veritas (French marine classification society)
- CCS (China Classification Society)
- Class NK (Nippon Kaiji Kyokai)
- DNV (Det Norske Veritas)
- KR (Korean Register of Shipping)
- LRS (Lloyds Register of Shipping)
- RINA (Registro Italiano Navale)

After a successful approval you can find the certificates with the certified article numbers in the Internet. See also: ET 200AL Marine/Shipbuilding (https://support.industry.siemens.com/cs/ww/en/ps/14245/cert?ct=446)

11.3 Standards and requirements

IEC 61131-2

The ET 200AL IO-Link I/O modules fulfill the requirements and criteria of the standard IEC 61131-2 (Programmable controllers, part 2: Equipment requirements and tests) and the EMC requirements for use in Zone B.

IEC 61010-2-201

The ET 200AL distributed I/O system fulfills the requirements and criteria of standard IEC 61010-2-201.

IO-Link standard

The ET 200AL IO-Link I/O modules fulfill the requirements and criteria of the IO-Link standard IEC 61131-9.

Use in industrial environments

The ET 200AL IO-Link I/O modules are designed for the industrial environment. It meets the following standards for this type of use:

- Requirements for interference emission EN IEC 61000-6-4
- Requirements for immunity EN IEC 61000-6-2

Use in mixed areas

Under certain circumstances, you can use the die ET 200AL IO-Link I/O modules in a mixed area. A mixed area is used for residential purposes and for commercial operations that do not significantly impact on residents.

If you want to use the ET 200AL IO-Link I/O modules in a mixed area, you must ensure that its radio frequency interference emissions comply with the limits of EN 61000-6-3. Suitable measures for observing these limits for use in a mixed area are, for example:

- Installation of ET 200AL IO-Link I/O modules in grounded control cabinets/control boxes
- Use of noise filters in the supply cables

An individual acceptance test is also required.

Use in residential areas

The ET 200AL IO-Link I/O modules are not intended for use in residential areas. Using the ET 200AL IO-Link I/O modules in residential areas can affect radio and television reception.

Importer addresses

The following table shows the importer addresses for specific countries:

Countries	Address
United Kingdom (UK)	Siemens plc. Manchester M20 2UR
Türkiye (TR)	Siemens San. ve Tic. A.Ş. Yakacık Cad. No:111 34870 Kartal/İstanbul

11.4 Electromagnetic compatibility

Definition

Electromagnetic compatibility is the ability of an electrical apparatus to function in a satisfactory manner in its electromagnetic environment without affecting this environment.

The ET 200AL IO-Link I/O modules fulfill the requirements of the EMC law of the European Single Market. The prerequisite for this is that the ET 200AL IO-Link I/O modules comply with the requirements and guidelines regarding the electrical configuration.

Pulse-shaped disturbance variables

The following table shows the electromagnetic compatibility of the ET 200AL IO-Link I/O modules with respect to pulse-shaped disturbance variables.

Table 1-58 Pulse-shaped disturbance variables

Pulse-shaped disturbance variable	Tested with	Conforms to degree of severity
Electrostatic discharge according to IEC 61000-4-2.	Air discharge: ±8 kV	3
	Contact discharge: ±4 kV	2
Burst pulses (rapid transient disturbance values) according to IEC 61000-4-4.	±2 kV (power supply cable)	3
	±1 kV (signal line <30 m)	3

Sinusoidal disturbance variables

The tables below show the electromagnetic compatibility of the ET 200AL IO-Link I/O modules with respect to sinusoidal disturbance variables.

Table 1-59 RF radiation

RF radiation according to IEC 61000-4-3 Electromagnetic RF field, amplitude modulated		Conforms to degree of severity
80 ... 1000 MHz	10 V/m	3
1.4 ... 6 GHz	3 V/m	2
80% AM (1 kHz)		

Table 1-60 RF coupling (signal and supply cables)

RF coupling according to IEC 61000-4-6.	Conforms to degree of severity
0.15 ... 80 MHz	3
10 V_{rms} unmodulated	
80% AM (1 kHz)	
150 Ω source impedance	

Emission of radio frequency interference

The following table shows the interference emission of electromagnetic fields according to EN IEC 61000-6-4/EN 55016-2-3.EN IEC 61000-6-4/EN 55016-2-3.

Table 1-61 Interference emission of electromagnetic fields

Frequency	Interference emission	Measuring distance
30 ... 230 MHz	<40 dB (µV/m) Q	10 m
230 ... 1000 MHz	<47 dB (µV/m) Q	10 m
1 GHz ... 3 GHz	<76 dB (µV/m) P	3 m
3 GHz ... 6 GHz	<80 dB (µV/m) P	3 m

Conducted emission

The following table shows the limits for power supply connections in accordance with EN IEC 61000-6-4/EN 55016-2-1.

Table 1-62 Interference emission from the power supply

Frequency	Interference emission
0.15 ... 0.5 MHz	89 dB (µV) Q 76 dB (µV) M
0.5 ... 30 MHz	83 dB (µV) Q 70 dB (µV) M

11.5 Transport and storage conditions

Transport and storage conditions

The ET 200AL IO-Link I/O modules surpass the requirements of IEC 61131-2 regarding transport and storage conditions. The following table shows the conditions that apply to modules transported or stored in their original packaging.

- Transport condition class: TTH4
- Storage condition class: STH4

Table 1-63 Transport and storage conditions

Type of condition	Permitted range
Free fall	≤0.3 m
Temperature	-40 °C ... +70 °C
Temperature variation	20 K/h
Barometric pressure	1140 ... 660 hPa (Corresponds to an altitude of -1000 m to 3500 m)
Relative humidity	5 ... 95%; no condensation

11.6 Mechanical and climatic ambient conditions

Operating conditions

The ET 200AL IO-Link I/O modules are intended for weather-proof, stationary use.

- The operating conditions surpass the requirements of IEC 61131-2:
  - Class OTH3

You can find the values for the operating conditions in the technical specifications of the equipment manuals or on the Internet (https://support.industry.siemens.com/cs/de/en/view/109742718).

Tests for mechanical ambient conditions

The following table shows the type and scope of the tests for mechanical ambient conditions.

Table 1-64 Tests for mechanical ambient conditions

Condition tested	Test standard	Values
Vibrations	Vibration test according to IEC 60068-2-6.	Type of oscillation: Frequency sweeps with a rate of change of 1 octave/minute. 5 Hz to 12.9 Hz, constant amplitude 15 mm 12.9 Hz to 150 Hz, constant acceleration 10 g Duration of oscillation: 10 frequency sweeps per axis at each of three vertically aligned axes
Shock	Shock, tested according to IEC 60068-2-27	Type of shock: Half-sine Shock intensity: 30g peak value, 18 ms duration Direction of shock: 3 shocks each in ± direction in each of the 3 axes vertical to one another

Climatic ambient conditions

The following table shows the type and scope of the tests on climatic ambient conditions.

Table 1-65 Climatic ambient conditions

Ambient conditions	Fields of application	Comments
Temperature	-30 °C ... 55 °C	All installation positions
Temperature variation	10 K/h	-
Relative humidity	5 ... 100%	With condensation and mounted covers
Barometric pressure	1140 ... 795 hPa	Corresponds to an altitude of -1000 m ... 2000 m
Pollutant concentration	ANSI/ISA-71.04 severity level G1; G2; G3	-

11.7 Details on insulation, protection class, degree of protection and rated voltage

Insulation

The insulation is designed in compliance with the requirements of IEC 61010-2-201.

NOTE

For modules with 24 V DC supply voltage (SELV/PELV), electrical isolations are tested with 707 V DC (type test).

Protection class according to IEC 61010-2-201

- Protection class III

Severity for voltage interruption

The ET 200AL IO-Link I/O devices meet the severity class PS1 for voltage interruptions.

Pollution degree / overvoltage category according to IEC 61131

Connected according to the specifications in the "Wiring (Page 41)" section:

- Pollution degree: 3 (macro environment)
- Overvoltage category: II

In delivery state, with one or more open connections:

- Pollution degree: 2 (micro environment)
- Overvoltage category: II

Degree of protection IP65 and IP67

Degree of protection IP65 and IP67 according to IEC 60529 for all ET 200AL IO-Link I/O modules:

- 1. Code number: Dust-proof and complete protection from contact
- 2. Code number: Protection from water
  - IP65: Protection from water jets from any angle
    The water must not have any damaging effect.
  - IP67: Protection against temporary immersion
    The water must not enter the enclosure in harmful quantities.

Rated voltage for operation

The following table shows the rated voltage and the corresponding tolerance with which the ET 200AL IO-Link I/O modules operate.

Table 1-66 Rated voltage for operation

Rated voltage (SELV/PELV)	Tolerance range
1L+	18 ... 30 V DC
2L+	20.4 ... 28.8 V DC

Industrial cybersecurity

12

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

In the first part of this section you will find basic information on the subject of industrial cybersecurity. Subsequent sections describe recommended measures for protecting the entire system and individual components from manipulation and unwanted access.

NOTE

Security-relevant changes to software or devices are documented in the section New features/functions (Page 19).

12.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

12.2 Security update notification

Read the special information on maintaining the operational safety of your plant in the Introduction (Page 5) section.

Set up notification of security updates

To receive notifications about security updates, proceed as follows:

1. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home).
2. Enter the keyword "Security" in the search engine.
3. Choose the "Search in Knowledge base" option.
4. In the "Product tree" filter menu, select your product or your product group, for example "Automation Technology" > "Automation Systems" > "Industrial Automation Systems SIMATIC" > "I/O systems" > "SIMATIC ET 200 systems without control cabinet" > "ET 200AL".
5. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".
6. Select the document about which you want to receive notifications using the 3 points on the right "Add to my favorites".
7. In the following dialog, select the name, the storage location and the "Notify me" option for the favorite. Then click on the "+ Add to my favorites" button.

Result: You will be notified by email each time the document is changed.

Under "mySiePortal" > "Lists & notifications" > "My notifications", you can display your notifications and delete them if necessary.

12.3 Basic information on industrial cybersecurity

12.3.1 Definition of industrial cybersecurity

Industrial cybersecurity is generally understood to mean all measures to protect against the following threats:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability (e.g. due to the destruction of data or denial of service (DoS))

12.3.2 Objectives of industrial cybersecurity

The objectives of industrial cybersecurity are:

- Ensuring trouble-free operation of industrial systems and production processes
- Preventing threats to people and production from cybersecurity attacks
- Protection of industrial plants against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Provision of a practical and cost-effective concept for securing existing plants and devices without their own security functions

- Use of existing, open and proven industrial cybersecurity standards
- Compliance with legal requirements

An optimized and adapted security concept applies to automation and drive technology. The security measures must not impede or endanger production.

12.4 Integrated security concept and security strategies

12.4.1 Comprehensive security concept "Defense in Depth"

With Defense in Depth, Siemens provides a multi-layer security concept that offers industrial plants comprehensive and far-reaching protection in accordance with the recommendations of the IEC 62443 international standard.

Productivity and know-how are protected on 3 levels:

Plant security
Plant security uses various methods to secure the physical access of people to critical components. This starts with classic building access and extends to securing sensitive areas using access control (for example, code card, iris scan, fingerprint or access code).

Network security
Automation networks must be protected against unauthorized access. This is achieved through security measures on the product, but also those in the product-related environment.

System integrity
Targeted measures must be taken to protect existing know-how or to prevent unauthorized access to automation processes. The measures protect against unauthorized configuration changes and highlight attempts at manipulation.

You can find more information on the topics of Defense in Depth, plant security, network security, and system integrity on the SIEMENS Industrial cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) Web page.

You can also visit the download center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) to obtain more information on the topic of industrial cybersecurity. The "Operational Guidelines", for example, provide recommendations on basic security measures for secure machine and plant operation in an industrial environment.

12.4.2 Security management

The ISO 27001 and IEC 62443 standards call for a comprehensive approach in information technology (IT) and operational technology (OT) to protect against cyber attacks.

Responsibility for cybersecurity and IT security

Every operator of machinery and equipment is responsible for:

- Defining cybersecurity and IT security as an important criterion in the procurement and selection of machines and software applications.
- Use of suitable measures to protect production resources, data, and communication from manipulation and theft
- Providing all necessary resources and training to employees to fully support these goals

For this purpose, suitable measures must be selected after a risk assessment and a cost-benefit analysis in order to protect material and intellectual property and prevent damage from occurring. These measures should be integrated into corporate processes and procedures, evaluated regularly, and firmly anchored in the corporate culture. In addition to protecting intellectual property, the protection of personal data must be ensured at all organizational units and levels.

Siemens will provide you with information and support. Subscribe to the Security feeds (https://www.siemens.com/cert) for information on vulnerabilities. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home) and create filters to be notified when important information is published. The procedure is described in the section Notification of security updates (Page 65). Consider using Siemens Cybersecurity Services.

Responsibility in the digital supply chain

Cybersecurity should play a critical role in the evaluation and procurement process. The entire life cycle of a product should be considered to ensure protection against current and future risks. These include, for example, security updates throughout the product life cycle, including guidelines for secure disposal of the product.

Siemens plans and announces the provision of security updates, as well as total discontinuation of products, as part of product support.

Employee awareness

Regular training in cybersecurity and continuous testing of training success are essential so that cybersecurity measures are internalized in processes and work instructions. This involves general training in the use of software and IT hardware for company communication and as work equipment e.g.:

- Secure handling of USB devices
- Encrypted communication
- Use of VPN
- Rules for passwords and use of access
- Setting up two-factor authentication
- Educating employees about the dangers posed by malware, phishing, social engineering and other factors

Furthermore, if applicable, production equipment and software training should always include the topic of cybersecurity.

Maintaining the security concept through updates

Keeping software up-to-date is essential, for example, to benefit from the following measures:

- Implementation of new security strategies, protocols and techniques
- Closing of security vulnerabilities
- Elimination of security vulnerabilities

To this end, it is necessary to keep a constant eye on the further development of protective measures and, if necessary, the expansion of requirements.

Recommendations:

- Set up notifications for (security) updates
- Subscribe to information on vulnerabilities
- Monitor and implement the further development of the technology, especially in the area of cybersecurity

Always keep technology and knowledge up to date.

Consideration of the risks posed by cyber attacks in the Threat and Risk Assessment (TRA)

Make an inventory of all software, hardware, and infrastructure devices, in order to identify risks to the location or organization. Incident response procedures must be incorporated into all IT and manufacturing processes. The choice of risk mitigation measures should be based on a cost-benefit analysis and classification of risks. This is followed by the introduction of cybersecurity rules and procedures and the training of personnel.

Living the concept

Technical solutions alone are not sufficient to effectively counter threats.

Cybersecurity must be part of the corporate culture and process landscape and must be internalized and lived by all employees.

Continuously monitoring the security situation

You have the following options for continuously monitoring the cybersecurity situation:

- Setting anomaly references and creating allow and deny lists based on normal network communication and production machine behavior. The SINEC software family offers you reliable security tools (https://www.siemens.com/global/en/products/automation/industrial-communication/sinec-network-software/cybersecurity.html) to detect potential vulnerabilities in OT networks, quickly initiate suitable measures and effectively resolve security vulnerabilities.
- Establishment of an intrusion detection system (IDS) that generates alarms when unusual behavior occurs in the network

- Introduction of a Security Information and Event Management (SIEM) system to collect, analyze, and evaluate events in real time to enable early countermeasures
- Measures regarding network security: for example network segmentation, firewalls, VPN, DMZ (demilitarized zones)

12.5 Operational application environment and security assumptions

12.5.1 Intended use

SIMATIC products are intended for use in industry. If you plan to use the product in a different environment, check the conditions required for such use.

The product may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety information. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products.

Operational reliability and intended use

Read the "Special information" in the Introduction (Page 5) section.

Area of application

Refer to the "Application area" section in the System overview (Page 20) chapter.

12.5.2 Requirements for the operational application environment and security assumptions

Siemens recommends the following security measures:

- Threat and risk assessment (as part of security management)
- Network security concepts
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
- Access control concepts (utilizing access control systems)
  - Physical protection
  - Physical corporate security
  - Physical product security

Threat and Risk Assessment

Vulnerabilities and risks are identified, and countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) on the Industrial Cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) website.

Access control concepts

Physical protection
In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security
You can ensure the physical security of the company by taking the following measures:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security
You can ensure physical production safety by taking the following measures, among others:

- Separate access control for critical areas, such as production zones.
- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.
- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).
- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsafe on systems.

12.6 Security properties of the devices

The security properties of the individual devices are listed in the Equipment Manuals.

12.7 Secure operation of the system

This section describes measures recommended by Siemens to protect your system from manipulation and unauthorized access.

12.7.1 Hardening measures

System hardening, simplify referred to as hardening, is the secure configuration of products or systems. The aim is to close security gaps and take various measures to reduce the attack surfaces for cyberattacks.

Measures for system hardening include, for example:

- Secure configuration in which only necessary software components and services are installed or activated for proper operation.
- Access control, by which restrictive user and rights management system is implemented.

12.7.2 Secure configuration

Secure configuration involves control over all software components, along with their interfaces, ports, and services.

Activated services and ports pose a risk, e.g. of unauthorized access to the network and programs.

To minimize risks, only activate the necessary services for all automation components. Take all activated services (especially Web servers, FTP, remote maintenance etc.) into account in the security concept. Consider the default states of ports and services in your security concept.

You can find an overview of all ports and services used in the Communication function manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

12.7.3 Handling of sensitive data

Data protection information

Siemens Aktiengesellschaft observes the applicable data protection laws, including the General Data Protection Regulation (GDPR), in particular the rules of data minimization and data protection-friendly default settings (privacy by design, privacy by default).

The products do not store any personal data.

If you establish a reference to an identifiable person by linking this functional data with other data (such as shift schedules) or if you store personal data on the same medium (such as a hard disk), you are responsible for ensuring that the data protection regulations are observed.

Information on the secure removal of data is provided in the section Secure decommissioning (Page 73).

Storage of security-related data

When storing your security-relevant data on your PC, independently ensure secure data storage.

12.7.4 Regular firmware updates

NOTE

Outdated firmware versions might not be monitored for security vulnerabilities.

- Always keep your plant/products up to date to benefit from troubleshooting and to minimize potential risks.
- Use email notifications to be automatically informed about firmware updates.

You can find more information in:

- Section Firmware update
- Section Notification of security updates (Page 65)

12.7.5 Notifications about security vulnerabilities (Siemens Security Advisories)

A vulnerability is a security vulnerability in information security. It can pose a threat as it provides intruders with the opportunity to access system resources and manipulate or steal data. Many vulnerabilities allow availability to be impaired.

Siemens ProductCERT

If Siemens identifies or fixes security gaps (Vulnerabilities) in the products, this will be published in the Security Advisories.

You can find the documents for SIMATIC on the following Siemens Aktiengesellschaft web page: Siemens ProductCERT and Siemens CERT (https://www.siemens.com/global/en/products/services/cert.html?s=SIMATIC&_originalHost=new.siemens.com#SecurityPublications)

"SIMATIC" is preset in the "Search Security Advisories" search field. You can also enter other product names or other terms in the search field and search for them.

On this page, you will also find all the required information on how to deal with vulnerabilities:

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities
- Notifications are also possible in CSAF format
- Option to subscribe to RSS feeds and newsletters
- List of all current vulnerabilities and detailed information such as:
  - Description
  - Classification according to Common Vulnerability Scoring System (CVSS)
  - Measures
  - Availability
  - Etc.

Set up Security feeds (https://www.siemens.com/cert) to receive notifications about security-related topics.

If you suspect or have discovered a vulnerability in a Siemens product, please inform us immediately. To do this, press the "Contact" button on the CERT Services page (https://www.siemens.com/cert) and follow the instructions.

12.7.6 Data backup

Secure your configuration and parameter settings so that you can quickly restore this data if needed.

12.7.7 Security checks

Security checks for data, files, and archives serve to ensure data integrity at the storage location and during file transmission, protecting against manipulation and transmission errors. This is often achieved using digital checksums that are provided alongside the data. Tools (such as SHA-256 or SHA-512) for calculating and verifying these checksums are provided in many systems and named according to their respective calculation methods.

File Integrity Guidelines describe the prescribed procedure for integrity checks

Integrity protection is a protection function for engineering data and firmware files

Communication integrity means protecting communication against unauthorized manipulations to ensure high system availability. A central element in this regard is, for example, the use of digital checksums when accessing controllers. (Source: Industrial Cybersecurity website (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html))

12.7.8 Secure decommissioning

In the following section, you will find information on how to properly decommission individual components of your automation system. Decommissioning is necessary when the component has reached the end of its service life.

Decommissioning includes environmentally sound disposal and secure removal of all digital data of electronic components with storage medium.

12.7.8.1 Securely removing data

Before disposing of components of your automation system, you should securely delete all data from the storage media of these components. How to securely delete data from the devices so that it cannot be recovered is described below.

NOTICE
Data misuse resulting from non-secure deletion of data Incomplete or non-secure deletion of data from data memories can result in data misuse by third parties. For this reason, ensure secure deletion of data from all storage media used before disposing of the product.

Securely removing data

You can restore the IO-Link I/O module to the factory settings via S7-PCT to safely remove the data.

The procedure is described in the "Resetting a module (Page 53)" section.

12.7.8.2 Recycling and disposal

For environmentally sustainable recycling and disposal of your old equipment, contact a certified electronic waste disposal service and dispose of the equipment according to the applicable regulations in your country.

12.8 Secure operation of the engineering software

For more information on secure operation of the engineering software, refer to the TIA Portal online help.

12.9 Safe operation of I/O modules

Device-specific security information and instructions for I/O modules can be found in the respective Equipment Manual.

12.9.1 Data integrity for I/O modules

Data integrity for I/O modules

In order to detect intentional or accidental changes to the data of an interface module and the assigned modules, the dynamic integrity check for I/O modules is introduced as of firmware version V2.0. You can also find out whether your I/O module supports the data integrity check in the Technical specifications section of the corresponding equipment manual.

Principle

The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as serial numbers, parameter settings, calibration data and I&M data of I/O modules. The interface module stores the checksums in the I&M4 data area.

You can find more information on the principle of data integrity and I&M4 data in the section Data integrity for interface modules.

Spare parts scenario

The spare parts scenario is still ensured. This means that you can replace I/O modules with the same article number. For the "new" I/O module, the static data such as the serial number will change. Note that the replacement is therefore reflected in the following modified I&M4 data of the interface module:

- CHK_STATIC_SUBS
- CHK_OVERALL_SUBS
- CHK_OVERALL

You can find the structure of I&M data in the section Record structure for I&M data.

12.9.2 Signed firmware update for I/O modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect internet source

Signed firmware update for I/O modules

Firmware updates for I/O modules as of firmware version V2.0 contain a digital signature. The digitally signed firmware update files are available for download on the Siemens Support Web page.

Principle, diagnostics alarms and remedies as for interface modules

The principle and diagnostics of the signed firmware update are the same for interface modules and I/O modules. The information in the section Signed firmware update for interface modules applies.

Safety-related shutdown of ET 200AL IO-Link modules

A

Introduction

The following structure describes how to shut down ET 200AL IO-Link modules in a fail-safe manner.

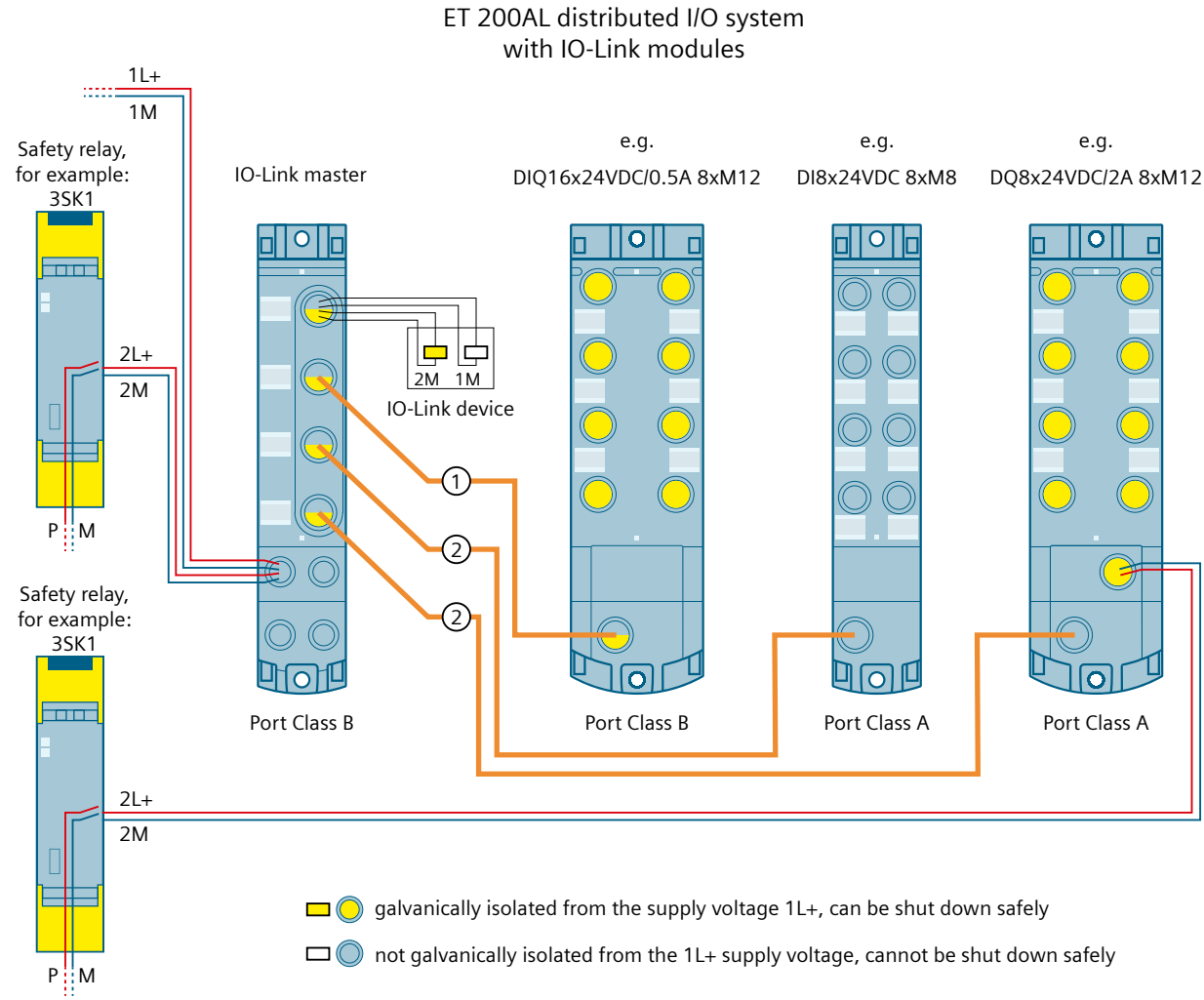
In the configuration shown in the diagram below (e.g. with the safety shutdown device 3SK1), all digital outputs that are connected to the 2L+ and 2M supply (24 V switched) of the ET 200AL IO-Link modules are switched to the safe OFF state. This step achieves the safety class SIL2/Category 3/PL d.

Principle of operation

The higher-level safety shutdown device (e.g. 3SK1) disconnects the supply 2L+ and 2M switched. The digital outputs of the ET 200AL IO-Link modules operated on the 2L+ and 2M (24 V switched) supply are switched to the safe state.
There are two ways to connect the 2L+ and 2M supply voltage to an IO-Link module.

- Via the IO-Link master Port Class B
- Via the M12-L plug for the supply voltage

Block diagram



① 5-wire cable for a Port Class B connection
② 3-wire cable for a Port Class A connection

Figure 1-70 Higher-level safety circuit of the outputs

⚠ WARNING

Note potential groups for safety-related shutdown
When a digital output is connected to a digital input, pay attention to the potential groups. Depending on the configuration, 1M and 2M can be connected through this, which leads to cancellation of the electrical isolation between 1L+ and 2L+.
The safety-related shutdown is not permitted if the electrical isolation is canceled.

NOTE

Safe electrical separation
Maintain safe galvanic isolation for voltages higher than SELV/PELV.

NOTE

Selection of the IO-Link master

If the safety-related shutdown is performed via the IO-Link master, ensure that the master has the appropriate safety characteristics.

NOTE

IO-Link cable

Use a 3-wire cable for the connection of an IO-Link master with Port Class B and an IO-Link device with Port Class A.

Limits of the higher-level safety circuit

The ET 200AL IO-Link modules do not perform any safety functions. Safety functions are performed by the safety relay to bring the system into a safe state.
Adjust the operation inspection interval of the safety relay with relay output according to the safety class.
Take the following measures if energy that is not provided by the higher-level safety circuit is used to control the safety function.

Cover critical errors in the safety function that are not detected by the higher-level safety circuit (e.g. 3SK1) with suitable safety measures. The "diagnostics" must be performed indirectly via the controlled process.

Specifications for safety-relevant process data:

- Functionally safe
- Read via fail-safe inputs (e.g. F-DI)
- Fail-safe processing unit (e.g. F-CPU) for issuing commands
- Output through fail-safe outputs (e.g. F-DQ) to control the safety function

Requirements on the power supply

Operation requires a SELV/PELV power supply to limit overvoltages to L+ and M (24 V). This measure prevents possible errors from the power supply side at the same time.

Select the power supply according to the requirements of the respective operating instructions for the shutdown device and for the ET 200AL system.

You can find more information on safe SELV/PELV in the data sheets of the power supplies used.

FAQ

Read the latest information on safety-related shutdown in the FAQ (https://support.industry.siemens.com/cs/us/en/view/39198632).

In this FAQ, you can find the SIMATIC standard modules that are suitable for safety-related shutdown.

Request German Technical Inspectorate report (Report no. SN89858T)

You can request copies of the German Technical Inspectorate report at the following address:

Siemens Aktiengesellschaft
Digital Industries
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg, Germany

Dimension drawings

B

Two module widths are available for the IO-Link I/O modules.

The figure below shows the height and width of the modules. The depth of the modules varies between 40 mm and 45 mm. Detailed information on the dimensions of the individual modules can be found in the equipment manuals for the IO-Link I/O modules in the section "Dimension drawing".

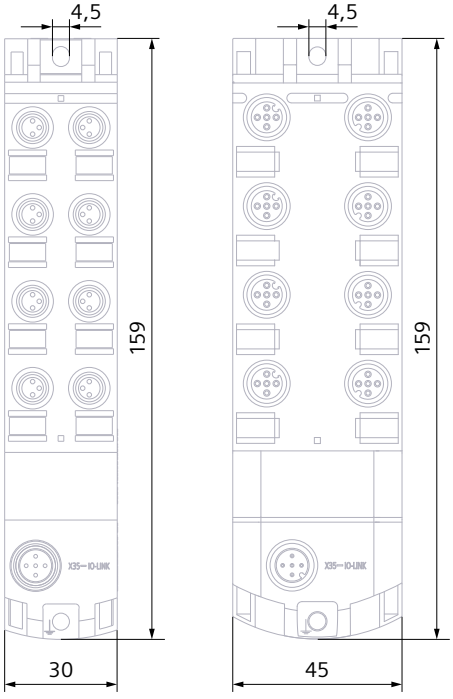


Figure 1-71 Module dimension drawings (front view)

Accessories/spare parts

C

C.1 Accessories/spare parts

Accessories for the ET 200AL IO-Link I/O modules

Table 1-67 Accessories for connection to an IO-Link master

Designation	Length	Article number
Cable is pre-assembled		
M12 CONNECTING CABLE, A-CODED ET 200 Pre-assembled cable with M12 plug and M12 socket, A-coded, 5-pole, 5 x 0.25	0.5 m	6XV1801-2CE50
	1.0 m	6XV1801-2CH10
	1.5 m	6XV1801-2CH15
	2.0 m	6XV1801-2CH20
	3.0 m	6XV1801-2CH30
	5.0 m	6XV1801-2CH50
	10.0 m	6XV1801-2CN10
	15.0 m	6XV1801-2CN15

Table 1-68 Accessories for power supply 2L+ of the DQ 8x24VDC/2A 8xM12

Designation	Length	Article number
Cable is pre-assembled		
M12 CONNECTING CABLE, L-CODED Power connecting cable M12-180/M12-180 for power supply of ET 200 Pre-assembled cable with M12 plug and M12 socket, L-coded, 4-pole	0.5 m	6XV1801-6DE50
	1.0 m	6XV1801-6DH10
	1.5 m	6XV1801-6DH15
	2.0 m	6XV1801-6DH20
	3.0 m	6XV1801-6DH30
	5.0 m	6XV1801-6DH50
	10.0 m	6XV1801-6DN10
	15.0 m	6XV1801-6DN15
Cable and socket can be assembled in the field		
Power M12 Cable Connector PRO; M12 connector with female contact insert, 4-pole, L-coded		6GK1906-0EB00
Energy cable 4 x 1.5; power cable (4-wire), by the meter, unassembled		6XV1801-2B

Table 1-69 Dual connection

Designation		Article number
SIMATIC DP, Y cable for distributed I/Os for double connection of I/Os using single cable, 5-pole, M12	0.2 m	6ES7194-6KA00-0XA0

Table 1-70 Additional accessories

Designation	Article number
Identification labels 10 x 5 mm RAL9016, composed of 200 labels on frames, per frame 40 labels	6ES7194-2BA00-0AA0
Sealing cap M8 for modules IP67	3RK1901-1PN00
Sealing cap M12 for modules IP67	3RX9802-0AA00

Online catalog

Additional article numbers for the ET 200AL IO-Link I/O modules can be found on the Internet (https://mall.industry.siemens.com) in the online catalog and online ordering system.

C.2 UL-approved cables

UL-approved cables from PHOENIX CONTACT

In combination with the named cables of the manufacturer PHOENIX CONTACT, the IO-Link I/O modules of the SIMATIC ET 200AL distributed I/O system meet the requirements for UL approval.

Table 1-71 Accessories for connection to an IO-Link master

Description	Length	Designation	Article number
Cable: pre-assembled 1.5 mm²			
M12 CONNECTING CABLE, A-CODED Sensor/actuator cable, 5-pole, PUR halogen-free, black gray RAL 7021, shielded, straight plug M12, coding: A, to straight socket M12, coding: A	0.3 m	SAC-5P-M12MS/ 0,3-PUR/M12FS SH	1500884
	0.6 m	SAC-5P-M12MS/ 0,6-PUR/M12FS SH	1500897
	1.5 m	SAC-5P-M12MS/ 1,5-PUR/M12FS SH	1500907
	3.0 m	SAC-5P-M12MS/ 3,0-PUR/M12FS SH	1500910
Cable: Socket - open end 1.5 mm²			
M12 CONNECTING CABLE, A-CODED Sensor/actuator cable, 5-pole, PUR halogen-free, black gray RAL 7021, shielded, free cable end, to straight socket M12, coding: A	1.5 m	SAC-5P-1,5-PUR/M12FS SH	1682935
	3.0 m	SAC-5P-3,0-PUR/M12FS SH	1682948
	5.0 m	SAC-5P-5,0-PUR/M12FS SH	1682951
	10.0 m	SAC-5P-10,0-PUR/M12FS SH	1500758

Table 1-72 Accessories for DI/DQ connection

Description	Length	Designation	Article number
Cable: pre-assembled 0.25 mm²			
M8 CONNECTING CABLE, straight Sensor/actuator cable, 3-pole, PUR halogen-free, black gray RAL 7021, straight plug M8, to straight socket M8	0.3 m	SAC-3P-M 8MS/ 0,3-PUR/M 8FS	1681907
	0.6 m	SAC-3P-M 8MS/ 0,6-PUR/M 8FS	1681910
	1.5 m	SAC-3P-M 8MS/ 1,5-PUR/M 8FS	1681923
	3.0 m	SAC-3P-M 8MS/ 3,0-PUR/M 8FS	1681936

Table 1-73 Accessories for additional power supply

Description	Length	Designation	Article number
Cable: pre-assembled 2.5 mm²			
M12 CONNECTING CABLE, L-CODED Power cable, 4-pole, PUR halogen-free, black gray RAL 7021, straight plug M12, coding: L, to straight socket M12, coding: L	0.3 m	SAC-4P-M12MSL/0,3-PUR/FSL	1425081
	0.6 m	SAC-4P-M12MSL/0,6-PUR/FSL	1425082
	1.5 m	SAC-4P-M12MSL/1,5-PUR/FSL	1425083
	3.0 m	SAC-4P-M12MSL/3,0-PUR/FSL	1425084
Cable: Socket - open end 2.5 mm²			
M12 CONNECTING CABLE, L-CODED Power cable, 4-pole, PUR halogen-free, black gray RAL 7021, straight socket M12, coding: L, to free cable end	5.0 m	SAC-4P-5,0-PUR/M12FSL	1425075
	10.0 m	SAC-4P-10,0-PUR/M12FSL	1425076
Cable: pre-assembled 1.5 mm²			
M12 CONNECTING CABLE, L-CODED Power cable, 4-pole, PUR halogen-free, black gray RAL 7021, straight plug M12, coding: L, to straight socket M12, coding: L	0.3 m	SAC-4P-M12MSL/0,3-105/FSL	1425041
	0.6 m	SAC-4P-M12MSL/0,6-105/FSL	1425042
	1.5 m	SAC-4P-M12MSL/1,5-105/FSL	1425043
	3.0 m	SAC-4P-M12MSL/3,0-105/FSL	1425044
Cable: Socket - open end 1.5 mm²			
M12 CONNECTING CABLE, L-CODED Power cable, 4-pole, PUR halogen-free, black gray RAL 7021, straight socket M12, coding: L, to free cable end	5.0 m	SAC-4P-5,0-105/M12FSL	1425035
	10.0 m	SAC-4P-10,0-105/M12FSL	1425036

UL-approved cables from Siemens

In combination with the named cables for the connection of DI/DQ of the manufacturer Siemens, the IO-Link I/O modules of the SIMATIC ET 200AL distributed I/O devices meet the requirements for UL approval.

Table 1-74 Accessories for DI/DQ connection

Designation	Length	Article number
Pre-assembled cables and connectors		
Power connecting cable M12-180/M12-180 for power supply of ET 200, pre-assembled cable with M12 plug and M12 socket, A-coded, 5-pole	0.3 m	6XV1801-5DE30
	0.5 m	6XV1801-5DE50
	1.0 m	6XV1801-5DH10
	1.5 m	6XV1801-5DH15
	2.0 m	6XV1801-5DH20
	3.0 m	6XV1801-5DH30
	5.0 m	6XV1801-5DH50
	10.0 m	6XV1801-5DN10
	15.0 m	6XV1801-5DN15
Power connecting cable M12-90/M12-90 for power supply of ET 200, pre-assembled cable with M12 plug and M12 socket, A-coded, 5-pole	0.3 m	6XV1801-5GE30
	0.5 m	6XV1801-5GE50
	1.0 m	6XV1801-5GH10
	1.5 m	6XV1801-5GH15
	2.0 m	6XV1801-5GH20
	3.0 m	6XV1801-5GH30
	5.0 m	6XV1801-5GH50
	10.0 m	6XV1801-5GN10

Designation	Length	Article number
Power connecting cable M12-90/M12-90 for power supply of ET 200, pre-assembled cable with M12 plug and M12 socket, A-coded, 5-pole	15.0 m	6XV1801-5GN15
Robust power connecting cable M12-180/M12-180 for power supply of ET 200, pre-assembled cable with M12 plug and M12 socket, A-coded, 5-pole	1.0 m	6XV1801-5AH10
	2.0 m	6XV1801-5AH20
	3.0 m	6XV1801-5AH30
	5.0 m	6XV1801-5AH50

SIMATIC ET 200AL IO-Link I/O modules data

D

The EU Data Act, a key component of the European data strategy, went into effect on January 11, 2024.

The following information provides an overview of the data that is generated by the SIMATIC ET 200AL IO-Link I/O modules and accessible to you.

Type, format, and estimated scope of data that the product is capable of generating

Type of data	Formats	Estimated scope
Process data (input and output data, states, alarms)	Numeric formats, binary formats	Cyclic processing Depending on application
Configuration and parameter data (upload to PG/PC)	Binary formats, string formats	Depending on application
Diagnostics data	Binary formats	Depending on application Less than 100 bytes per diagnostic event
Identification data	Binary formats, string formats	Approximately 100 bytes per read-out data record

Continuous and real-time data generation

The IO-Link I/O modules are able to generate data continuously and in real time. Data acquisition takes place continuously throughout the entire operation. The cycle time is specified by the IO-Link master.

Data storage and storage duration

Local data storage

The IO-Link I/O modules store data in integrated memory areas.

Local data storage	Storage capacity	Storage duration
Retentive memory (for identification data and parameter data)	1 to 2 MB I/O modules	Permanent
Work memory (for process data, diagnostics data and parameter data)	I/O modules several hundred KB	During operation of the module

Data access/retrieval, terms of use, and quality of service

Type of data	Access/retrieval via	Terms of use	Quality of service*
Process data (input and output data, states, alarms)	IO-Link master S7-PCT (for IO-Link masters)	Depending on the connected IO-Link master	Depending on the IO-Link master and the fieldbus used on the IO-Link master
Configuration and parameter data (upload to PG/PC)	IO-Link master S7-PCT (for IO-Link masters)	Depending on the connected IO-Link master	Depending on the IO-Link master and the fieldbus used on the IO-Link master
Diagnostics data	IO-Link master S7-PCT (for IO-Link masters)	Depending on the connected IO-Link master	Depending on the IO-Link master and the fieldbus used on the IO-Link master
Identification data	IO-Link master S7-PCT (for IO-Link masters)	Depending on the connected IO-Link master	Depending on the IO-Link master and the fieldbus used on the IO-Link master

* "Quality of service" refers to the ability of the I/O modules to manage network resources efficiently and to ensure that specific performance requirements for data transmission are met.

Deleting data of the IO-Link I/O modules

I/O modules
The data of an IO-Link I/O module can be deleted using S7-PCT by executing the "Reset to factory settings" function.

More information
You can find more information on deleting data in the "Securely removing data (Page 73)" and "Reset to factory settings (Page 53)" sections.

SIEMENS

SIMATIC
ET 200SP
Product Information Mixed Configuration ET 200SP / ET 200AL
Product Information

Application planning

Mixed configuration ET 200SP and ET 200AL with ET-Connection
You have the option of integrating the I/O modules of the ET 200AL distributed I/O system (IP65/IP67) in a configuration of the ET 200SP distributed I/O system (IP20).
The figure below shows a combination of the modules of the ET 200AL and ET 200SP distributed I/O system.

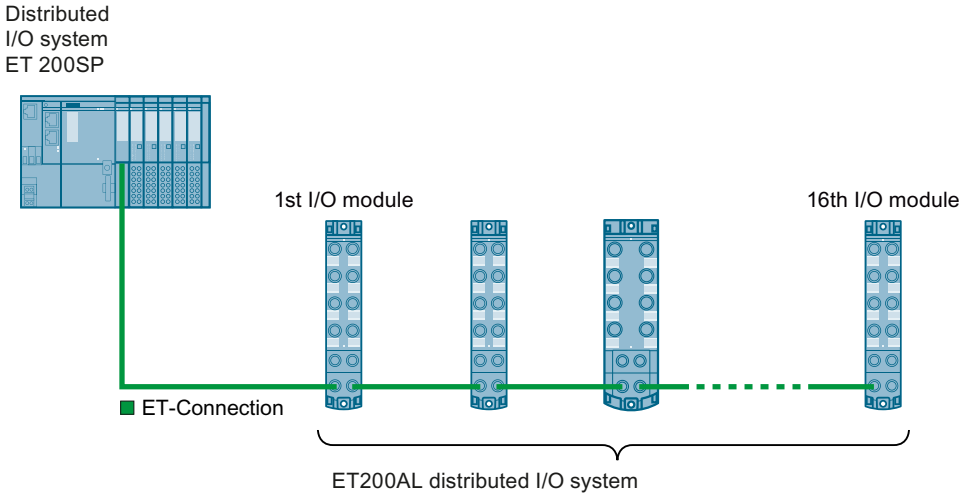


Figure 1 Mixed configuration ET 200SP and ET 200AL with ET-Connection

Requirement
The following components support mixed configuration:

- Interface module
  - IM 155-6 PN HF (V3.0 or higher)
  - IM 155-6 PN ST (V3.1 or higher)
  - IM 155-6 DP HF (V3.0 or higher)
- CPU
  - CPU 1510SP-1 PN (V2.0 or higher)
  - CPU 1510SP F-1 PN (V2.0 or higher)
  - CPU 1512SP-1 PN (V2.0 or higher)
  - CPU 1512SP F-1 PN (V2.0 or higher)
- BaseUnit BU-Send with BusAdapter BA-Send 1xFC
- ET-Connection cable
- Power cable

© Siemens 2014 - 2016. All rights reserved

Rules

You must observe the following rules when assembling a mixed configuration:

- The bus length of the ET 200SP distributed I/O system must not exceed 1 m (without interface module, including BU-Send/BA-Send 1xFC and server module)
- A maximum of 16 ET 200AL I/O modules can be connected to ET-Connection.
- The maximum length of the bus cable for ET-Connection between BA-Send and the first module or between two modules is 15 m.

The following table shows which firmware versions of your IM or CPU support which maximum bus cable length.

IM/CPU	2 m	5 m	10 m	15 m
IM 155-6 PN HF	V3.0 or higher	V3.0 or higher	V3.0 or higher	V3.3 or higher
IM 155-6 PN ST	V3.1 or higher	V3.1 or higher	V3.1 or higher	V3.3 or higher
IM 155-6 DP HF	V3.0 or higher	V3.0 or higher	V3.0 or higher	--
CPU 1510SP-1 PN	V2.0 or higher	V2.0 or higher	V2.0 or higher	V2.0 or higher
CPU 1510SP F-1 PN	V2.0 or higher	V2.0 or higher	V2.0 or higher	V2.0 or higher
CPU 1512SP-1 PN	V2.0 or higher	V2.0 or higher	V2.0 or higher	V2.0 or higher
CPU 1512SP F-1 PN	V2.0 or higher	V2.0 or higher	V2.0 or higher	V2.0 or higher

Procedure

To assemble a multi-tier configuration, follow these steps:

1. Install the BaseUnit BU-Send to the immediate right of the ET 200SP CPU/interface module.
   When the BaseUnit BU-Send is used next to the ET 200SP CPU, a CM DP and an Ethernet CP or a maximum of 2 Ethernet CPs can be inserted between the CPU and BU-Send.
2. Then mount the additional BaseUnits / I/O modules for the ET 200SP distributed I/O system and the server module.
3. Connect the bus cable for ET-Connection to the BusAdapter BA-Send 1xFC and mount this on the BaseUnit BU-Send.
4. Screw the BusAdapter BA-Send 1×FC to the BaseUnit BU-Send (1 screw with 0.2 Nm tightening torque). To do this, use a screwdriver with a 3 to 3.5 mm blade.
5. Connect the other end of the bus cable for ET-Connection (with M8 connector) to the first ET 200AL I/O module (X30 socket ET-Connection IN).
6. Connect the supply voltage (24 V DC) to the ET 200AL I/O modules (X80 connector).

NOTE

Firmware update of an ET 200AL I/O module

When you run a firmware update of an ET 200AL I/O module, ET-Connection is briefly interrupted by the restart of the module. All downstream ET 200AL I/O modules report a pull/plug interrupt.

Mounting

Introduction

For the connection of the ET 200AL I/O module via ET-Connection to the ET 200SP, you require the BaseUnit BU-Send with the BusAdapter BA-Send 1xFC.

Requirement

- The mounting rail is mounted.
- The interface module is mounted.

Required tools
3 to 3.5 mm screwdriver (only for dismantling the BusAdapter)

Mounting BaseUnit BU-Send
To mount the BaseUnit BU-Send, follow these steps:
1. Mount the BU-Send to the right of the CPU/interface module.
2. Swivel the BU-Send back until you hear the mounting rail release click into place.
3. Move the BU-Send to the left until you hear it click into place on the CPU/interface module.

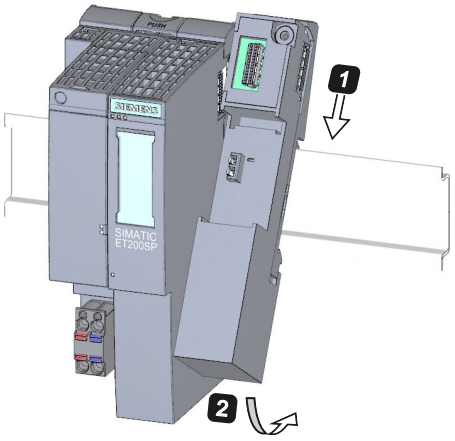
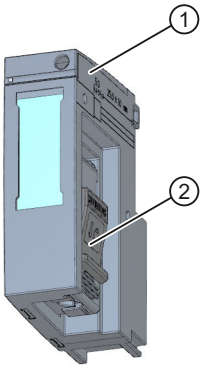


Figure 2 Mounting BU-Send

4. Mount the BusAdapter BA-Send 1xFC only after you have connected the bus cable for ET-Connection (see section Connecting (Page 3)).

Connection

Introduction
You connect the ET 200AL I/O modules via the BusAdapter BA-Send 1×FC using ET-Connection.



① BusAdapter BA-Send 1×FC
② Connection element for ET-Connection bus cable

Figure 3 BusAdapter BA-Send 1xFC

Required tools
Screwdriver with 3 to 3.5 mm blade

Required accessories
Use the bus cable for ET-Connection as connecting cable between the BusAdapter BA-Send 1xFC and the ET 200AL I/O modules.
We recommend using the stripping tool for ET-Connection (6ES7194-2KA00-0AA0) with blade cassette green (6GK1901-1B...). This guarantees fast and safe stripping.
The bus cable for ET-Connection M8, prefabricated on one side with 1 x M8 connector, 4-pole, shielded, is available in the following lengths:

- Length 2 m: 6ES7194-2LH20-0AC0
- Length 5 m: 6ES7194-2LH50-0AC0
- Length 10 m: 6ES7194-2LN10-0AC0
- Length 15 m: 6ES7194-2LN15-0AB0

Procedure
To connect the BusAdapter BA-Send 1xFC, follow these steps:

1. Strip the sheath of the bus cable at the open end as follows:

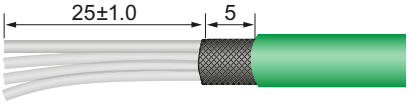
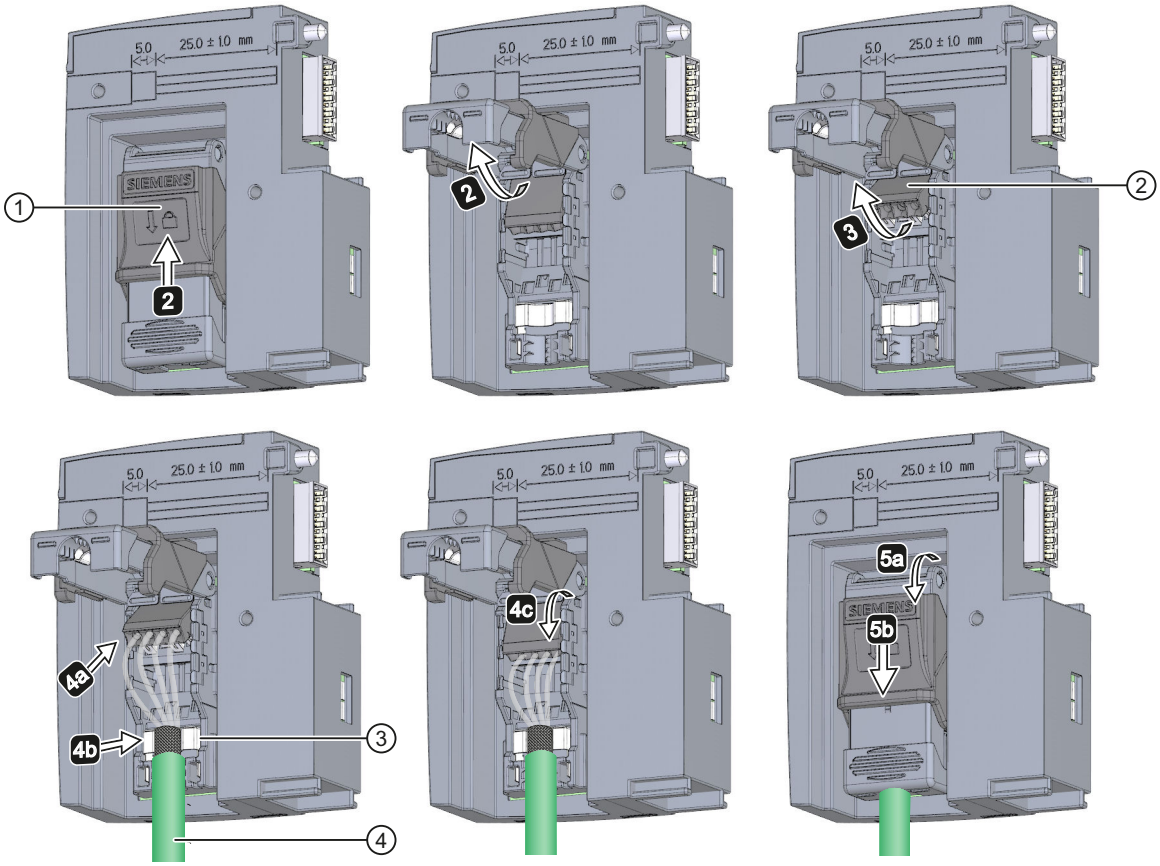


Figure 4 Connecting cable

Use the stripping tool for ET-Connection to do this. The relevant settings are shown on the tool.

2. Pull back the locking slide of the BusAdapter BA-Send 1×FC and open the cover of the connection element.
3. Lift the cable routing up as far as it will go.
4. Insert the unstripped single cores of the bus cable (according to the imprinted color coding) into the cable routing as far as they will go and press the cable routing down as far as it will go.
5. Close the cover of the connection element and push the locking slide forward.
6. Connect and screw the BusAdapter BA-Send 1×FC to the BaseUnit BU-Send (1 screw with 0.2 Nm tightening torque.) To do this, use a screwdriver with a 3 to 3.5 mm blade.

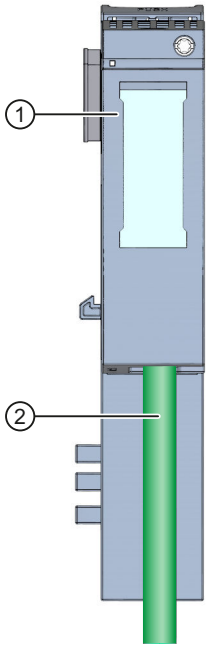
7. Connect the M8 connector of the bus cable to the first ET 200AL I/O module (socket X30 ET-Connection IN). For more information about wiring the ET 200AL I/O module refer to the system manual of the ET 200AL distributed I/O system.



①	Locking slide	③	Shield contact
②	Cable routing	④	Bus cable for ET-Connection

Figure 5 Connection of the BusAdapeter BA-Send 1xFC

BusAdapter BA-Send 1×FC mounted



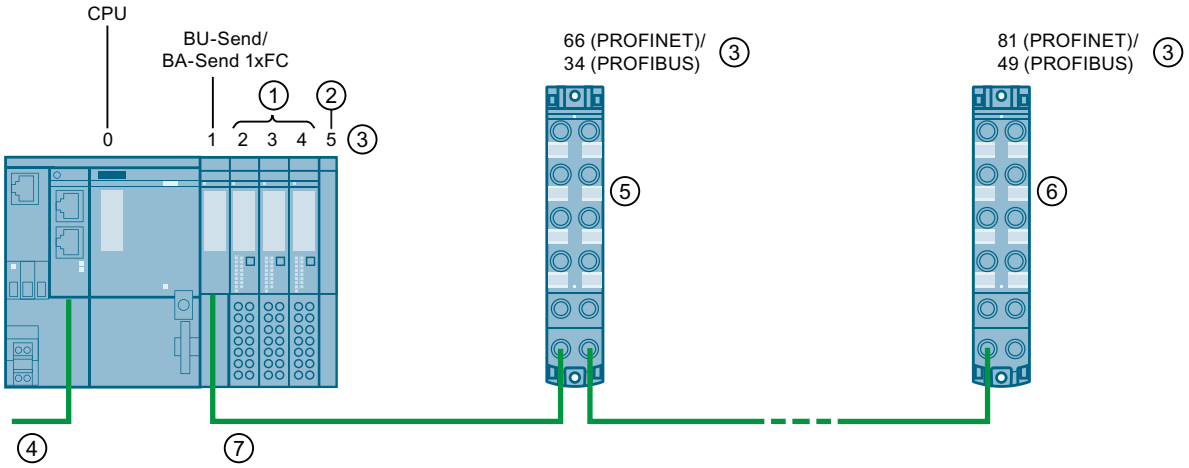
① BusAdapter BA-Send 1×FC
② Bus cable for ET-Connection

Figure 6 BusAdapter BA-Send 1×FC mounted

Configuring

Introduction

The mixed configuration allows the connection of up to 16 ET 200AL I/O modules to the ET 200SP via ET-Connection. The figure below shows the configuration of the ET-Connection and the assignment of the slots.



① ET 200SP I/O modules
② ET 200SP server module
③ Slots
④ PROFINET IO
⑤ 1st ET 200AL I/O module
⑥ 16th ET 200AL I/O module
⑦ ET-Connection

Figure 7 Mixed configuration

For more information about connecting the ET-Connection, supply voltages, actuators and sensors, refer to the ET 200AL system manual.

Configuration with a CPU

In a configuration with a CPU, a maximum of 2 slots can be used immediately to the right of the CPU with CM DP module or Ethernet CP. Combinations are also possible, i.e. CM DP module and one Ethernet CP or two Ethernet CPs.
BU-Send and BA-Send should always be inserted to the immediate right of the CM/CP.

Rules

Observe the following rules when configuring:

- With mixed configurations, the following maximum configuration is possible:
  - 31 (IM 155-6 DP HF and IM 155-6 PN ST)/63 (IM 155-6 PN HF and CPUs) slots for ET 200SP modules
  - 16 slots for ET 200AL I/O modules
  - 1 slot for BU-Send/BA-Send 1xFC
  - 1 slot for server module.
- The mixed configuration may contain a maximum of 31 (IM 155-6 DP HF and IM 155-6 PN ST)/63 (IM 155-6 PN HF) ET 200SP I/O modules.

- The server module can also be mounted right next to the BU-Send/BA-Send 1xFC.
- Supported functions:

Function	Mixed configuration		
	ET 200SP		ET 200AL I/O modules on ET-Connection
	IM	CPU	
Isochronous mode	⑥	--	--
Configuration control	⑥	⑥	⑥
Shared device	⑥	⑥	⑥
PROFIenergy	⑥	--	⑥
System redundancy S2	--	--	--

Configuring

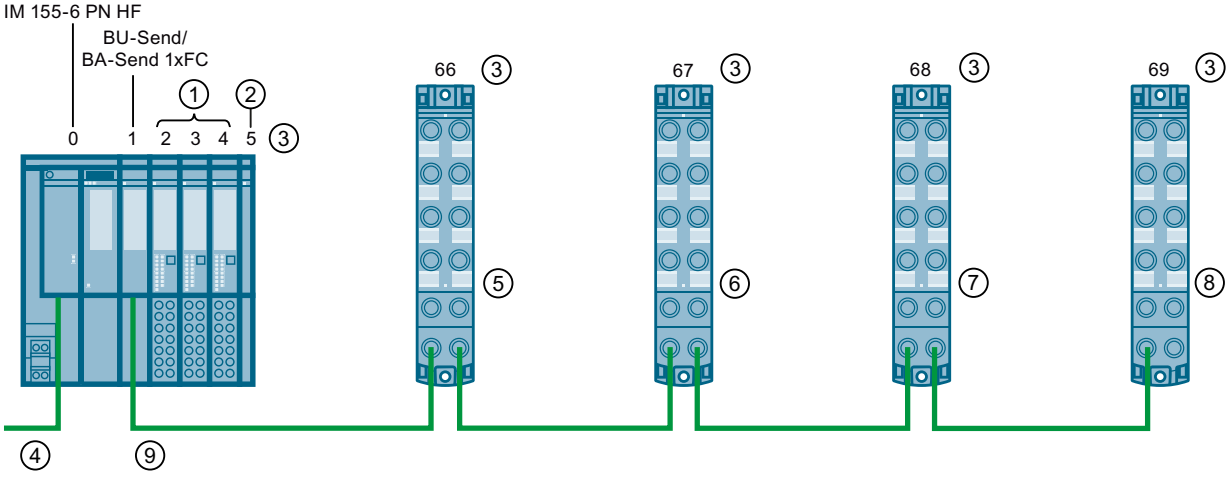
Observe the following points when configuring:

- BU-Send/BA-Send 1xFC and server module must be configured. With BU-Send/BA-Send 1xFC, no parameters are available.
- Arrangement of the modules in the configuration:
  - Configure the BU-Send/BA-Send 1xFC downstream from the interface module in slot 1. Position the ET 200SP modules behind it.
  - Configure the ET 200AL I/O modules from slot 66 (PROFINET)/67 (CPU)/34 (PROFIBUS).
- The layout of the modules represents a preset configuration and is independent of the configuration control.
- The system redundancy S2 function is not available in a mixed configuration.

Configuration example

An example of a mixed configuration is shown below:

Hardware configuration



① ET 200SP I/O modules
② ET 200SP server module
③ Slots
④ PROFINET IO
⑤ 1st ET 200AL I/O module
⑥ 2nd ET 200AL I/O module
⑦ 3rd ET 200AL I/O module
⑧ 4th ET 200AL I/O module
⑨ ET-Connection

Figure 8 Mixed configuration

Configuring configuration example

Table 1 Overview

Mixed configuration	Module	Slot
ET 200SP	IM 155-6 PN HF	0
	BA-Send 1xFC	1
	DI 16×24VDC ST	2
	DI 16×24VDC ST	3
	DI 16×24VDC ST	4
	Server module	5
ET 200AL	DI 8x24VDC 8xM8	66
	DIQ 4+DQ 4x24VDC/0.5A 8xM8	67
	AI 4xU/I/RTD 4xM12	68
	CM 4xIO-Link 4xM12	69

NOTE

Configuration using PROFIBUS GSD file

When you use the PROFIBUS GSD file for the configuration, you must configure the gaps between the server module and the first ET 200AL I/O module with BU-Cover.

BaseUnit BU-Send

Product overview

Article number
6ES7193-6BN00-0NE0

View

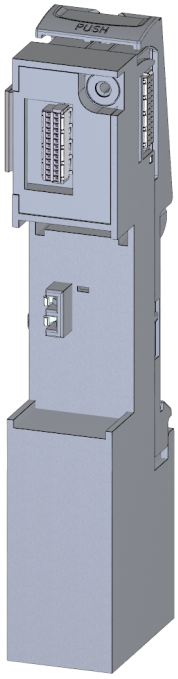


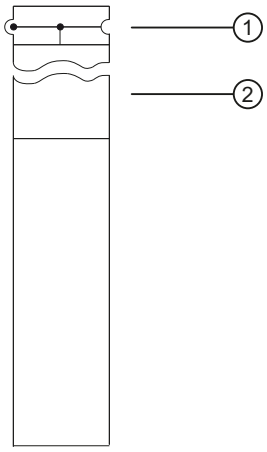
Figure 9 BaseUnit BU-Send

Properties
BaseUnit suitable for BusAdapter BA-Send 1xFC

Connection

Pin assignment
The BaseUnit BU-Send has only one slot for an expansion module. No other connections are available.

Schematic circuit diagram



① Backplane bus
② BA-Send 1xFC expansion module

Figure 10 Schematic circuit diagram BU-Send

Technical specifications

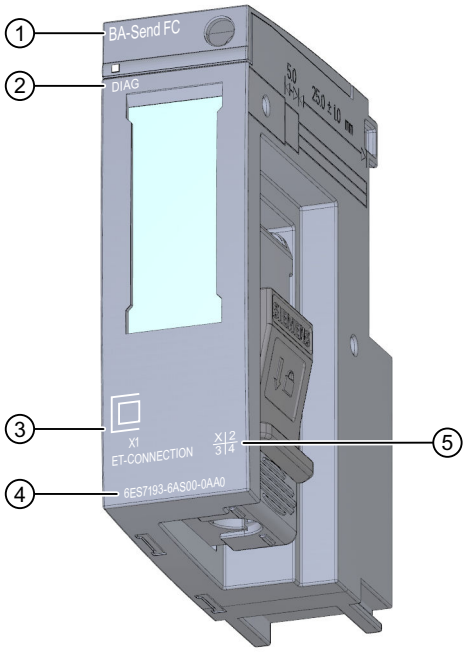
Technical specifications of the BaseUnit BU-Send

XE TDB_S	6ES7193-6BN00-0NE0
Product type designation XE T:0	BaseUnit BU-Send
Installation type/mounting XE U0:0	
Rack mounting possible XE B:1	Yes
Front installation possible XE B:1	Yes
Rail mounting possible XE B:1	Yes
Wall/direct mounting possible XE B:1	No
Hardware configuration XE U0:0	
Slots XE U1:1	
Number of slots XE N:2	1
Plug-in modules, other XE B:2	Yes; BusAdapter BA-Send
Dimensions XE U0:0	
Width XE N:1	20 mm
Height XE N:1	117 mm
Depth XE N:1	32 mm
Weights XE U0:0	
Weight, approx. XE N:1	30 g

BusAdapter BA-Send 1xFC
Properties

Article number
6ES7193-6AS00-0AA0

View of the module



① Module type and name
② LED for diagnostics
③ ((Connection for ET-CONNECTION))
④ Article number
⑤ Functional version

Figure 11 View of the BusAdapter BA-Send 1xFC

Properties
The module has the following technical properties:
- BusAdapter for the direct connection of ET-Connection
- Connects the interface module via ET-Connection with the ET 200AL I/O modules
- Supports all ET 200AL I/O modules

The module supports the following functions:
- Identification data I&M 0 to 3. See system manual ET 200SP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/58649293).

Maximum configuration

- 16 ET 200AL I/O modules
- 15 m bus cable between BusAdapter BA Send and the first ET 200AL I/O module and between two ET 200AL I/O modules.
- Supported functions:

Function	Mixed configuration		
	ET 200SP		ET 200AL I/O modules on ET-Connection
	IM	CPU	
Isochronous mode	⑥	--	--
Configuration control	⑥	⑥	⑥
Shared device	⑥	⑥	⑥
PROFIenergy	⑥	--	⑥
System redundancy S2	--	--	--

Accessories

The following components must be ordered separately:

- Labeling strips
- Reference identification label
- Stripping tool for ET-Connection
- Bus cables for ET-Connection

See also

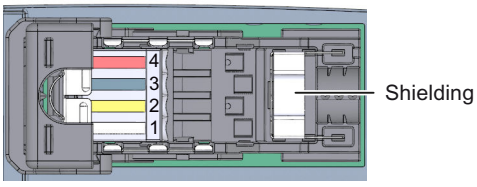
You can find more information on accessories and additional components in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

Pin assignment

ET-Connection with BusAdapter BA-Send 1xFC

The following table shows the signal names and the designations for the pin assignment of the BusAdapter BA-Send 1xFC.

Table 2 ET-Connection pin assignment with BusAdapter BA-Send 1×FC

View		Signal name	Description
Port 1 	1	TD	Transmit data +
	2	RD	Receive data +
	3	TD_N	Transmit data –
	4	RD_N	Receive data -

Schematic circuit diagram

Schematic circuit diagram

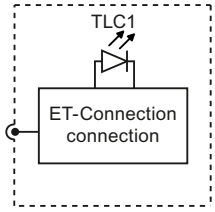
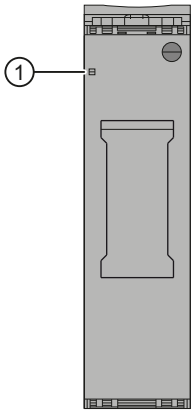


Figure 12 Schematic circuit diagram for BusAdapter BA-Send 1xFC

Diagnostics by means of LED display

LED display

The figure below shows the LED display (status and fault display) of the BusAdapter BA-Send 1xFC.



① DIAG (green/red)

Figure 13 LED display

Meaning of the LED display

The table below explains the meaning of the status and fault display.

DIAG LED

Table 3 Status and fault display DIAG

DIAG LED	Meaning	Remedy
□ Off	There is no connection between the ET-Connection interface of the BusAdapter BA-Send 1xFC and ET 200AL.	Check whether the bus cable is interrupted.
	The interface module does not support the BA-Send 1xFC.	Run a firmware update.

DIAG LED	Meaning	Remedy
On	There is a connection between the ET-Connection interface of the BusAdapter BA-Send 1xFC and ET 200AL.	---
Flashes	There is (at least) one diagnostics alarm of an ET-Connection device. Group error for all ET-Connection bus nodes.	Check the ET-Connection device.
	Set configuration does not match the actual configuration on the ET-Connection.	Check the configuration of the ET-Connection to see whether a module is missing or defective, or whether a non-configured module is wired.

Technical specifications

Technical specifications of the BusAdapter BA-Send 1xFC

XE TDB_S	6ES7193-6AS00-0AA0
Interfaces XE U0:0	
PROFINET IO XE U1:1	
Cable length XE U2:2	
Copper cables XE N:3	15 m; as of IM firmware V3.3: Bus nodes between BA-Send and the first ET-Connection as well as between all other bus nodes.
ET-Connection XE U1:1	
Number of interfaces ET-Connection XE N:2	1
FC (FastConnect) XE B:2	Yes
Ambient conditions XE U0:0	
Ambient temperature in operation XE U1:1	
Min. XE N:2	0 °C
Max. XE N:2	60 °C
Dimensions XE U0:0	
Width XE N:1	20 mm
Weights XE U0:0	
Weight, approx. XE N:1	44 g

SIEMENS

SIMATIC
ET 200AL
Product information for the documentation of the ET 200AL distributed I/O system

Product Information

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.
Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.
Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit (http://www.siemens.com/industrialsecurity).
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (http://www.siemens.com/industrialsecurity).

Safety-related shutdown of ET200AL standard modules

Introduction ET200AL standard modules safety-related shutdown
The diagram below illustrates the fail-safe shutdown of ET 200AL standard modules.
In the configuration shown in the diagram below, all digital outputs that are operated with the 2L+ and 2M supply of the ET 200AL standard modules are switched to the safe OFF state. This step achieves the safety class SIL2/category 3/PLd.

Principle of operation
The higher-level safety relay (for example: 3SK1) disconnects the 2L+ and 2M supply. This switches all digital outputs operated with the 2L+ and 2M (switched) supply to the safe state. The digital outputs connected to the 1L+ and 1M (non-switched) supply are not intended for functional switching and therefore cannot be shut down safely.
There is no interaction between the outputs supplied by 1L+ and 2L+. Safety relay

© Siemens 2014 - 2016. All rights reserved

Block diagram

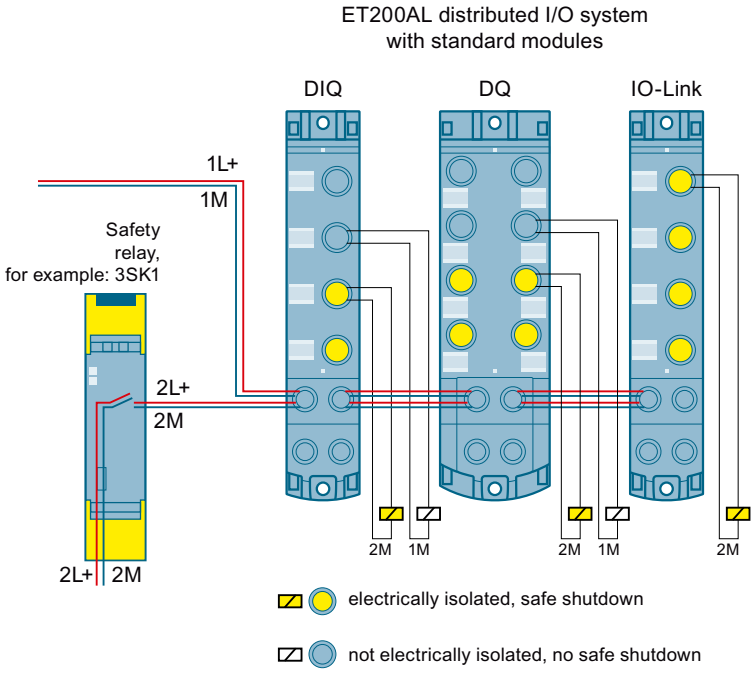


Figure 1 Higher-level safety circuit with safety relay

Requesting TÜV certificate (report no. SN89858T, revision 1.0 dated 18 August 2016) TÜV certificate
You can request copies of the TÜV certificate and the accompanying report at the following address:
Siemens AG
Digital Factory
DF FA AS DH AMB
Postfach 1963
D-92209 Amberg

Reference
You can find additional information as well as an overview of the modules with safety-related shutdown on the Internet (https://support.industry.siemens.com/cs/us/en/view/39198632).

SIEMENS

SIMATIC

ET 200AL
IM 157-1 MF
(6ES7157-1MA00-0AB0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Connecting 4

PROFINET IO 5

EtherNet/IP 6

Modbus TCP 7

Parameters 8

Operation and maintenance 9

Technical specifications 10

Dimension drawing 11

Cycle times A

05/2025
A5E52816358-AB

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 Tool support 6
1.2 MultiFieldbus Configuration Tool (MFCT) 7
1.3 SIMATIC Technical Documentation 8

2 Industrial cybersecurity 10

2.1 Introduction to industrial cybersecurity 10
2.2 Cybersecurity information 10
2.3 Cybersecurity-relevant information 11

3 Product overview 13

3.1 Properties 13
3.2 Operator controls and display elements 15
3.3 MultiFieldbus engineering 16
3.4 Detect active fieldbus 16

4 Connecting 17

4.1 Terminal and block diagram 17
4.2 Pin assignment 18

5 PROFINET IO 20

5.1 PROFINET IO functions 20
5.1.1 PROFINET IO 20
5.1.2 Media redundancy 22
5.1.3 Real-time communication 22
5.1.4 Isochronous real-time communication 22
5.1.5 Prioritized startup 23
5.1.6 System redundancy S2 23
5.1.7 Shared device 24
5.1.8 Device replacement without programming device 24
5.1.9 PROFIenergy 25
5.1.9.1 What is PROFIenergy? 25
5.1.9.2 Principle of operation 26
5.1.9.3 Parameter assignment 28
5.1.9.4 PROFIenergy control data records 29
5.1.10 Configuration control (option handling) 30
5.1.11 Interface local coupling of IO data 31

5.2 Interrupts, error messages, diagnostics and system alarms ... 33
5.2.1 Status and error displays for PROFINET IO ... 33
5.2.2 Interrupts ... 35
5.2.2.1 Evaluating interrupts ... 35
5.2.2.2 Trigger a diagnostics interrupt ... 36
5.2.2.3 Triggering a hardware interrupt ... 36
5.2.2.4 Triggering an insert/remove module interrupt ... 36
5.2.3 Alarms ... 37
5.2.3.1 Diagnostics alarms ... 37
5.2.3.2 Maintenance events ... 38
5.2.3.3 Channel diagnostics ... 39
5.2.3.4 Invalid configuration states of ET 200AL on the PROFINET IO ... 39
5.2.3.5 STOP of the IO controller and recovery of the IO device ... 39

6 EtherNet/IP ... 40

6.1 Supported EtherNet/IP functions ... 40
6.2 Applicable modules with EtherNet/IP ... 41
6.3 Update time of the I/O data ... 42
6.4 I/O data mapping ... 42
6.5 MF Shared Device ... 44
6.6 Diagnostics ... 46
6.6.1 Status and error displays for EtherNet/IP ... 46

7 Modbus TCP ... 50

7.1 Supported Modbus TCP functions ... 50
7.2 Modules that can be used with Modbus TCP ... 51
7.3 Update time of the I/O data ... 51
7.4 I/O data mapping ... 52
7.5 MF Shared Device ... 54
7.6 Diagnostics ... 55
7.6.1 Status and error displays for Modbus TCP ... 55

8 Parameters ... 59

8.1 Parameters ... 59
8.2 Explanation of the parameters ... 59

9 Operation and maintenance ... 61

9.1 Firmware update ... 61
9.2 Resetting an interface module to factory settings ... 61

10 Technical specifications ... 62

11 Dimension drawing ... 67

A Cycle times ... 68

Introduction

1

Purpose of this documentation

This Equipment Manual supplements the System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965). Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209) Function Manual describes general MultiFieldbus functions. This Equipment Manual describes the specific adaptations for this I/O device.

The information provided in the present manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Changes compared to the previous version

This manual contains the following changes/additions compared with the previous version:

- Adaptations in the Technical specifications (Page 62) section
- Adaptations in the Cycle times (Page 68) section

Conventions

Also observe notes marked as follows:

NOTE

A note contains important information:

- On the product described in the documentation
- On handling the product
- On the part of the documentation to which particular attention is paid

---

1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.1 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 MultiFieldbus Configuration Tool (MFCT)

MultiFieldbus Configuration Tool

MultiFieldbus Configuration Tool (MFCT) is a PC-based software and supports the configuration of MultiFieldbus- and DALI-devices. In addition, the MFCT offers convenient options for mass firmware updates of ET 200 devices with MultiFieldbus- support and reading service data for many other Siemens devices.

Functional scope of the MFCT

- MultiFieldbus configuration:
  Engineering, configuration and diagnostics of MultiFieldbus-devices, provision of the required project files (project, UDT-, CSV- and EDS-file), transfer/export of the files to device and/or data memory.
- DALI configuration:
  Device selection and online configuration of DALI devices.
- TM FAST:
  Generation and download of FPGA-UPD- and FPGA-DB-files.
- Maintenance:
  Topology scan of a Ethernet network, reading of service data, parameter assignment and firmware update.
- Settings:
  Language switching German / English, network scanner speed, setting of the network adapter, installation of GSDML-and EDS-files.

System/installation requirements for MFCT

The MFCT runs under Microsoft Windows and does not require installation or administrator rights.

For MFCT you must also install the following software:

- Microsoft .NET Framework 4.8 (You can find an Offline Installer on the Internet. (https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0))
- NPcap from directory "Misc"
- PG/PC interface from directory "Misc"
- Microsoft C++ Redistributable for x86-systems (you can find the installation data for download on the Internet. (https://aka.ms/vs/15/release/vc_redist.x86.exe))

The download of the tool and further information as well as documentation on the individual functions of the MFCT can be found on the Internet.
(https://support.industry.siemens.com/cs/de/en/view/109773881)

1.3 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the SIMATIC ET 200AL Distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965) System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-relevant information pertaining to your SIEMENS device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all cybersecurity-relevant information.

Topics with cybersecurity-relevant information	Reference
Operational application environment and security assumptions	
Requirements for the operational application environment of the system and security assumptions	This section can be found in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Security properties of the product	
Access protection	Also note the information on access protection in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965), Protection section.
Data integrity	Data integrity is described in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965), Industrial cybersecurity section.
Signed firmware update	Signed firmware update is described in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965), Industrial cybersecurity section.
PROFINET Security Class 1 • The device supports PROFINET Security Class 1. • With the introduction of PROFINET Security Class 1, additional security settings have been integrated into the PROFINET communication.	You can find detailed information on PROFINET Security Class 1 and the additional security settings in the PROFINET with STEP 7 Function Manual (https://support.industry.siemens.com/cs/us/en/view/49948856).
Supported Ethernet services	You can find information on supported services in the Technical specifications (Page 62) section. You can find detailed information on supported Ethernet services in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Interfaces, ports, protocols and services	
Information on the following is relevant for security: • Communications layer and communication role • Default states • Enabling/disabling of ports and services	You can find detailed information on these topics in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Secure operation	
Recommendations for secure operation	You can find cross-system information on secure operation of interface modules in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Corrective measures for known risks	Corrective measures for known risks are announced on the Siemens ProductCERT and Siemens CERT (https://siemens.com/productcert) web page. You can find more information on SIEMENS ProductCERT in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).

Topics with cybersecurity-relevant information	Reference
Security checks	You can find a description of application-related security measures, such as cyclic checks of the configuration via checksums, in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965), Industrial cybersecurity section.
Secure decommissioning Products that contain security-relevant data must be securely decommissioned before disposal or resale.	You can find information on secure decommissioning in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965), Secure operation of the system section

Product overview

3

3.1 Properties

Article number

6ES7157-1MA00-0AB0

View of the module



Figure 2-1 View of the IM 157-1 MF interface module

Properties

The module has the following technical properties:

- Connects the ET 200AL distributed I/O system with these fieldbuses:
  - PROFINET IO
  - EtherNet/IP
  - Modbus TCP
- 24 V DC supply voltage
- Support for 2 ET-Connection lines
- Dimensions: 45 x 159 x 40 mm

The functions supported by the module can be found in these sections:

- PROFINET IO functions (Page 20)
- Supported EtherNet/IP functions (Page 40)
- Supported Modbus TCP functions (Page 50)

Maximum configuration

The module has the following maximum configuration:

- 1440 bytes input data
- 1440 bytes output data
- 32 I/O modules, up to 16 I/O modules can be connected to each ET-Connection line

NOTE

- In the case of a shared device configuration, the sum of the I/O data of all controllers that share the device applies.
- If more than 2 (max. 4) controllers share the device, the maximum amount of I/O data including user data qualifiers is limited to 360 bytes per controller.

Accessories

The following component is included with the module in the packaging:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

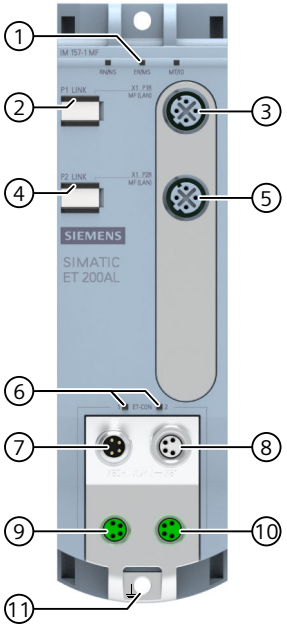
- Connectors
- Cables
- Stripping Tool for PROFINET
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You will find more information on accessories and the other components in the System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965) in the Accessories/Spare parts section.

3.2 Operator controls and display elements

The figure below shows the operator control and display elements of the IM 157-1 MF interface module.



① RN/NS, ER/MS, MT/IO: LED indicators for the current operating state and diagnostic status
② P1 LINK: LED indicators for the current operating state of the 1st MultiFieldbus interface
③ X1 P1R: 1. MultiFieldbus interface
④ P2 LINK: LED indicators for the current operating state of the 2nd MultiFieldbus interface
⑤ X1 P2R: 2. MultiFieldbus interface
⑥ ET-CON1, ET-CON2: LED indicators for ET-Connection
⑦ X80: Connector for infeed of the supply voltage (POWER input)
⑧ X81: Socket for looping-through the supply voltage (POWER output)
⑨ X30: Socket for ET-Connection1
⑩ X31: Socket for ET-Connection2
⑪ Functional grounding (FE)

Figure 2-2 Operator controls and display elements

3.3 MultiFieldbus engineering

MultiFieldbus Configuration Tool (MFCT)

The configuration and parameter assignment of the MultiFieldbus interface module is created and downloaded with MFCT and stored retentively in the interface module.

MFCT creates the following files and makes them available:

- UDT (User Defined Data Types) file (file extension *.l5x), enables structured access to I/O data with EtherNet/IP.
- Electronic Data Sheet (EDS) according to CIP Specification Vol. 1 for integrating into EtherNet/IP configuration systems.
- Comma Separated Values (CSV), contains the I/O data mapping of your configuration

You can find more information on MFCT in the "SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209)" Function Manual.

3.4 Detect active fieldbus

For exclusive operation on a fieldbus (not MF Shared Device) you can recognize the active fieldbus by the number of green LEDs on the MF device.

This requires that there are no errors and that the MF device is in cyclic data exchange with a controller.

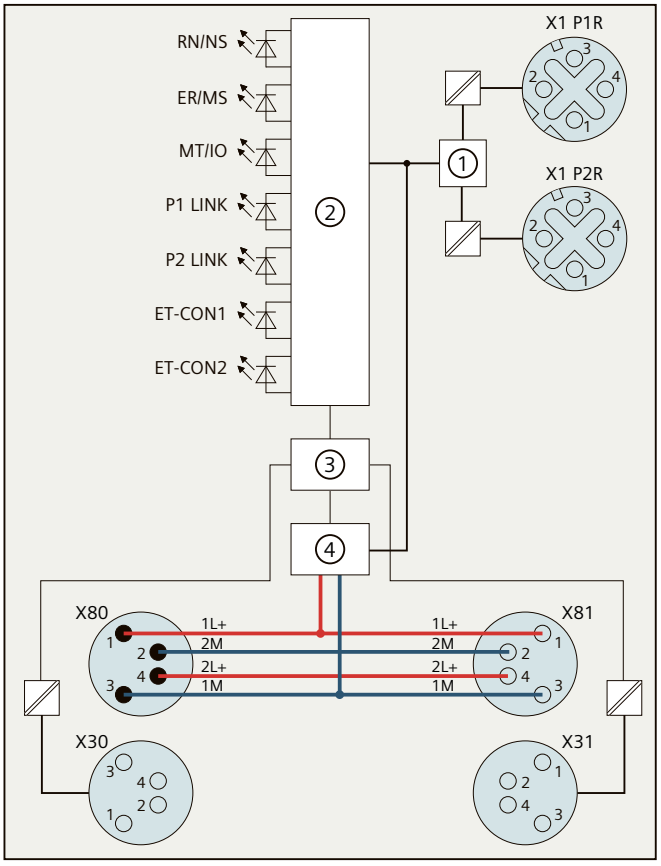
LED schematic:	RN/NS	ER/MS	MT/IO
PROFINET	■ Green	□ Off	□ Off
Modbus TCP	■ Green	■ Green	□ Off
EtherNet/IP	■ Green	■ Green	■ Green

Connecting

4

4.1 Terminal and block diagram

The figure below shows the connection and schematic circuit diagram of the IM 157-1 MF interface module.



①	Switch	1L+	Supply voltage 1L+ (non-switched)
②	Electronics	1M	Ground 1M (non-switched)
③	ET-Connection interface	2L+	Load voltage 2L+ (switched)
④	Internal supply voltage	2M	Ground 2M (switched)
X1 P1R	1st MultiFieldbus interface:	RN/NS	Operating status LED (red/green)
X1 P2R	2nd MultiFieldbus interface:	ER/MS	Diagnostic status LED (red/green)
X80	Infeed of supply voltages	MT/IO	Diagnostic status LED (red/green/yellow)
X81	Loop-through of supply voltages	P1 LINK, P2 LINK	MultiFieldbus status LEDs (green)
X30	1st ET-Connection interface	ET-CON1, ET-CON2	ET-Connection LEDs (green)
X31	2nd ET-Connection interface		

Figure 2-3 Terminal and block diagram

4.2 Pin assignment

NOTE

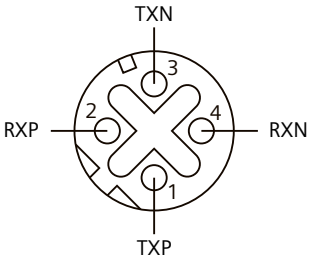
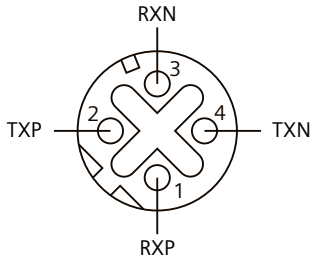
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the MultiFieldbus sockets

The following table shows the pin assignment of the 2 sockets for MultiFieldbus.

Table 2-1 Pin assignment of the MultiFieldbus sockets

Pin	Assignment		Front view of the sockets	
	X1 P1R socket	X1 P2R socket	X1 P1R	X1 P2R
1	TXP	RXP		
2	RXP	TXP		
3	TXN	RXN		
4	RXN	TXN		
Shield-ing	Functional earth FE			

NOTE

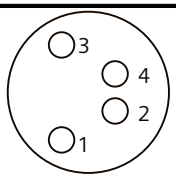
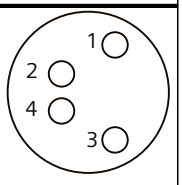
Pin assignments

If you disable "Autonegotiation" in STEP 7, you must pay attention to the different pin assignments of X1 P1R and X1 P2R.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

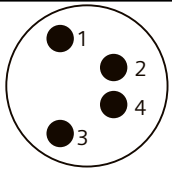
Table 2-2 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection1)	X31 socket (ET-Connection2)		X30	X31
1	RXP	RXP	Yellow		
2	TXP	TXP	White		
3	TXN	TXN	Blue		
4	RXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The following table shows the pin assignment for infeed of the supply voltage.

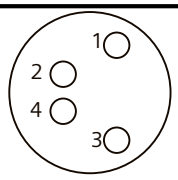
Table 2-3 Pin assignment of the supply voltage connector

Pin	Assignment X80 connector (power input)	Assignment of the wire color of the power line cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The following table shows the pin assignment for loop-through of the supply voltage.

Table 2-4 Pin assignment of the supply voltage socket

Pin	Assignment X81 Socket (power output)	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage

Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage.
If you interchange the connectors for ET-Connection and the connector for the supply voltage, the module may be destroyed.

⚠ CAUTION

MultiFieldbus

Modules with MultiFieldbus interfaces may only be operated under the following condition:
All connected devices must be equipped with SELV/PELV power supplies.

PROFINET IO

5

5.1 PROFINET IO functions

5.1.1 PROFINET IO

Introduction

The interface module supports the following PROFINET IO functions:

- Integrated switch with 2 ports
- Supported Ethernet services: ping, arp, network diagnostics (SNMP)/MIB-2, LLDP
- Port diagnostics
- Deactivating of ports
- Real-time communication
- Isochronous real-time communication
- Minimum update time 250 µs
- Media redundancy (MRP)
- Media redundancy with planned duplication (MRPD)
- Device replacement with topological configuration
- Device replacement without topological configuration
- Shared Device
- Identification data I&M0 to I&M4
- PROFIenergy
- Configuration control (option handling)
- Value status (of I/O modules)
- System redundancy S2
- Prioritized startup
- Local data coupling
- Reset to factory settings via PROFINET IO
- Secure and complete deletion of retentive data
- Integrity of information
- Secure firmware update via PROFINET IO
- Secure Boot
- PROFINET Security Class 1

Requirements

The following table shows the software requirements for the use of PROFINET IO functions with the IM 157-1 MF interface module.

Table 2-5 Software requirements for PROFINET IO functions

PROFINET IO function	Configuration software	
	STEP 7 (TIA Portal) V13 or higher (with GSD file)	STEP 7 V5.5 SP4 or higher (with GSD file)/Software from third-party manufacturer[2]
Real-time communication	X	X
Isochronous real-time communication	X	X
Device replacement without programming device	X	X
Media redundancy	X	X
Shared device	X[1]	X

1 Use a S7-1500 CPU as a controller to use a shared device with STEP 7 (TIA Portal).

2 Systems of third-party manufacturers: Depending on the range of functions of the third-party system

Cabling with fixed connection setting

If you configure a fixed connection setting for the port in STEP 7, you also have to disable "Autonegotiation/Autocrossover". By disabling "Autonegotiation/Autocrossover" you speed up establishment of the communication path.

Replacement of an IM 157-1 MF

If you replace an interface module that has already been used, you must reset this interface module to the delivery state with "Reset to factory settings".

You will find more information on "Resetting to factory settings" in the System Manual ET 200AL Distributed I/O System (https://support.industry.siemens.com/cs/ww/en/view/89254965).

Reference

You will find more information on the PROFINET IO functions in the Function Manual SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856) and in the STEP 7 online help.

5.1.2 Media redundancy

Media redundancy

Function for ensuring communication and plant availability. Redundant transmission links (ring topology) ensure that another communication path is made available in the event of a transmission link failure.

5.1.3 Real-time communication

Real-time communication

A transmission method for PROFINET IO based on cyclic data exchange with a provider-consumer model.

Detailed information

You can find additional information on the topic of **Real-time communication** in the STEP 7 online help and in the function manual SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

5.1.4 Isochronous real-time communication

Isochronous real-time communication

Synchronized communication protocol for cyclic exchange of IRT data between PROFINET devices. A reserved bandwidth is available within the send cycle for IRT I/O data. The reserved bandwidth ensures that the IRT data is transmitted at reserved, synchronized intervals while remaining uninfluenced by another greater network load (for example, TCP/IP communication or additional real-time communication).

- IRT option:
  A topological configuration is required
  - From STEP 7 V5.5 and higher
  - From TIA V19 or higher with HSP 0419 and higher

NOTE

IO controller as a sync master with IRT communication
Operate the IO controller also as a sync master when configuring IRT communication. Otherwise, IRT and RT configured IO devices can fail if the sync master fails.

Detailed information

You can find additional information on the topic of **isochronous real-time communication** in the STEP 7 online help and in the SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856) function manual.

5.1.5 Prioritized startup

Prioritized startup

Prioritized startup denotes the PROFINET functionality for accelerating the startup of IO devices operated on a PROFINET IO system with RT and IRT communication.

The function reduces the time that the correspondingly configured IO devices require to return to the cyclic user data exchange in the following cases:

- After the supply voltage has returned
- After station recovery
- After IO Devices have been activated

You can recognize valid input values and output values from the value status QI = 1. In the case of analog devices and IO-Link master communication modules, the determination of the analog value or the establishment of the IO-Link connection can take more time, for example. You will receive invalid values with the value status QI = 0 until then.

Detailed information

You can find more information on the topic of **Prioritized startup** in the STEP 7 online help and in the Function Manual SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

5.1.6 System redundancy S2

System redundancy S2

An IO device with S2 system redundancy supports redundant ARs.

In a redundant system, an IO device with system redundancy S2 has a redundant AR for each of the two CPUs (IO controllers). If one CPU fails, the IO device with S2 system redundancy remains accessible to the remaining IO controller via the AR.

The I/O devices support system redundancy S2 (as of FW V1.0.0) on S7-400H CPUs (as of FW V3.0) and on S7-1500R/H CPUs (as of FW V2.6).

NOTE

Restrictions in operation with activated system redundancy S2

You cannot use the following functions during operation of the IM157-1 MF, firmware version V1.0 with activated system redundancy S2:

- Configuration control (option handling)
- Local data coupling of IO data

Detailed information

You can find additional information on the topic of **system redundancy S2** in the STEP 7 online help and in the function manual SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

5.1.7 Shared device

Shared device

IO device that makes its data available to up to 4 PROFINET IO controllers.

If **there is no validity check of the shared device projects by the Engineering System**, note the following:

- Make sure the configurations are consistent. Assign each module or submodule to only one IO controller. Multiple assignment will result in an error as the module or submodule will only be available in the first controller.
- If you reconfigure shared device configurations without the validity check mentioned above, you have to commission the ET 200AL once again. This means that after reconfiguration, you must download the projects of all involved PROFINET IO controllers to the respective CPU once again. If necessary, perform a POWER OFF/POWER ON of the IO controller and the I/O device.

NOTE

Ensure with Shared Device applications that all controllers work with the same send clock. If the controller does not have the same send clock, this may result in communication relationships not being set up.

If you set up all controllers in one project, the same send clock is ensured. Set the same send clock for engineering in separate projects.

Detailed information

You can find additional information on the topic of **shared device** in the STEP 7 online help and in the SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856) function manual.

5.1.8 Device replacement without programming device

Device replacement without programming device

IO devices with this function can easily be replaced. You do not have to assign the device name with the PG.

The replacement IO device is assigned the device name by the IO controller and not by the PG. The IO controller uses the configured topology and the neighboring relationships determined by the IO devices for this purpose. To do this, all devices involved must support the LLDP protocol (Link Layer Discovery Protocol). The configured target topology must match the actual topology.

IO devices which were already used in another configuration must be reset to factory settings before being reused.

5.1.9 PROFIenergy

5.1.9.1 What is PROFIenergy?

Introduction

PROFIenergy is a PROFINET-based data interface which makes it possible to switch off consumers in a coordinated and centrally controlled manner during break times regardless of the manufacturer or device. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

PROFINET devices are switched off with special commands in the user program of the PROFINET IO controller. Additional hardware is not needed: The PROFIenergy commands are interpreted by the PROFINET devices.

The device which provides PROFIenergy and supports the matching control data record owns the PE-Entity, the access point for these control data records. This PE-Entity represents I/O modules which do not have their own PE-Entity on the interface module. I/O modules that have their own PE-Entity are always addressed directly.

For the ET 200AL distributed I/O system, the PE-Entity is exclusively provided by the PROFINET interface module.

Procedure

To configure PROFIenergy, follow these steps:

1. Create the parameter data record, Index 3, in STEP 7.
2. Transfer the parameter data record to the interface module with the instruction "WRREC" - SFB 53.
3. Create the user program with the FBs to control the PROFIenergy commands ("PE_START_END" - FB 815, "PE_CMD" - FB 816).
4. Transfer the user program to the CPU.

Additional information

You will find more information on the Internet (http://www.profibus.com) under Common Application Profile PROFIenergy; Technical Specification for PROFINET; as well as in the following documentation:

- System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965)
- Equipment Manuals ET 200AL I/O modules (https://support.industry.siemens.com/cs/ww/en/ps/14247/man)
- System Manual SIMATIC PROFINET System Description (https://support.industry.siemens.com/cs/ww/en/view/19292127)
- Function Manual SIMATIC PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856), section: Saving energy with PROFIenergy

- Application guide for implementation of shutdown concepts with PROFIenergy. (https://support.industry.siemens.com/cs/ww/en/view/96837137)
- PROFIenergy - Saving Energy with SIMATIC S7 (STEP 7 V5.5) (https://support.industry.siemens.com/cs/ww/en/view/41986454)
- SIMATIC S7 Library for Easy Configuring of PROFIenergy (https://support.industry.siemens.com/cs/ww/en/view/109478388)
- You will find additional information on the PROFIenergy FBs ("PE_START_END" - FB 815, "PE_CMD" - FB 816) in the online help for STEP 7 V5.5 SP2 and higher on system functions/system function blocks.

Application examples and manual information are also available online FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

5.1.9.2 Principle of operation

"Pause" control and "Pause" behavior

At the beginning/end of pauses, enable/disable the pause function on the system; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules. The module then interprets the content of the PROFIenergy command and turns it off or on again. The ET 200AL interface module is the PE-Entity for the PROFIenergy-capable I/O modules of the ET 200AL distributed I/O system in this case.

Device information can be called up using additional PROFIenergy commands during the pauses. You can use these commands to transfer the "Start_Pause" / "End_Pause" command in good time.

NOTE

A complete PROFIenergy sequence consists of the commands "Start_Pause" and "End_Pause". Always observe this sequence during programming.

LED displays

PROFIenergy generally has no effect on the LED display. Exceptions can be found in the device manuals of the I/O modules.

Response to error detection

All channels whose pause mode is set to "PE_MODE_PROCEED" report errors as in productive operation.

The following rules apply to channels which switch to a pause mode other than "PE_MODE_PROCEED":

- All errors that are unrelated to the switch to "Pause" are reported.
- If error recognition is possible during "Pause", these errors continue to be reported.
- All error messages which are caused by the switch to "Pause" are suppressed.

- The following applies if error recognition is not possible during the "Pause":
  - The status of errors already pending before the "Pause" is retained.
  - Incoming and outgoing errors are reported once the "Pause" has been ended.

NOTE
Switching to "Pause" and out of "Pause" may cause an error to be reported.

Additional information

Additional information on diagnostics can be found in the I/O module device manuals.

Hardware interrupt

Ending a "Pause" causes hardware interrupts to be detected again.

"Pause" behavior under certain operating conditions

A "Pause" is ended in the following cases:

Table 2-6 Ending a "Pause"

Ending a "Pause"	Explanation
The supply voltage 1L+ of the interface module module has failed.	The "pause" is exited and can be re-activated by re-sending the PROFIenergy parameter assignment followed by the "Start_Pause" command.
• Stop controller[1] • Controller failure (connection interrupted)[1] • Firmware update • Reset to factory settings • Deactivating the IO device[1]	
The I/O module was pulled and plugged	
Station stop[1] • Removing an I/O module	The "pause" is exited , the PROFIenergy parameter assignment is still on the I/O module and the "pause" can be re-activated by the "Start_Pause" command.
The supply voltage 1L+ of the I/O module has failed	
The parameter settings of the I/O module were changed during operation using data record 128	

[1] The substitute value behavior was activated.

5.1.9.3 Parameter assignment

Parameter assignment

Keep the following points in mind when assigning parameters for PROFIenergy:

- Parameters for PROFIenergy are assigned with the parameter data record (version 2), index 3. The interface module distributes the PROFIenergy parameters to the I/O modules.
- The parameter assignment of an additional pause behavior is possible immediately after the start of the previous "Pause". The required state for the following pause is activated with a new "Start_Pause" command.
- You can write the parameter assignment as often as needed.
- The interface module checks the distribution of the parameters to the I/O modules and returns the result as a return value of the write job. In the case of a negative return value, there are one or more I/O modules that have not accepted the parameter data record. In this case, the I/O modules respond according to their last PROFIenergy parameter assignment in case of an incoming "Start_Pause" command. "Start_Pause"/"End_Pause" commands can be executed as planned with a positive return value.
- In case of a failure of an I/O module or station outage, you must repeat the parameter assignment using the parameter data record.
- The ET 200AL distributed I/O system supports configuration of the behavior of **a** "pause". If a different response is required for an additional "Pause", you will have to assign parameters again.

NOTE

Effect: The response (switch-off) of the I/O modules to PROFIenergy is related to the slot, which means all channels in the slot behave accordingly.

Parameter data record

You specify in the parameter data record for PROFIenergy which I/O modules (slots) are controlled with the PROFIenergy commands.

The following table shows the content of the parameter data record for PROFIenergy, index 3, which you create yourself and can transfer to the interface module.

Table 2-7 Parameter data record for PROFIenergy (version 2), index 3

Byte	Element		Code	Explanation
0	Version		02_D	Cannot be modified
1	Number of blocks		01_D to 34_D	Slots 1 to 34 depending on the configuration of the distributed I/O system ET 200AL
2	Block 1	Slot number	00_D	Not assigned
			01_D to 34_D	I/O module slot with PROFIenergy

1 The specific behavior depends on the used I/O module (with a digital input module, for example, the sensor supply is turned off or the outputs are without power supply and voltage supply with an analog output module)

2 An analog output module (e. g. with the output range 0 mA to 20 mA, ± 20 mA) or a digital output module issues the value "0".

Byte	Element		Code	Explanation
3	Block 1	Mode	0_D: PE_MODE_PROCEED, proceed at "Pause" 1_D: PE_MODE_SHUTDOWN, shut down at "Pause" [1] 3_D: PE_MODE_LAST_VALUE, last output or measured value is retained 4_D: PE_MODE_SUBST_VALUE, substitute value "0" [2]	
:	:	:	:	
64	Block 32	Slot number	See Block 1	
65		Mode		

1 The specific behavior depends on the used I/O module (with a digital input module, for example, the sensor supply is turned off or the outputs are without power supply and voltage supply with an analog output module)

2 An analog output module (e. g. with the output range 0 mA to 20 mA, ± 20 mA) or a digital output module issues the value "0".

Error messages

The following table shows which error messages the feedback data record returns, if necessary:

Table 2-8 Error messages

Error code	Meaning	
$80B1_H$	Impermissible length	Check the length of the data record
$80E0_H$	Error in header information	Check the data record header information
$80E1_H$	Parameter error • at least one I/O module does not support PROFIenergy • A parameter value has been incorrectly encoded	Check the content of the data record and correct the parameter assignment error before starting the "Pause". Parameter assignment errors which are not corrected can result in incorrect I/O module shutdown behavior.

5.1.9.4 PROFIenergy control data records

PROFIenergy control data records

The control data record for PROFIenergy, Index $80A0_H$, supports the following services for the IM 157-1 MF interface module:

Table 2-9 Control data records for PROFIenergy

Service	Service ID	Meaning
Start pause [1]	01_H	Assuming the configured Pause behavior, suppressing all associated diagnostics data
End Pause	02_H	Leaving the pause
Query Modes	03_H	Reads the supported modes • Request List Energy Saving Modes • Request Get Mode (Energy Saving Mode Data)
PEM status	04_H	Reading the PROFIenergy status
PE_Identify	05_H	Reading the supported PROFIenergy services

1 The minimum (configurable) pause time for the ET 200AL distributed I/O system is 10 s.

5.1.10 Configuration control (option handling)

Properties

Configuration control allows you to prepare your distributed I/O system for future extensions or options. Configuration control means that you can configure the planned maximum configuration of your distributed I/O system in advance and vary it later in a flexible manner by means of the user program.

Reference

You can find more information on configuration control

- In the system manual ET 200AL Distributed I/O System (https://support.industry.siemens.com/cs/ww/en/view/89254965)
- On the Internet under the following link: Application collection (https://support.industry.siemens.com/cs/ww/en/view/29430270).
- In the STEP 7 online help.

5.1.11 Interface local coupling of IO data

Module-internal shared output

In this example, IO data are transferred from one controller to other controllers over the PROFINET interface X1 by means of the module-internal shared output.

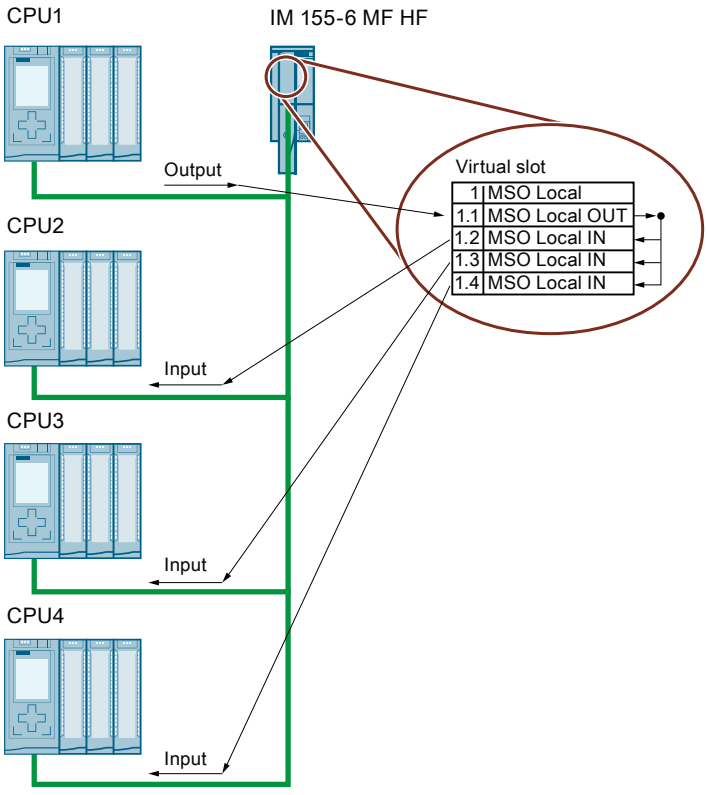


Figure 2-4 I/O data are transferred to other controllers in the same PROFINET network

Configuration

Table 2-10 Example of the configuration

Virtual slot	Type	I-length	Q-length	Access
1	MSO Local	-	-	-
1.1	MSO Local OUT	-	4 bytes	CPU 1
1.2	MSO Local IN	5 bytes incl. 1 byte DS	-	CPU 2
1.3	MSO Local IN	5 bytes incl. 1 byte DS	-	CPU 3
1.4	MSO Local IN	5 bytes incl. 1 byte DS	-	CPU 4

Editing in the user program

The controller CPU 1 writes I/O data to the MSO Local OUT module with the virtual slot 1.1 of the interface module. The data is available to CPUs 2 to 4 for reading with the remaining MSO Local IN modules. The validity of the provided user data is displayed by the data status byte (DS) of the MSO Local IN modules.

You can also use this example:

- with fewer controllers and
- configure it with other virtual modules.

NOTE

Virtual IO modules

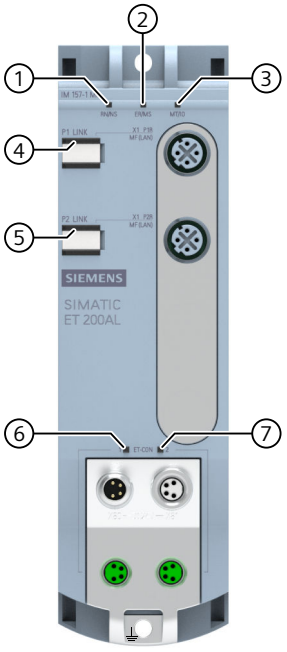
The use of virtual IO modules increases the communication load. This increases the data update time of all IO data accordingly.

5.2 Interrupts, error messages, diagnostics and system alarms

5.2.1 Status and error displays for PROFINET IO

LED indicators

The figure below shows the LED indicators (status and error displays) on the IM 157-1 MF interface module.



①	RN/NS	Green/red
②	ER/MS	Green/red
③	MT/IO	Green/red/yellow
④	P1 LINK	Green
⑤	P2 LINK	Green
⑥	ET-CON1	Green
⑦	ET-CON2	Green

Figure 2-5 LED indicators

Meaning of the RN/NS, ER/MS, MT/IO LED indicators

The following tables set out the meaning of the status and error displays for PROFINET IO. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 37).

The LEDs display the status with the **highest priority** if there are different LED states due to overlaid events. (0 = off, 1 = green flashing, 2 = green, 3 = yellow flashing, 4 = yellow, 5 = red flashing, 6 = red)

Table 2-11 Status and error displays of the LEDs RN/NS, ER/MS, MT/IO

LEDs			Meaning	Solution
RN/NS	ER/MS	MT/IO		
Off	Off	Off	Missing or insufficient supply voltage on interface module.	Check the supply voltage or switch it on at the interface module.
On	On	On	Booting active	---
Flashes	Flashes	Flashes	Error when booting	Replace the interface module.
Flashes	Flashes	Flashes	LED testing during startup. The three LEDs light up simultaneously: Red for the duration of the booting process + approximately 0.25 s thereafter, then green for approximately 0.25 s.	---
Flashes	Off	Off	Interface module is deactivated.	Activate the interface module with the configuration software or the user program.
			Interface module is not configured.	Configure the interface module with the configuration software.
			ET 200AL starts up.	---
			ET 200AL is being assigned parameters.	
On	Not relevant	Not relevant	ET 200AL is currently exchanging data with the IO controller.	---
Not relevant	Flashes	Not relevant	Group error	Evaluate the diagnostics and eliminate the error.
			The preset configuration does not correspond to the actual configuration of the ET 200AL.	Check the configuration of the ET 200AL to see whether a module is missing or defective or if a module that is not configured is connected to ET-CON1 or ET-CON2.
			Parameter assignment error in the I/O module	Evaluate the display of the module status in STEP 7 or in STEP 7 (TIA portal) and correct the errors in the I/O module.
Not relevant	Not relevant	On	Maintenance	See section Maintenance events (Page 38)
Flashes	Flashes	Flashes	The "Node flash test" is running.	The P1 LINK and P2 LINK LEDs of the MultiFieldbus interface also flash.
Flashes	Flashes	Flashes	Hardware or firmware defective (the P1 LINK and P2 LINK LEDs of the MultiFieldbus interface do not flash).	Replace the interface module. You can read out the service data.
On	On	On	RN/NS, ER/MS and MT/IO LEDs are permanently on: Hardware or firmware defective. Error information is determined and stored retentively in flash memory.	Do not disconnect the interface module from the supply voltage as long as the LEDs display a steady light. This may take a few minutes.

P1 LINK and P2 LINK LEDs

Table 2-12 Status displays of the P1 LINK and P2 LINK LEDs

LEDs		Meaning	Solution
P1 LINK	P2 LINK		
□ Off		There is no connection between the MultiFieldbus interface of your module and a communication partner (e.g. IO controller).	Check whether the bus cable to the switch or to the IO controller is disconnected.
■ On		There is a connection between the MultiFieldbus interface of your module and a communication partner (e.g. IO controller).	---
☼ Flashes		The "Node flash test" is run (the RN/NS, ER/MS and MT/IO LEDs also flash).	---

ET-CON1 and ET-CON2 LEDs

Table 2-13 Status displays of the ET-CON1 and ET-CON2 LEDs

LEDs		Meaning	Solution
ET-CON1	ET-CON2		
□ Off		There are no I/O modules at the respective ET-Connection or the modules do not have supply voltage.	Check the wiring for the ET-Connection or the supply voltage for the I/O module.
■ On		A communication connection to at least one I/O module of the respective ET-Connection is available.	-

5.2.2 Interrupts

5.2.2.1 Evaluating interrupts

Introduction

Interrupts are triggered by the IO device in case of errors. Interrupts are evaluated based on the I/O controller used.

Evaluating interrupts with I/O controllers

The ET 200AL distributed I/O system supports the following interrupts:

- Diagnostics interrupts
- Hardware interrupts
- Pull/plug module interrupt

In the event of an interrupt, interrupt OBs are automatically called in the CPU of the IO controller.

Information on the cause and class of the error is already available, based on the OB number and start information.

Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).

System diagnostics

In STEP 7 (TIA Portal), the updated system diagnostic is available for the modules of the S7-1500 automation system (IO controller CPU S7-1500) and ET 200AL (IO device). Independent of the cyclic user program, messages are made available on the display of the CPU S7-1500, the CPU web server and the HMI device.

You will find more information on systemic diagnostics in the Function Manual Diagnostics (http://support.automation.siemens.com/WW/view/en/59192926).

5.2.2.2 Trigger a diagnostics interrupt

For an incoming or outgoing event (for example, wire break on a channel of an I/O module), the interface module triggers a diagnostics interrupt if the parameters were assigned accordingly.

The CPU interrupts the processing of the user program and processes the diagnostics interrupt OB (OB 82). The event that triggered the interrupt is entered in the start information of the diagnostics interrupt OB.

5.2.2.3 Triggering a hardware interrupt

During a hardware interrupt, the CPU interrupts the processing of the user program and processes the hardware interrupt OB (e.g., OB 40). The event that triggered the interrupt is entered in the start information of the hardware interrupt OB.

NOTE

Diagnostics "Hardware interrupt lost" (from I/O module)
Avoid creating hardware interrupts cyclically.
If the hardware interrupt load is too high, hardware interrupts can get lost depending on the number of I/O modules and the communication load.

5.2.2.4 Triggering an insert/remove module interrupt

When an insert/remove module interrupt occurs, the CPU interrupts execution of the user program and processes the insert/remove module interrupt OB (OB 83). The event that triggered the interrupt is entered in the start information of the insert/remove OB.

The pull/plug OB (OB 83) is also triggered for all subsequent I/O modules, because the ET-Connection and/or the power supply is interrupted.

5.2.3 Alarms

5.2.3.1 Diagnostics alarms

Actions after a diagnostics alarm

There can be more than one diagnostic alarm at a given time. Actions initiated by diagnostics alarms:

- The ERROR LED of the interface module flashes.
- Diagnostic data is reported as diagnostics interrupts to the CPU of the IO controller and can be read via data records.
- Incoming diagnostics alarms are saved to the diagnostics buffer of the I/O controller.
- OB 82 is called. If OB 82 is not available, the I/O controller goes into STOP mode.

You can find more information on this topic in the STEP 7 online help.

Reading out the diagnostics data

Table 2-14 Reading the diagnostics with STEP 7

Automation system with IO controller	Application	See...
SIMATIC S7	Diagnostics as plain text in STEP 7 in online and diagnostics view	STEP 7 online help • STEP 7 V13 and higher Function Manual PROFINET with STEP 7 V13 (http://support.automation.siemens.com/WW/view/en/49948856) • STEP 7 V5.5 and higher System Manual PROFINET System Description (http://support.automation.siemens.com/WW/view/en/19292127)
	"RDREC" instruction (SFB 52) Reading data records from the IO device	
	"RALRM" instruction (SFB 54) Receiving alarms from the IO device	
	Diagnostics as plain text in MFCT in online and diagnostics view	SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209)

Additional information on the data records for PROFINET IO

The structure of the diagnostics data records and programming examples can be found in the Programming Manual From PROFIBUS DP to PROFINET IO (http://support.automation.siemens.com/WW/view/en/19289930) and in the Application example (http://support.automation.siemens.com/WW/view/en/24000238).

Causes of error and troubleshooting

Causes of errors and corrective measures of diagnostics alarms are described in the device manuals of the I/O modules (http://support.automation.siemens.com/WW/view/en/89013554) in the section Interrupt, Error and System Messages.

5.2.3.2 Maintenance events

Triggering of a maintenance event

The PROFINET IO interfaces of the interface module support the diagnostics concept and maintenance concept in PROFINET IO according to standard IEC 61158-6-10. The goal is the early recognition and correction of potential disruptions.

For the interface module, maintenance events signal to the user when a network component must be checked or replaced.

The CPU interrupts user program execution and processes the diagnostic block OB 82. The event that triggered the maintenance event is entered in the start information of the OB 82.

The interface module signals a maintenance event to the higher-level diagnostics system in the case of the following event:

Table 2-15 Triggering of a maintenance event

Maintenance alarm	Event	Alarm/Meaning
Maintenance demanded LED MAINT is lit.	Synchronization loss	• No synchronization frame received. No synchronization message frame was received by the sync master within the timeout period after parameter assignment or during operation. • Successive synchronization frames are located outside permitted limits (jitter).

System alarms in STEP 7 (TIA Portal)

The maintenance information is generated in STEP 7 (TIA Portal) V12 SP1 and higher with the following system alarms:

- Maintenance demanded - indicated for each port by a yellow wrench icon in the device view or in the hardware configuration.

You can find more information on this topic in the STEP 7 online help.

5.2.3.3 Channel diagnostics

Function

Channel-related diagnostics provides information about channel faults in modules.
Channel faults are mapped as channel diagnostics data in IO diagnostics data records.
The data record is read with the "RDREC" instruction (SFB 52).

Structure of the diagnostics data records

The data records supported by the ET 200AL distributed I/O system are based on the PROFINET IO standard - Application Layer Service definition V2.2.
You can download the standard on the Internet (http://www.profibus.com) from home page of the PROFIBUS user organization free of charge.

Structure of the manufacturer-specific diagnostics data records

The structure of the diagnostics data records is differentiated by the BlockVersion. The following BlockVersion applies to the IM 157-1 MF interface modules:

Table 2-16 Structure of the manufacturer-specific diagnostics data records

IM 157-1 MF interface module	BlockVersion
6ES7157-1MA00-0AB0	W#16#0101

5.2.3.4 Invalid configuration states of ET 200AL on the PROFINET IO

Invalid configuration states

If the number of modules exceeds the maximum configuration limit, the extra modules are ignored by the system. No data exchange takes place.

5.2.3.5 STOP of the IO controller and recovery of the IO device

STOP of the SIMATIC IO controller

If diagnostics from the IO device are received by the IO controller in the STOP state, these diagnostics do not result in a start of the organization blocks after startup of the IO controller. You must read the data record $E00C_H$ in OB 100 with the "RDREC" instruction.

Return of the SIMATIC IO device

If you want to read out the diagnostics of a station after the station return, you must read the data record $E00C_H$ in OB 86 with the "RDREC" instruction.

EtherNet/IP

6

6.1 Supported EtherNet/IP functions

Supported functions

The table below shows the functions that the module supports with EtherNet/IP.

Supported functions	Remarks
I/O communication with scanner	As of FW 1.0.x
Parameter assignment	As of FW 1.0.x
Reading diagnostics	As of FW 1.0.x
Normative CIP objects	As of FW 1.0.x
Reset to factory settings	As of FW 1.0.x
Diagnostics bit in data status of cyclic I/O data per submodule	As of FW 1.0.x
Shared device functions	As of FW 1.0.x
EtherNet/IP basic service	As of FW 1.0.x
Reading events (hardware interrupts)	As of FW 1.0.x
Data record interface	As of FW 1.0.x

Supported troubleshooting functions

The table below shows the functions for troubleshooting that the module supports with EtherNet/IP.

Supported troubleshooting functions	Remarks
Reading diagnostics via CIP EtherNet/IP	As of FW 1.0.x
Reading diagnostics with MFCT	As of FW 1.0.x
Reading hardware interrupt via CIP EtherNet/IP	As of FW 1.0.x
PULL/PLUG event EtherNet/IP	As of FW 1.0.x
Reading service data with MFCT	As of FW 1.0.x

Supported CIP objects for EtherNet/IP

The table below shows the CIP objects that the I/O device supports with EtherNet/IP.

Supported CIP objects	Remarks
Identity object	As of FW 1.0.x
Assembly object	As of FW 1.0.x
Connection Manager object	As of FW 1.0.x
TCP/IP Interface object	As of FW 1.0.x

Supported CIP objects	Remarks
EtherNet Link object	As of FW 1.0.x
LLDP Management object	As of FW 1.0.x
LLDP Data Table object	Not supported
Param object	As of FW 1.0.x

6.2 Applicable modules with EtherNet/IP

With EtherNet/IP the following modules cannot be used or can be used only with limitations. These modules are divided into 4 categories:

Category	Description
1	Module can be used without functional restrictions. The module needs simple parameter reassignment. Records/interface are described in the Equipment Manual.
2	A function block must be created for the module for the target control. The module operates with a non-locked function block. The function block can be reimplemented.
3	Subfunctions of the module are not supported by the selected fieldbus. Subfunctions are only possible using blocks or additional interfaces.
4	The module is not supported by the selected fieldbus. The module needs a protected function block (e.g. for F-modules).

NOTE
Module operating modes based on isochronous operation (e.g. oversampling or time stamping) are not supported.

F-module

Module	Article number	Category	Note
F-DI 4+F-DQ 2x24VDC/2A, 4xM12	6ES7146-5FF00-0BA0	4	-

6.3 Update time of the I/O data

You can estimate the typical update time for an I/O cycle as follows:

RPI time (can be set starting at 2 ms)

+ Processing time I/O data (typically 1.4 ms, +/- 1 ms jitter due to free-running cycles)

+ Conversion time in module (dependent on cycle time and parameter assignment of the module)

If necessary, you must take into account other influences caused by the EIP scanner and network components by adding them.

NOTE

With ET 200AL I/O modules, a search for devices at the ET connection lasting up to 5 seconds takes place. The user data is temporarily invalid during this period (IDS/ODS = 0x40).

6.4 I/O data mapping

In this chapter, you will find an example configuration of the I/O data mapping for EtherNet/IP with the I/O data alignment byte. To derive the I/O data mapping with the MFCT tool, proceed as follows:

1. Open the MFCT
2. Create or open a project
3. Select the station
4. Configure the station with the modules
5. Assign parameters to the modules
6. Export the general settings as a CSV file
7. Open the CSV file with a spreadsheet program

Configuration example

The following figure shows the configuration for this example:

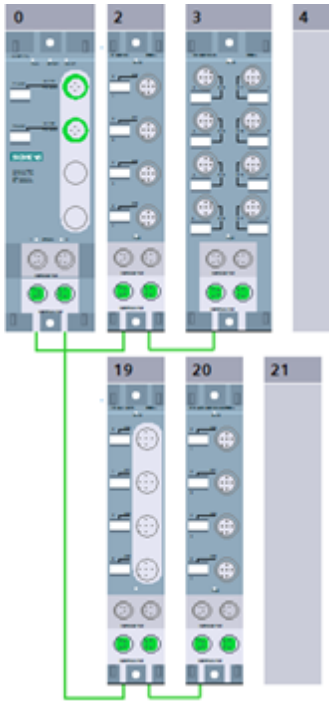


Figure 2-6 Configuration example

The example uses the following modules:

Slot	Module
0	IM 157-1 MF
2	DI 8x24VDC 4xM12
3	DQ 8x24VDC/2A 8xM12
19	AQ 4xU/I 4xM12
20	DIQ 4+DQ 4x24VDC/0.5A 4xM12

Input buffer for EtherNet/IP

The following table shows the input buffer for the example configuration for the I/O data alignment Byte:

Slot	Byte address	Dataltem	Lo/Hi	Module
0	0	IDS	MSB	IM 157-1 MF V1.0
1	1	IDS	LSB	ET-Con1
2	2	Inputs	MSB	D 8x24VDC 4xM12
	3	IDS	LSB	DI 8x24VDC 4xM12
18	4	IDS	MSB	ET-Con2
20	5	Inputs	LSB	DIQ 4+DQ 4x24VDC/0.5A 4xM12
	6	IDS	MSB	DIQ 4+DQ 4x24VDC/0.5A 4xM12

Slot	Byte address	DataItem	Lo/Hi	Module
3	7	ODS	LSB	DQ 8x24VDC/2A 8xM12
19	8	ODS	MSB	AQ 4xU/I 4xM12
20	9	ODS	LSB	DIQ 4+DQ 4x24VDC/0.5A 4xM12

The sum of the input data is 10 bytes.

Output buffer for EtherNet/IP

The following table shows the output buffer for the example configuration for the I/O data alignment Byte:

Slot	Byte address	DataItem	Lo/Hi	Module
3	0	Outputs	MSB	DQ 8x24VDC/2A 8xM12
19	1	O_channel_0_0	LSB	AQ 4xU/I 4xM12
	2	O_channel_0_1	MSB	AQ 4xU/I 4xM12
	3	O_channel_1_0	LSB	AQ 4xU/I 4xM12
	4	O_channel_1_1	MSB	AQ 4xU/I 4xM12
	5	O_channel_2_0	LSB	AQ 4xU/I 4xM12
	6	O_channel_2_1	MSB	AQ 4xU/I 4xM12
	7	O_channel_3_0	LSB	AQ 4xU/I 4xM12
	8	O_channel_3_1	MSB	AQ 4xU/I 4xM12
20	9	Outputs	LSB	DIQ 4+DQ 4x24VDC/0.5A 4xM12

The sum of the output data is 10 bytes.

6.5 MF Shared Device

Four ARs are available; these are shared by the fieldbuses. For EtherNet/IP and Modbus TCP, only one AR is reserved in each case, regardless of the number of controller connections used.

The maximum amount of I/O data must comply with the rules of the following table:

Number of fieldbus connections			Maximum I/O data per connection[1]		Max. download size with MFCT [1]	
PROFINET	EtherNet/IP	Modbus TCP	Inputs	Outputs	Inputs	Outputs
1	1 ... 2	0	EtherNet/IP **or** Modbus TCP: 500 PROFINET: 1440	EtherNet/IP **or** Modbus TCP: 246 PROFINET: 1440	Download size[2]: 1440	Download size[2]: 1440
1	0	1 ... 10				
0	1 ... 2	1 ... 10	500	246	1440	1440
0	0	1 ... 10	500	246	1440	1440
0	1 ... 2	0				
1	1 ... 2	1 ... 10	360	EtherNet/IP **or** Modbus TCP: 246 PROFINET: 360	360	360
2	1 ... 2	0				
2	0	1 ... 10				
2	1 ... 2	1 ... 10				

1 Including PROFINET payload qualifier or data status byte for signaling the data validity

2 PROFINET data + download size as displayed in MFCT ≤ 1440

Number of fieldbus connections			Maximum I/O data per connection[1]		Max. download size with MFCT [1]	
PROFINET	**EtherNet /IP**	**Modbus TCP**	**Inputs**	**Outputs**	**Inputs**	**Outputs**
3	0	1 ... 10	360	EtherNet/IP **or** Modbus TCP: 246 PROFINET: 360	360	360
3	1 ... 2	0				
4	0	0	360	360	1400	1400

1 Including PROFINET payload qualifier or data status byte for signaling the data validity

2 PROFINET data + download size as displayed in MFCT ≤ 1440

The download size contains the I/O data of all EtherNet/IP and Modbus TCP connections as well as additional bytes for controlling the download.

NOTE

To avoid temporarily exceeding the I/O quantity structure, you must proceed as follows in case of a reconfiguration that results in changed I/O lengths:

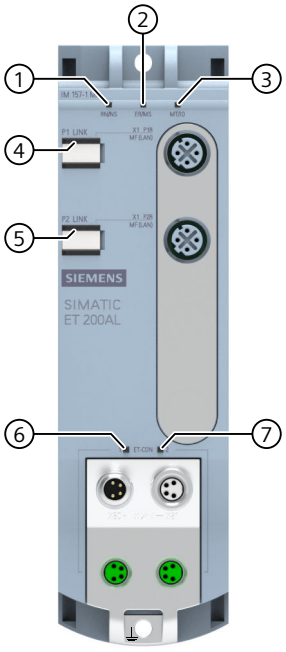
1. Reduce the amount of I/O data in one configuration and download it to the MF device/CPU.
2. Increase the amount of I/O data in another configuration and download it to the MF device/CPU.

6.6 Diagnostics

6.6.1 Status and error displays for EtherNet/IP

LED indicators

The figure below shows the LED indicators (status and error displays) on the IM 157-1 MF interface module.



①	RN/NS	Green/red
②	ER/MS	Green/red
③	MT/IO	Green/red/yellow
④	P1 LINK	Green
⑤	P2 LINK	Green
⑥	ET-CON1	Green
⑦	ET-CON2	Green

Figure 2-7 LED indicators

Meaning of the RN/NS, ER/MS, MT/IO LED indicators

The following tables set out the meaning of the status and error displays for EtherNet/IP.

The LEDs display the status with the **highest priority** if there are different LED states due to overlaid events. (0 = off, 1 = green flashing, 2 = green, 3 = yellow flashing, 4 = yellow, 5 = red flashing, 6 = red)

Table 2-17 Status and error displays of the RN/NS, ER/MS, MT/IO LEDs

LEDs			Meaning	Notes
RN/NS	**ER/MS**	**MT/IO**		
□ Off	□ Off	□ Off	Missing or insufficient supply voltage on the MF device.	• Check the supply voltage or switch on the supply voltage on the MF device.
■ On	■ On	■ On	Booting active	---
☼ Flashes	☼ Flashes	☼ Flashes	Error when booting	• Replace the interface module.
Flashes	Flashes	Flashes	LED testing during startup. The three LEDs light up simultaneously: Red for the duration of the booting process + approximately 0.25 s thereafter, then green for approximately 0.25 s.	---
☼ Flashes	□ Off	□ Off	The MF device is not exchanging data. There is no MultiFieldbus project in the MF device.	• Create a project with MFCT and transfer it to the MF device. Then establish the cyclic I/O communication with the MF device.
■ On	□ Off	□ Off	The MF device is exchanging data via PROFINET IO. There is no MultiFieldbus project in the MF device.	• Exclusive PROFINET use
☼ Flashes	☼ Flashes	□ Off	The MF device is not exchanging data. There is a MultiFieldbus project in the MF device.	• Establish the cyclic communication via EtherNet/IP.
■ On	■ On	□ Off	The MF device is exchanging data error-free via a connection (EtherNet/IP).	• If a data exchange was configured for EtherNet/IP, the assigned EtherNet/IP scanner is in STOP mode.
■ On	■ On	■ On	The MF device is exchanging data error-free via a connection (EtherNet/IP). I/O used by EtherNet/IP is in RUN mode.	---
Not relevant	Not relevant	■ On	Diagnostics maintenance requested	---
■ On	☼ Flashes	■ On **or** □ Off	The MF device is exchanging data via at least one connection. Errors in the configuration or parameter assignment.	• At least one module is configured incorrectly, there is no missing module or I/O diagnostics information. • Check the station configuration and, if necessary, correct the configuration and parameter assignment of the MF device in the MFCT and download them to the MF device again. • Check the device status in the Device-Info area and, if necessary, eliminate the diagnostics error.

LEDs			Meaning	Notes
RN/NS	**ER/MS**	**MT/IO**		
Flashes	Flashes	Off	The MF device is not exchanging data. The MF device has an error.	• Establish the cyclic communication via the I/O register area of the MF device or via EtherNet/IP. • Check the station configuration and eliminate configuration and parameter assignment errors via MFCT and eliminate diagnostics errors.
Flashes	Flashes	Not relevant	At least one connection existed (EtherNet/IP). A connection has been terminated by timeout.	• Reduce the cycle time. • Check the accessibility of the MF device via the network from the perspective of the EtherNet/IP scanner.
Flashes	Flashes	Not relevant	At least one connection existed (EtherNet/IP or Modbus TCP). A connection has been terminated by timeout. Error in the configuration or parameter assignment, or diagnostics present.	• Check the accessibility of the MF device via the network from the perspective of the EtherNet/IP scanner. • Check the station configuration and eliminate configuration and parameter assignment errors via MFCT and eliminate diagnostics errors.
Flashes	Flashes	Flashes	The "Node flash test" is running.	• The P1 LINK and P2 LINK LEDs of the MultiFieldbus interface also flash.
Flashes	Flashes	Flashes	Hardware or firmware defective.	• Read out the service data. • Replace the ET 200AL module.
On	On	On	RN/NS, ER/MS and MT/IO LEDs are permanently on: Hardware or firmware defective. Error information is determined and stored retentively in flash memory.	Do not disconnect the interface module from the supply voltage as long as the LEDs display a steady light. This may take a few minutes.

P1 LINK and P2 LINK LEDs

Table 2-18 Status displays of the P1 LINK and P2 LINK LEDs

LEDs		Meaning	Solution
P1 LINK	**P2 LINK**		
Off		There is no connection between the MultiFieldbus interface of your module and a communication partner (for example, EIP scanner).	Check whether the bus cable to the switch or to the EIP scanner is disconnected.
On		There is a connection between the MultiFieldbus interface of your module and a communication partner (for example, EIP scanner).	---
Flashes		The "Node flash test" is run (the RN/NS, ER/MS and MT/IO LEDs also flash).	---

ET-CON1 and ET-CON2 LEDs

Table 2-19 Status displays of the ET-CON1 and ET-CON2 LEDs

LEDs		Meaning	Solution
ET-CON1	ET-CON2		
□ Off		There are no I/O modules at the respective ET-Connection or the modules do not have supply voltage.	Check the wiring for the ET-Connection or the supply voltage for the I/O module.
■ On		A communication connection to at least one I/O module of the respective ET-Connection is available.	-

Modbus TCP

7

7.1 Supported Modbus TCP functions

Supported functions

The table below shows the functions that the module supports with Modbus TCP.

Supported functions	RegLayoutVersion	Remarks
I/O communication with Modbus client	V1.0	As of FW 1.0.x
Free user registers (e.g. for coordination of the redundancy)	V1.0	As of FW 1.0.x
Device information	V1.0	As of FW 1.0.x
Module configuration status register	≥ V1.1	As of FW 1.0.x
Diagnostics bit in data status of cyclic I/O data per submodule	V1.0	As of FW 1.0.x
Shared device functions	V1.0	As of FW 1.0.x
Reading events (hardware interrupts)	V1.0	As of FW 1.0.x
Data record interface	≥ V1.1	As of FW 1.0.x

Supported troubleshooting functions

The table below shows the troubleshooting functions that the module supports for Modbus TCP.

Supported troubleshooting functions	Remarks
Reading diagnostics with MFCT	As of FW 1.0.x
Reading hardware interrupts via event interface	As of FW 1.0.x
PULL/PLUG event Modbus TCP	As of FW 1.0.x
Reading service data with MFCT	As of FW 1.0.x

7.2 Modules that can be used with Modbus TCP

With Modbus TCP, the following modules cannot be used or can be used only with limitations.

These modules are divided into 4 categories:

Category	Description
1	This category is not relevant for Modbus TCP.
2	A function block must be created for the module for the target control. The module operates with a non-locked function block. The function block can be reimplemented.
3	Subfunctions of the module are not supported by the selected fieldbus. Subfunctions are only possible using blocks or additional interfaces.
4	The module is not supported by the selected fieldbus. The module needs a protected function block (e.g. for F-modules).

NOTE

Module operating modes based on isochronous operation (e.g. oversampling or time stamping) are not supported.

F-module

Module	Article number	Category	Note
F-DI 4+F-DQ 2x24VDC/2A, 4xM12	6ES7146-5FF00-0BA0	4	-

7.3 Update time of the I/O data

You can estimate the typical update time for an I/O cycle as follows:

Update time (can be set starting at 2 ms)

+ Processing time I/O data (typically 1.4 ms, +/- 1 ms jitter due to free-running cycles)

+ Conversion time in module (dependent on cycle time and parameter assignment of the module)

If necessary, you must take into account other influences caused by the Modbus client and network components by adding them.

NOTE

With ET 200AL I/O modules, a search for devices at the ET connection lasting up to 5 seconds takes place. The user data is temporarily invalid during this period (IDS/ODS = 0x40).

7.4 I/O data mapping

In this chapter, you will find an example configuration of the I/O data mapping for Modbus TCP with the I/O data alignment byte. To derive the I/O data mapping with the MFCT tool, proceed as follows:

1. Open the MFCT
2. Create or open a project
3. Select the station
4. Configure the station with the modules
5. Assign parameters to the modules
6. Export the general settings as a CSV file
7. Open the CSV file with a spreadsheet program

Configuration example

The following figure shows the configuration for this example:

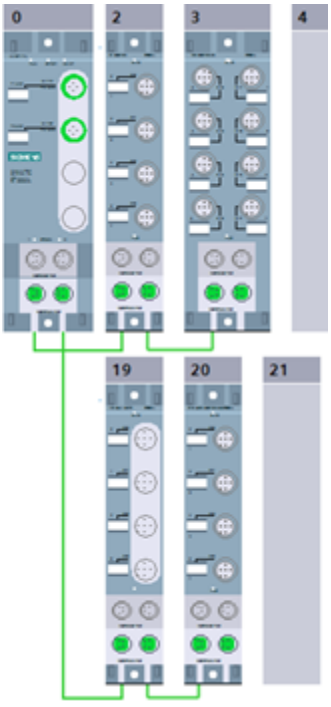


Figure 2-8 Configuration example

The example uses the following modules:

Slot	Module
0	IM 157-1 MF
2	DI 8x24VDC 4xM12
3	DQ 8x24VDC/2A 8xM12
19	AQ 4xU/I 4xM12
20	DIQ 4+DQ 4x24VDC/0.5A 4xM12

Input buffer for Modbus TCP

The following table shows the input buffer for the example configuration for the I/O data alignment Byte:

Slot	Byte address	Register address	DataItem	Lo/Hi byte	Bit address	Module
0	0	0	IDS	MSB	0x0000	IM 157-1 MF V1.0
1	1		IDS	LSB	0x0008	ET-Con1
2	2	1	Inputs	MSB	0x0010	DI 8x24VDC 4xM12
	3		IDS	LSB	0x0018	DI 8x24VDC 4xM12
18	4	2	IDS	MSB	0x0020	ET-Con2
20	5		Inputs	LSB	0x0028	DIQ 4+DQ 4x24VDC/0.5A 4xM12
	6	3	IDS	MSB	0x0030	DIQ 4+DQ 4x24VDC/0.5A 4xM12
3	7		ODS	LSB	0x0038	DQ 8x24VDC/2A 8xM12
19	8	4	ODS	MSB	0x0040	AQ 4xU/I 4xM12
20	9		ODS	LSB	0x0048	DIQ 4+DQ 4x24VDC/0.5A 4xM12

The sum of the input data is 10 bytes.

Output buffer for Modbus TCP

The following table shows the output buffer for the example configuration for the I/O data alignment Byte:

Slot	Byte address	Register address	DataItem	Lo/Hi byte	Bit address	Module
3	0	720	Outputs	MSB	0x0000	DQ 8x24VDC/2A 8xM12
19	1		O_channel_0_0	LSB	0x0008	AQ 4xU/I 4xM12
	2	721	O_channel_0_1	MSB	0x0010	AQ 4xU/I 4xM12
	3		O_channel_1_0	LSB	0x0018	AQ 4xU/I 4xM12
	4	722	O_channel_1_1	MSB	0x0020	AQ 4xU/I 4xM12
	5		O_channel_2_0	LSB	0x0028	AQ 4xU/I 4xM12
	6	723	O_channel_2_1	MSB	0x0030	AQ 4xU/I 4xM12
	7		O_channel_3_0	LSB	0x0038	AQ 4xU/I 4xM12
	8	724	O_channel_3_1	MSB	0x0040	AQ 4xU/I 4xM12
20	9		Outputs	LSB	0x0048	DIQ 4+DQ 4x24VDC/0.5A 4xM12

The sum of the output data is 10 bytes.

7.5 MF Shared Device

Four ARs are available; these are shared by the fieldbuses. For EtherNet/IP and Modbus TCP, only one AR is reserved in each case, regardless of the number of controller connections used.

The maximum amount of I/O data must comply with the rules of the following table:

Number of fieldbus connections			**Maximum I/O data per connection**[1]		**Max. download size with MFCT** [1]	
PROFINET	**EtherNet /IP**	**Modbus TCP**	**Inputs**	**Outputs**	**Inputs**	**Outputs**
1	1 ... 2	0	EtherNet/IP **or** Modbus TCP: 500 PROFINET: 1440	EtherNet/IP **or** Modbus TCP: 246 PROFINET: 1440	Download size[2]: 1440	Download size[2]: 1440
1	0	1 ... 10				
0	1 ... 2	1 ... 10	500	246	1440	1440
0	0	1 ... 10	500	246	1440	1440
0	1 ... 2	0				
1	1 ... 2	1 ... 10	360	EtherNet/IP **or** Modbus TCP: 246 PROFINET: 360	360	360
2	1 ... 2	0				
2	0	1 ... 10				
2	1 ... 2	1 ... 10				
3	0	1 ... 10				
3	1 ... 2	0				
4	0	0	360	360	1400	1400

1 Including PROFINET payload qualifier or data status byte for signaling the data validity

2 PROFINET data + download size as displayed in MFCT ≤ 1440

The download size contains the I/O data of all EtherNet/IP and Modbus TCP connections as well as additional bytes for controlling the download.

NOTE

To avoid temporarily exceeding the I/O quantity structure, you must proceed as follows in case of a reconfiguration that results in changed I/O lengths:

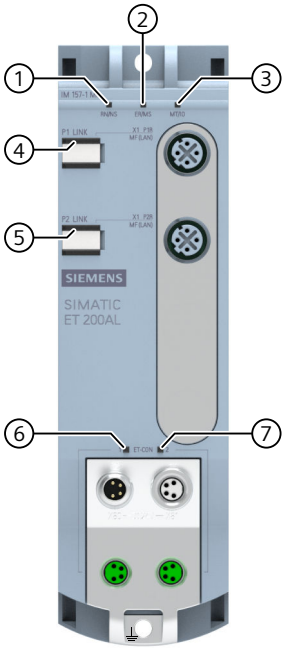
1. Reduce the amount of I/O data in one configuration and download it to the MF device/CPU.
2. Increase the amount of I/O data in another configuration and download it to the MF device/CPU.

7.6 Diagnostics

7.6.1 Status and error displays for Modbus TCP

LED indicators

The figure below shows the LED indicators (status and error displays) on the IM 157-1 MF interface module.



①	RN/NS	Green/red
②	ER/MS	Green/red
③	MT/IO	Green/red/yellow
④	P1 LINK	Green
⑤	P2 LINK	Green
⑥	ET-CON1	Green
⑦	ET-CON2	Green

Figure 2-9 LED indicators

Meaning of the RN/NS, ER/MS, MT/IO LED indicators

The following tables set out the meaning of the status and error displays for Modbus TCP:

The LEDs display the status with the **highest priority** if there are different LED states due to overlaid events. (0 = off, 1 = green flashing, 2 = green, 3 = yellow flashing, 4 = yellow, 5 = red flashing, 6 = red)

Table 2-20 Status and error displays of the RN/NS, ER/MS, MT/IO LEDs

LEDs			Meaning	Notes
RN/NS	ER/MS	MT/IO		
Off	Off	Off	Missing or insufficient supply voltage on the MF device.	• Check the supply voltage or switch on the supply voltage on the MF device. *
On	On	On	Booting active	---
Flashes	Flashes	Flashes	Error when booting	• Replace the interface module.
Flashes	Flashes	Flashes	LED testing during startup. The three LEDs light up simultaneously: Red for the duration of the booting process + approximately 0.25 s thereafter, then green for approximately 0.25 s.	---
Flashes	Off	Off	The MF device is not exchanging data. There is no MultiFieldbus project in the MF device.	• Create a project with MFCT and transfer it to the MF device. Then establish the cyclic I/O communication with the MF device.
On	Off	Off	The MF device is exchanging data via PROFINET IO. There is no MultiFieldbus project in the MF device.	• Exclusive PROFINET use
Flashes	Flashes	Off	The MF device is not exchanging data. There is a MultiFieldbus project in the MF device.	• Establish the cyclic communication via Modbus TCP I/O register area for configured modules.
On	Flashes	Off	The MF device is exchanging data via PROFINET IO. There is a MultiFieldbus project in the MF device.	• Establish the cyclic I/O communication with a Modbus TCP controller. The corresponding fieldbus must have been selected via MFCT and downloaded to the MF device in advance. • Select "PROFINET" as the fieldbus in the MFCT for exclusive operation with PROFINET controllers.
On	On	Off	The MF device is exchanging data error-free via a connection (Modbus TCP).	---
Not relevant	Not relevant	On	Diagnostics maintenance requested	---
On	Flashes	Off	The MF device is exchanging data. The MF device has an error.	• Check the station configuration and, if necessary, correct the configuration and parameter assignment of the MF device in the MFCT and download them to the MF device again. • Check the device status in the Device-Info area and, if necessary, eliminate the diagnostics error.

LEDs			Meaning	Notes
RN/NS	ER/MS	MT/IO		
Flashes	Flashes	Off	The MF device is not exchanging data. The MF device has an error.	• Establish the cyclic communication via the I/O register area of the MF device. • Check the station configuration and eliminate configuration and parameter assignment errors via MFCT and eliminate diagnostics errors.
Flashes	Flashes	Off	At least one connection existed (Modbus TCP). A connection has been terminated by timeout.	• Reduce the cycle time for writing the output registers in the Modbus TCP controller to less than the time for the Modbus hold time configured via the MFCT. • Check the accessibility of the MF device via the network from the perspective of the Modbus TCP controller.
Flashes	Flashes	Off	At least one connection existed (Modbus TCP). A connection has been terminated by timeout. Errors in the configuration or parameter assignment.	• Reduce the cycle time for writing the output registers in the Modbus TCP controller to less than the time for the Modbus hold time configured via the MFCT. • Check the accessibility of the MF device via the network from the perspective of the Modbus TCP controller. • Check the station configuration and eliminate configuration and parameter assignment errors via MFCT and eliminate diagnostics errors.
Flashes	Flashes	Flashes	The "Node flash test" is running.	• The P1 LINK and P2 LINK LEDs of the MultiFieldbus interface also flash.
Flashes	Flashes	Flashes	Hardware or firmware defective.	• Read out the service data. • Replace the ET 200AL module.
On	On	On	RN/NS, ER/MS, MT/IO LEDs are permanently on: Hardware or firmware defective. Error information is determined and stored retentively in flash memory.	Do not disconnect the interface module from the supply voltage as long as the LEDs display a steady light. This may take a few minutes.

P1 LINK and P2 LINK LEDs

Table 2-21 Status displays of the P1 LINK and P2 LINK LEDs

LEDs		Meaning	Solution
P1 LINK	P2 LINK		
☐ Off		There is no connection between the MultiFieldbus interface of your module and a communication partner (for example, server).	Check whether the bus cable to the switch or to the server is disconnected.
■ On		There is a connection between the MultiFieldbus interface of your module and a communication partner (for example, server).	---
☼ Flashes		The "Node flash test" is run (the RN/NS, ER/MS and MT/IO LEDs also flash).	---

ET-CON1 and ET-CON2 LEDs

Table 2-22 Status displays of the ET-CON1 and ET-CON2 LEDs

LEDs		Meaning	Solution
ET-CON1	ET-CON2		
☐ Off		There are no I/O modules at the respective ET-Connection or the modules do not have supply voltage.	Check the wiring for the ET-Connection or the supply voltage for the I/O module.
■ On		A communication connection to at least one I/O module of the respective ET-Connection is available.	-

Parameters

8

8.1 Parameters

The following table shows the parameters for the IM 157-1 MF interface module.

Table 2-23 Parameters (GSD file)

Parameters	Value range	Default	Efficiency range
Configuration control	• Deactivated • Activated	Deactivated	ET 200AL
MultiFieldbus parameter[1] I/O data alignment	• Byte • Word	Byte	ET 200AL
MultiFieldbus Modbus TCP[1] Hold time connection #0 ... #9	1 ... 30000 ms	5000 ms	ET 200AL
MultiFieldbus Modbus TCP[1] Reset hold connection #0 ... #9	0 ... 30000 ms	0 ms	ET 200AL
MultiFieldbus connection[1] Fieldbus connection	• PROFINET • EtherNet/IP • Modbus TCP	PROFINET	ET 200AL

[1] = A change of the default is possible via MFCT

8.2 Explanation of the parameters

Configuration control

You can use this parameter to enable the configuration control function in the ET 200AL distributed I/O system.

NOTE

If you enable the configuration control, the ET 200AL distributed I/O system requires a control data record 196 from the user program. With control data record 196, the ET 200AL distributed I/O system can operate the I/O modules.

Further information is available in the chapter Configuration control (option handling) (Page 30) and in the STEP 7 online Help.

MultiFieldbus parameter

I/O data alignment

Use this parameter to select the input/output data alignment between "Byte" and "Word". The "I/O Data Mapping" section of the respective fieldbus contains the following in this regard:

- A short instruction for CSV export of the I/O data alignment
- An example of the I/O data alignment byte of a configuration example

Further information is available in the SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209) Function Manual.

MultiFieldbus Modbus TCP

Hold time of the connection #0 ... #9

Use this parameter to set the hold time of each parameterized Modbus TCP. This parameter is not relevant for the PROFINET IO and EtherNet/IP fieldbuses. If no data is exchanged during the parameterized time, the connection is interrupted.

You can change the parameter with the MFCT program.

Reset hold connection #0 ... #9

Use this parameter to set the reset time of each Modbus TCP connection that has been set to "Timeout". This parameter is not relevant for the PROFINET IO and EtherNet/IP fieldbuses.

You can change the parameter with the MFCT program.

Additional information is available in the SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209) Function Manual.

MultiFieldbus connection

Use this parameter to select the fieldbus connection.

Further information is available in the SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209) Function Manual.

Operation and maintenance

9

9.1 Firmware update

During operation, it can become necessary to update the firmware (e.g. for function extensions). Firmware Update is used to update the firmware of the interface module.

NOTE

Temporary bus interruption
When you perform a firmware update of an ET 200AL I/O module, the ET-Connection is temporarily interrupted due to the restart of the I/O module. All downstream ET 200AL I/O modules report a pull/plug interrupt.

NOTE

I/O device remains in configured fieldbus mode
After a firmware update, the I/O device remains in the bus protocol in which the update was installed.
For example, in the case of an update via EtherNet/IP, the I/O device remains in EtherNet/IP mode.

For more information on the firmware update using STEP 7, refer to the "Maintenance" section in the System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965).

For more information on the firmware update using MFCT, refer to the "Firmware update with MFCT" section in the Function Manual SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209).

9.2 Resetting an interface module to factory settings

When you reset to factory settings, the interface module is reset to the delivery state settings. This means that all information that was saved internally on the interface module is deleted.

For more information on "Resetting to factory settings" using STEP 7, refer to the "Maintenance" section in the System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965).

For more information on "Resetting to factory settings" using MFCT, refer to the "Resetting MF device" section in the Function Manual SIMATIC MultiFieldbus (https://support.industry.siemens.com/cs/ww/en/view/109773209).

Technical specifications

10

Technical specifications of the interface module IM 157-1 MF

The following table lists the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7157-1MA00-0AB0/td?dl=en).

Article number	6ES7157-1MA00-0AB0
General information	
Product type designation	IM 157-1 MF
HW functional status	FS01
Firmware version	V1.0.x
• FW update possible	Yes
Vendor identification (VendorID)	002AH
Device identifier (DeviceID)	0314H
Manufacturer ID according to ODVA (VendorID)	0x04E3
Device ID according to ODVA (Product code)	0x0FB6
Product function	
• I&M data	Yes; I&M0 to I&M4
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V19 or higher
• STEP 7 configurable/integrated from version	from V5.6
• PROFINET from GSD version/GSD revision	GSDML V2.4.x
• Multi Fieldbus Configuration Tool (MFCT)	from V1.5
Configuration control	
via dataset	Yes
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Input current	
Current consumption (rated value)	80 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Power loss	
Power loss, typ.	2.5 W

Article number	6ES7157-1MA00-0AB0
Address area	
Address space per module	
• Address space per module, max.	264 byte; For input and output data respectively
Address space per station	
• Address space per station, max.	1 440 byte
Hardware configuration	
Submodules	
• Number of submodules per station, max.	125
Interfaces	
Number of PROFINET interfaces	1; 2 ports (switch)
1. Interface	
Interface type	PROFINET
Interface types	
• M12 port	Yes; 2x M12 D-coded
• integrated switch	Yes
Protocols	
• PROFINET IO Device	Yes
• Open IE communication	Yes
Interface types	
M12 port	
• Transmission procedure	PROFINET with 100 Mbit/s full duplex (100BASE-TX)
• 100 Mbps	Yes; PROFINET with 100 Mbit/s full duplex (100BASE-TX)
• Autonegotiation	Yes
• Autocrossing	Yes
Protocols	
Supports protocol for PROFINET IO	Yes
PROFIsafe	No
PROFIBUS	No
EtherNet/IP	Yes
Modbus TCP	Yes
PROFINET IO Device	
Services	
– IRT	Yes; 250 µs, 500 µs, 1 ms, 2 ms, 4 ms, 8 ms, 16 ms, 32 ms, 64 ms, 128 ms
– PROFIenergy	Yes
– Shared device	Yes
– Number of IO Controllers with shared device, max.	14; 4x PN controller + 2x EtherNet/IP scanner + 10x Modbus TCP master
Redundancy mode	
• PROFINET system redundancy (S2)	Yes
– on S7-1500R/H	Yes
– on S7-400H	Yes
• PROFINET system redundancy (R1)	No
• H-Sync forwarding	Yes

Article number	6ES7157-1MA00-0AB0
Media redundancy	
– MRP	Yes
– MRPD	Yes
EtherNet/IP	
Services	
– CIP Implicit Messaging	Yes
– CIP Explicit Messaging	Yes
– CIP Safety	No
– Configuration control via Explicit Messaging	No
– Shared device	Yes; 4x PN controller + 2x EtherNet/IP scanner + 10x Modbus TCP master
– Number of scanners with shared device, max.	2
Updating times	
– Requested Packet Interval (RPI)	2 ms
Redundancy mode	
– DLR (Device Level Ring)	No
Address area	
– Address space per module, max.	264 byte
– ForwardOpen (Class1 & 32 bit Header)	500 byte
– LargeForwardOpen (Class3)	4 002 byte
Modbus TCP	
Services	
– read coils (code=1)	Yes
– read discrete inputs (code=2)	Yes
– Read Holding Registers (Code=3)	Yes
– Read Input Register (Code=4)	Yes
– write single coil (code=5)	Yes
– Write Single Register (Code=6)	Yes
– write multiple coils (code=15)	Yes
– Write Multiple Registers (Code=16)	Yes
– Read/Write Multiple Registers (Code=23)	Yes
– Parameter change by master	Yes
– Modbus TCP Security Protocol	No
Address space per station	
– Address space per station, max.	500 byte; (246 byte outputs / 500 byte inputs)
– Access-consistent address space	250 byte; (246 byte outputs / 250 byte inputs)
Updating time	
– I/O request interval	2 ms
Connections	
– number of connections per device	9; (1x inputs / 2x outputs / 4x volatile registers / 2x Device Info)
Open IE communication	
• TCP/IP	Yes

Article number	6ES7157-1MA00-0AB0
• SNMP	Yes
• LLDP	Yes
• ARP	Yes
Interrupts/diagnostics/status information	
Diagnostics function	Yes
Alarms	
• Diagnostic alarm	Yes
Diagnostics indication LED	
• RUN LED	Yes; green LED
• ERROR LED	Yes; red LED
• MAINT LED	Yes; Yellow LED
• NS LED	Yes; green/red LED
• MS LED	Yes; green/red LED
• IO LED	Yes; red/green/yellow LEDs
• Connection display LINK TX/RX	Yes; 2x green LED
Potential separation	
between the load voltages	Yes
between PROFINET and all other circuits	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; from FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198632
product functions / security / header	
PROFINET Security Class	1
signed firmware update	Yes
Secure Boot	Yes
safely removing data	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions

Article number	6ES7157-1MA00-0AB0
connection method	
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	215 g

Dimension drawing

11

The figure below shows the dimension drawing of the IM 157-1 MF interface module in the front and side views.

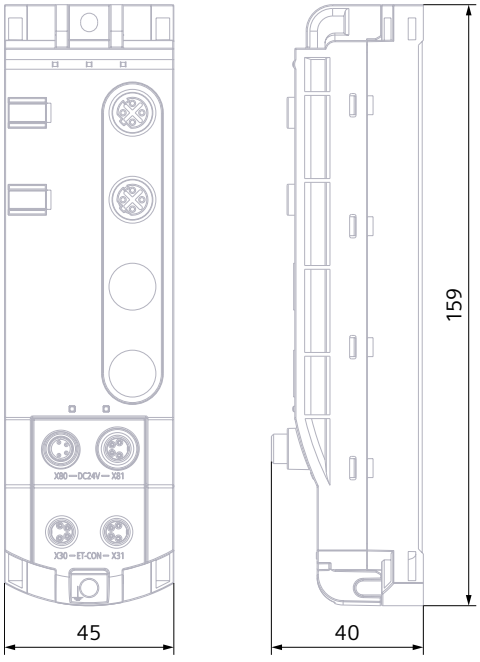
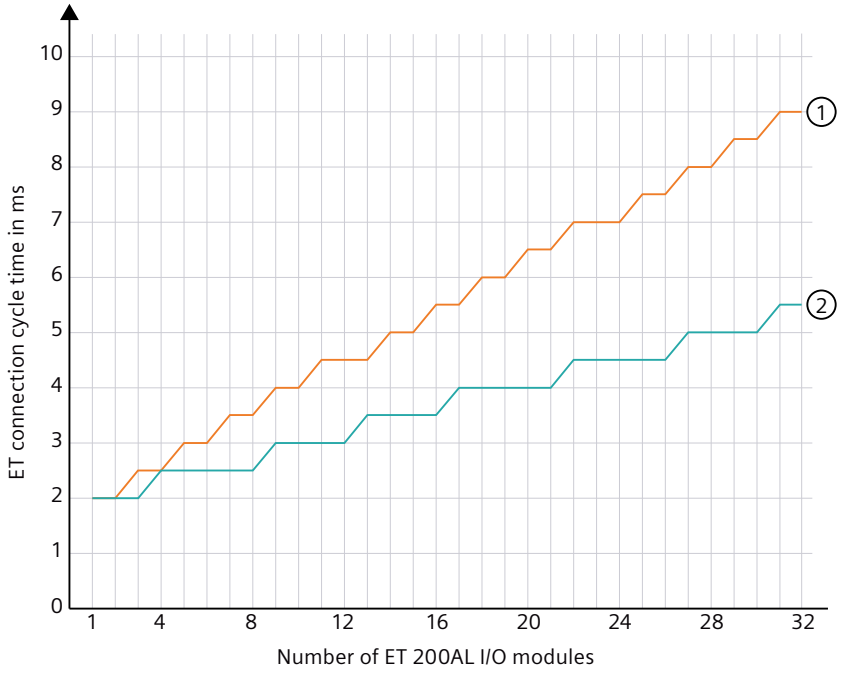


Figure 2-10 Dimension drawing

Cycle times

A

The chart below shows the cycle times at ET-Connection based on the number of I/O modules with a send clock of 0.5 ms.



① Cycle time for modules with firmware < V2.0.0

② Cycle time for modules with firmware ≥ V2.0.0

Figure 2-11 Cycle times

The cycle time at ET-Connection is synchronized with the send clock of the active fieldbus. The input data of the I/O modules is transmitted via the ET-Connection without any further delay (waiting time in the interface module). The output data is also transmitted via the fieldbus to the I/O modules without any further delay via the ET-Connection. The cycle time of the ET-Connection is always a multiple of the set send clock and depends on the number of I/O modules.

The chart above shows the trend for a send clock of 0.5 ms. With larger send clocks, the gradation of the trend changes according to the send clock.

If there are modules with a firmware version < V2.0.0 and modules with a firmware version ≥ V2.0.0 present in the ET-Connection, then the cycle time is between trends ① and ②.

When using a larger number of IO-Link masters with a large I/O data configuration (> 32 bytes), there may be a slight increase in the cycle time at the ET connection.

SIEMENS

SIMATIC

ET 200AL
IM 157-1 DP
(6ES7157-1AA00-0AB0)

Equipment Manual

ET 200AL Documentation Guide 1

Product overview 2

Wiring 3

Parameters 4

Interrupts, error messages, diagnostics and system alarms 5

Technical specifications 6

Dimension drawing A

Cycle times B

08/2021
A5E32100641-AE

Preface

Purpose of the documentation

This manual supplements the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965) system manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present manual, the system manual and the function manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 ET 200AL Documentation Guide 4

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

2.3 Functions 11
2.3.1 PROFIBUS DP 11
2.3.2 Configuration control (option handling) 12

3 Wiring 13

3.1 Terminal and block diagram 13

3.2 Pin assignment 14

3.3 Configuring PROFIBUS DP address and terminating resistor 15

4 Parameters 19

4.1 Parameters 19

4.2 Explanation of the parameters 19

5 Interrupts, error messages, diagnostics and system alarms 21

5.1 Status and error displays 21

5.2 Interrupts 23
5.2.1 Evaluating interrupts 23
5.2.2 Trigger a diagnostics interrupt 24
5.2.3 Triggering a hardware interrupt 24
5.2.4 Triggering an insert/remove module interrupt 24
5.2.5 Structure of data records 24

5.3 Alarms 33
5.3.1 Diagnostics alarms 33
5.3.2 Slave diagnostics 34
5.3.3 Station statuses 1 to 3 35
5.3.4 Master PROFIBUS address 36
5.3.5 Manufacturer ID 36
5.3.6 Identifier-related diagnostics 37
5.3.7 Module status 38
5.3.8 Channel diagnostics 39

6 Technical specifications 40

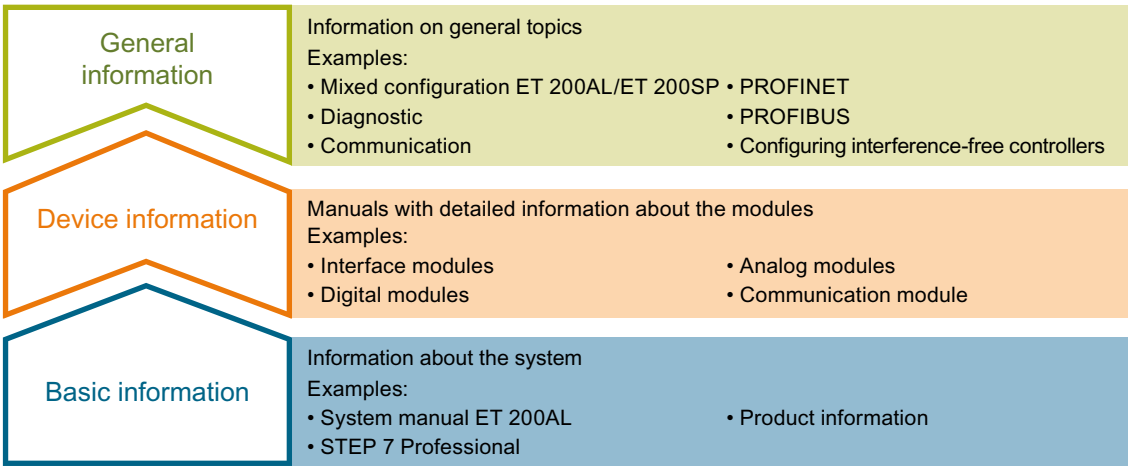
A Dimension drawing 43

B Cycle times 44

ET 200AL Documentation Guide

1

The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The System Manual and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system. The STEP 7 online help supports you in the configuration and programming.

Device information
Product manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC ET 200AL distributed I/O system, e.g. diagnostics, communication, Motion Control, Web server.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area of "mySupport", you can access the latest product data for your CAx or CAe system.

You configure your own download package with a few clicks.

In doing so you can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" - CAx data on the Internet (https://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/ae).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109767888).

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities simultaneously on various SIMATIC S7 stations as a bulk operation independent of TIA Portal.

The SIMATIC Automation Tool provides a multitude of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Address assignment (IP, subnet, gateway) and station name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization by means of LED flashing
- Reading out of CPU error information
- Reading of the CPU diagnostics buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/98161300).

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning. PRONETA features two core functions:

- The topology overview automatically scans the PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://www.siemens.com/sinetplan).

Product overview

2

2.1 Properties

Article number

6ES7157-1AA00-0AB0

View of the module

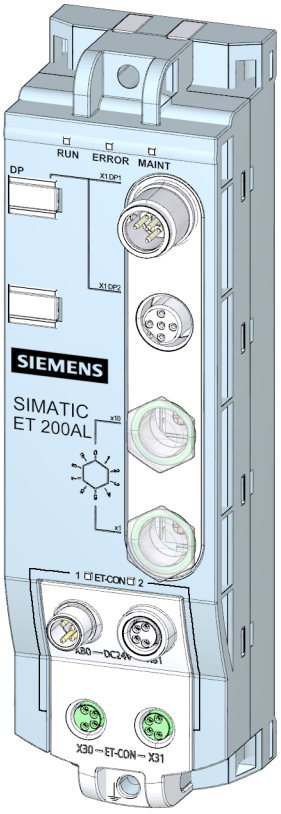


Figure 2-12 View of the IM 157-1 DP interface module

Properties

The module has the following technical properties:

- Connects the ET 200AL distributed I/O system with PROFIBUS DP
- 24 V DC supply voltage
- Operation as DP1 slave possible
- Direct data exchange (data exchange broadcast)
- Support for 2 ET-Connection lines
- Dimensions: 45 x 159 mm

The functions supported by the module are found in the chapter Functions (Page 11).

Maximum configuration

The module has the following maximum configuration:

- 244 bytes input data
- 244 bytes output data
- 32 I/O modules, up to 16 I/O modules can be connected for each ET-Connection line

Accessories

The following component is included with the module in the packaging:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

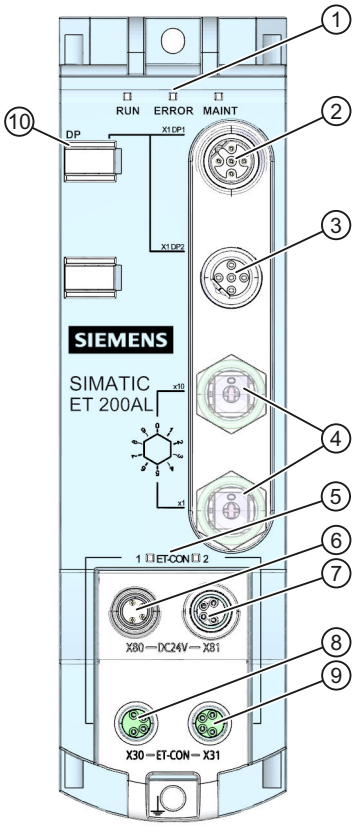
- Connectors
- Cables
- Stripping Tool for PROFIBUS
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You will find additional information on accessories and the other components in the Accessories/Spare parts section of the ET 200AL Distributed I/O System (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

2.2 Operator controls and display elements

The figure below shows the operator control and display elements of the interface module IM 157-1 DP.



① RUN, ERROR, MAINT: LED displays for the current operating status and diagnostics status
② X1 DP1: 1st PROFIBUS interface
③ X1 DP2: 2nd PROFIBUS interface
④ Rotary coding switch for setting the PROFIBUS address
⑤ ET-CON1, ET-CON2: LED displays for ET-Connection
⑥ X80: Connector for infeed of the supply voltage (POWER input)
⑦ X81: Socket for loop-through of the supply voltage (POWER output)
⑧ X30: Socket for ET-Connection1
⑨ X31: Socket for ET-Connection2
⑩ DP: LED displays for the current operating status of the PROFIBUS interfaces

Figure 2-13 Operator controls and display elements

2.3 Functions

2.3.1 PROFIBUS DP

Introduction

The interface module supports the following PROFIBUS DP functions:

- Operation as DPV0 and DPV1 slave
- Identification data I&M0 to I&M3
- Firmware update
- Configuration control by means of the user program

PROFIBUS DP

The PROFIBUS DP interface is used for connection to CPUs. With PROFIBUS DP you can set up extended subnets.

PROFIBUS is the network for the cell and field area in the open, manufacturer-independent communication system SIMATIC NET. Physically, PROFIBUS is an electrical network based on a shielded two-wire cable or an optical network based on a fiber optic cable.

Data transmission via PROFIBUS DP features a standardized interface (EN 50170 Vol. 2) for the transmission of process input and process output data between SIMATIC S7 and field devices (DP slaves).

The transmission behavior via PROFIBUS DP is characterized by cyclical data exchange between the DP master and the DP slaves.

Reference

You will find more information on PROFIBUS DP in the STEP 7 online help and in the Function Manual PROFIBUS with STEP 7 V13 (http://support.automation.siemens.com/WW/view/en/59193579).

2.3.2 Configuration control (option handling)

Properties

Configuration control allows you to prepare your distributed I/O system for future extensions or options. Configuration control means that you can configure the planned maximum configuration of your distributed I/O system in advance and vary it later in a flexible manner by means of the user program.

Reference

You can find more information on configuration control

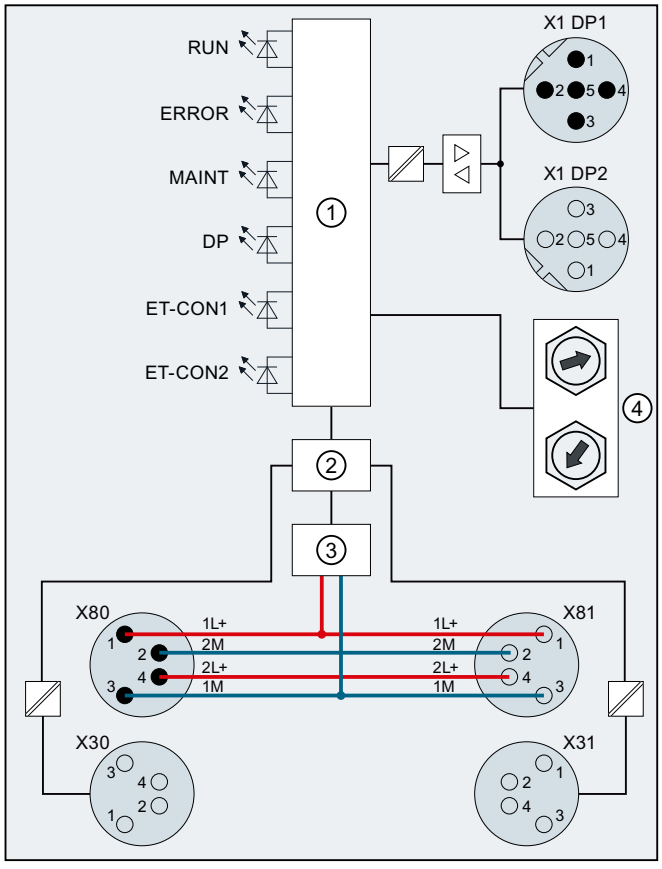
- In the system manual ET 200AL Distributed I/O System (https://support.industry.siemens.com/cs/ww/en/view/89254965)
- On the Internet under the following link: Application collection (https://support.industry.siemens.com/cs/ww/en/view/29430270).
- In the STEP 7 online help.

Wiring

3

3.1 Terminal and block diagram

The image below shows the terminal and block diagram of the IM 157-1 DP interface module.



①	Electronics	1L+	Supply voltage 1L+ (non-switched)
②	ET-Connection interface	1M	Ground 1M (non-switched)
③	Internal supply voltage	2L+	Load voltage 2L+ (switched)
④	Rotary coding switch for PROFIBUS addresses	2M	Ground 2M (switched)
X1 DP1	1. PROFIBUS interface	RUN	LED operating state (green)
X1 DP2	2. PROFIBUS interface	ERROR	LED diagnostics status (red)
X80	Infeed of supply voltages	MAINT	LED diagnostics status (yellow)
X81	Loop-through of supply voltages	DP	PROFIBUS LED (green)
X30	Infeed of the ET-Connection	ET-CON1, ET-CON2	ET-Connection LEDs (green)
X31	Loop-through of the ET-Connection		

Figure 2-14 Terminal and block diagram

3.2 Pin assignment

NOTE

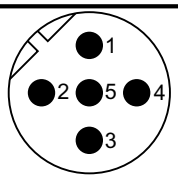
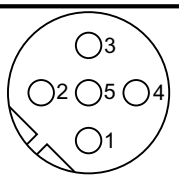
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for PROFIBUS

The following table shows the pin assignment of the connectors and sockets for the connection of PROFIBUS.

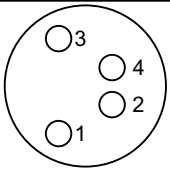
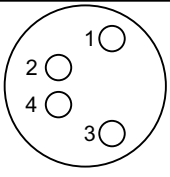
Table 2-24 Pin assignment for PROFIBUS

Pin	Assignment		Front view of the connector X1 DP1	Front view of the socket X1 DP2
	X1 DP1 connector (feed in)	X1 DP2 Socket (loop-through)		
1	-	Supply plus P5V*		
2	Data cable A			
3	Data reference potential M5*			
4	Data cable B			
5	Functional earth FE			
Shield-ing	Functional earth FE			
* The voltage may only be used for supplying the external terminating resistor. It is not permitted to loop-through the voltage by means of a cable to the next connector.				

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

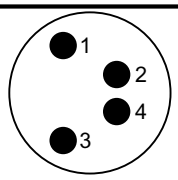
Table 2-25 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection1)	X31 socket (ET-Connection2)		X30	X31
1	RXP	RXP	Yellow		
2	TXP	TXP	White		
3	TXN	TXN	Blue		
4	RXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The following table shows the pin assignment of the connector for infeed of the supply voltage.

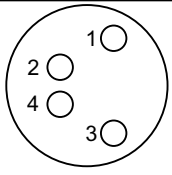
Table 2-26 Pin assignment of the supply voltage connector

Pin	Assignment X80 connector (power input)	Assignment of the wire color of the power line cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-27 Pin assignment of the supply voltage socket

Pin	Assignment X81 Socket (power output)	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage

Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage.

Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

3.3 Configuring PROFIBUS DP address and terminating resistor

Properties

Use the PROFIBUS address to specify at which address the ET 200AL distributed I/O system is addressed on the PROFIBUS DP.

The PROFIBUS DP address is configured for the ET 200AL distributed I/O system with a rotary coding switch on the front of the housing.

Requirements

The following requirements apply:

- Each address is only assigned once on the PROFIBUS DP.
- The configured PROFIBUS DP address must match the PROFIBUS address defined in the configuration software.
- A change of the PROFIBUS DP address is only valid after POWER ON/POWER OFF on the IM 157-1 DP interface module.

Required tools

You need the following tools to configure the PROFIBUS DP address:

- 14 mm socket wrench
- 2.5 mm screwdriver

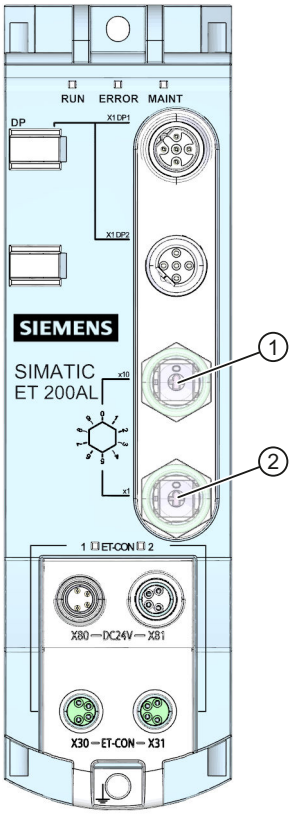
Setting the PROFIBUS DP address

Configurable PROFIBUS DP addresses are 1 to 99.

Proceed as follows to configure the PROFIBUS DP address:

1. Remove the two M12 sealing caps from the rotary coding switches (use 14 mm socket wrench, if needed).
2. Configure the desired PROFIBUS DP address with a screwdriver on the rotary coding switches.
   - Top rotary coding switch: Tens digit
   - Bottom rotary coding switch: Ones digit
3. Screw the two M12 sealing caps back onto the thread to protect the rotary coding switches (torque: 0.5 to 0.8 Nm).
4. Switch the supply voltage off and on again (POWER OFF/POWER ON).

The figure below shows the rotary coding switches for configuring the PROFIBUS DP address.

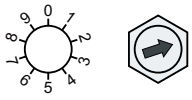
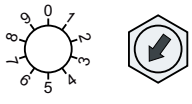


① Rotary coding switch for PROFIBUS DP (tens digit)
② Rotary coding switch for PROFIBUS DP address (ones digit)

Figure 2-15 Setting the PROFIBUS address

The following table shows how to set PROFIBUS address 26 as an example.

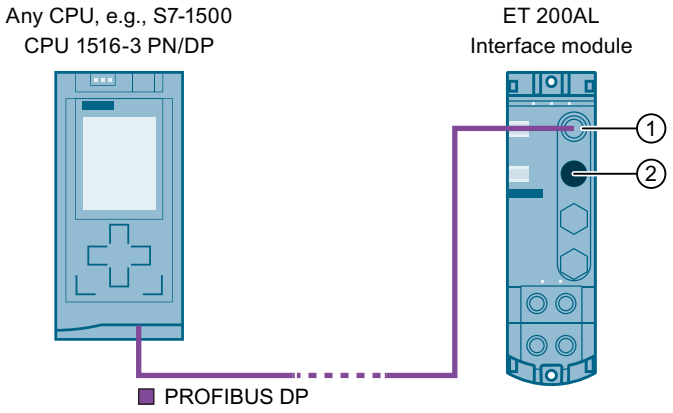
Table 2-28 Setting of the PROFIBUS address

	Tens digit	Position 2
	Ones digit	Position 6

Connecting the terminating resistor for PROFIBUS DP

Terminate a PROFIBUS DP segment, on both of its ends, which means on the first and last device of the segment, with its characteristic impedance. There are two different terminating resistors available for this purpose, for sockets and for connectors.

The figure below shows typical use of a terminating resistor.



① PROFIBUS infeed (connector)
② M12 socket with terminating resistor

Figure 2-16 Terminating resistor

Parameters

4

4.1 Parameters

The following table shows the parameters for the IM 157-1 DP interface module.

Table 2-29 Parameters

Parameters	Value range	Default[2]	Efficiency range
Configuration control[1]	• Disable • Enable	Disable	ET 200AL
Startup if preset configuration does not match actual configuration	• Disable • Enable	Disable	ET 200AL
Diagnostics interrupt	• Disable • Enable	Enable	ET 200AL
Hardware interrupt	• Disable • Enable	Enable	ET 200AL
Pull/plug module interrupt	• Disable • Enable	Enable	ET 200AL

1 Note that the "Startup if preset configuration does not match actual configuration" parameter is always activated when you use configuration control.

2 The defaults apply to the default startup. If no other parameters are specified by the DP master, the interface moduleIM 157-1 DP starts up with these parameters.

4.2 Explanation of the parameters

Configuration control

You can use this parameter to enable the configuration control function in the ET 200AL distributed I/O system.

NOTE

Configuration control

The configuration control function can only be used if you set the "Startup if preset configuration does not match actual configuration" parameter to "YES".

NOTE

Configuring the enable

If you configure the enable, the ET 200AL distributed I/O system requires a control data record 196 from the user program in order for the ET 200AL distributed I/O system to operate the I/O modules.

Additional information is available in the section Configuration control (option handling).

Startup if preset configuration does not match actual configuration

Enabled parameter
If the preset/actual configuration differ, **a** data exchange occurs between the DP master and the ET 200AL distributed I/O system.

Disabled parameter
If the preset/actual configuration differ, **no** data exchange occurs between the DP master and the ET 200AL distributed I/O system.

NOTE

More than 16 I/O modules in real configuration per ET-Connection line
The preset/actual configuration do not match parameter is valid for 16 I/O modules per ET-Connection line.
Up to 16 I/O modules are recognized per line. Additional I/O modules are not recognized. A diagnostics alarm is not issued for these I/O modules. All I/O modules in the actual system after the 16th I/O module remain unconfigured (LED DIAG flashes green) and are not involved in the data exchange.

Diagnostics interrupt

You can use this parameter to enable or disable diagnostics interrupts.

Hardware interrupt

You can use this parameter to enable or disable hardware interrupts.

Pull/plug module interrupt

You can use this parameter to enable or disable pull/plug module interrupts.

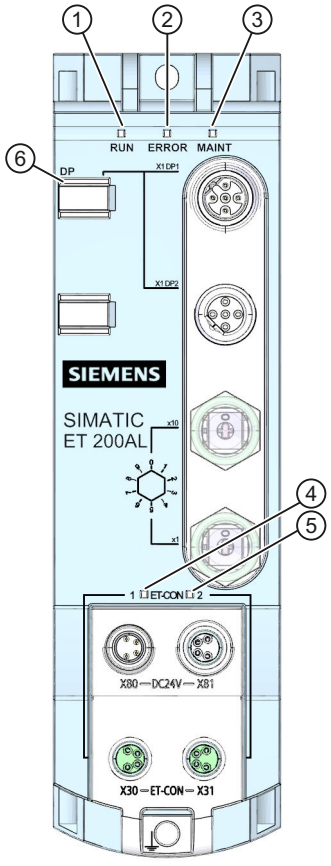
Interrupts, error messages, diagnostics and system alarms

5

5.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the IM 157-1 DP interface module.



①	RUN	(green)
②	ERROR	(red)
③	MAINT	(yellow)
④	ET-CON1	(green)
⑤	ET-CON2	(green)
⑥	DP	(green)

Figure 2-17 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 33).

LED RUN, LED ERROR, LED MAINT

Table 2-30 Status and error displays of the LEDs RUN, ERROR, MAINT

LEDs			Meaning	Solution
RUN	ERROR	MAINT		
Off	Off	Off	Supply voltage at interface module missing or too low	Check the supply voltage or switch it on on the interface module.
On	On	On	Test of LEDs during startup: The three LEDs light up simultaneously for approximately 0.25 s.	-
Flashes	Off	Off	Interface module is deactivated.	Activate the interface module with the configuration software or the user program.
			Interface module is not configured.	Configure the interface module with the configuration software.
			ET 200AL starts up.	-
			ET 200AL is being assigned parameters.	
On	Not relevant	Not relevant	ET 200AL is currently exchanging data with the DP master.	-
Not relevant	Flashes	Not relevant	Group error and group error channels	Evaluate the diagnostics and eliminate the error.
			The preset configuration does not correspond to the actual configuration of the ET 200AL.	Check the configuration of the ET 200AL to see whether a module is missing, defective or if a module that is not configured is connected to ET-CON1 or ET-CON2.
			Parameter assignment error in the I/O module	Evaluate the display of the module status in STEP 7 or in STEP 7 (TIA portal) and correct the errors in the I/O module.
Not relevant	Not relevant	On	Maintenance is demanded.	Execute maintenance
Flashes	Flashes	Flashes	Hardware or firmware faulty.[1]	Replace the interface module.
Flashes	Not relevant	Not relevant	Firmware is loading (all LEDs remain in their current state while the firmware update is being written)	---

1 LED DP off

DP LED

Table 2-31 Status display of the DP LED

DP LED	Meaning	Solution
☐ Off	There is no connection between the PROFIBUS interface of your PROFIBUS device and a communication partner (e.g. DP master).	Check whether the bus cable to the DP master is disconnected.
■ On	There is no connection between the PROFIBUS interface of your PROFIBUS device and a communication partner (e.g. DP master).	-

LED ET-CON1, LED ET-CON2

Table 2-32 Status displays of the LEDs ET-CON1 and ET-CON2

LEDs		Meaning	Solution
ET-CON1	ET-CON2		
☐ Off		There are no I/O modules available at the respective ET-Connection or the modules do not have supply voltage.	Check the wiring for the ET-Connection or the supply voltage for the I/O module.
■ On		A communications connection to at least one IO module at the corresponding ET-Connection is available.	-

5.2 Interrupts

5.2.1 Evaluating interrupts

Introduction

With certain process statuses/errors, the DP slave in each case creates an interrupt block with the corresponding information in the diagnostics frame (DPV1 interrupt mechanism). Regardless of this, the diagnostic status of the DP slave is displayed in the identifier-related diagnostics, in the module status, and in the channel diagnostics.

Interrupts in DPV1 mode

The ET 200AL distributed I/O system supports the following interrupts:

- Diagnostics interrupts
- Hardware interrupts
- Pull/plug module interrupt

5.2.2 Trigger a diagnostics interrupt

For an incoming or outgoing event (for example, wire break on a channel of an I/O module), the interface module triggers a diagnostics interrupt if the I/O modules were configured accordingly and "Enable:diagnostics interrupt" is set.

The CPU interrupts user program execution and processes the diagnostics interrupt OB (OB 82). The event that triggered the interrupt is entered in the start information of the diagnostics interrupt OB.

5.2.3 Triggering a hardware interrupt

When a hardware interrupt occurs, the CPU interrupts execution of the user program and processes the hardware interrupt OB, for example OB 40. The event that triggered the interrupt is entered in the start information of the hardware interrupt OB.

NOTE

Diagnostics "Hardware interrupt lost" (from I/O module)
Do not use hardware interrupts for technological purposes (e.g., cyclical generation of hardware interrupts).
If the hardware interrupt load is too high, hardware interrupts can get lost depending on the number of I/O modules and the communication load.

5.2.4 Triggering an insert/remove module interrupt

When an insert/remove module interrupt occurs, the CPU interrupts execution of the user program and processes the insert/remove module interrupt OB (OB 83). The event that triggered the interrupt is entered in the start information of the insert/remove OB.

The pull/plug OB (OB 83) is also triggered for all subsequent I/O modules, because the ET-Connection and/or the power supply is interrupted.

5.2.5 Structure of data records

Definition

The interrupt section of the slave diagnostics indicates the interrupt type and the event that led to an interrupt being triggered. The interrupt section comprises 62 bytes including an interrupt header.

Position in the diagnostics frame

The interrupt section is located after the channel diagnostics.

Data records

The diagnostics data of a module are located in the data records 0 and 1:

- Data record 0 contains 4 bytes of diagnostics data that describe the current status of the distributed I/O system. Data record 0 is part of the header information of the OB 82 (local data bytes 8 to 11).
- Data record 1 contains 4 bytes of diagnostics data that are also available in data record 0.

The figure below shows the structure of data record 0.

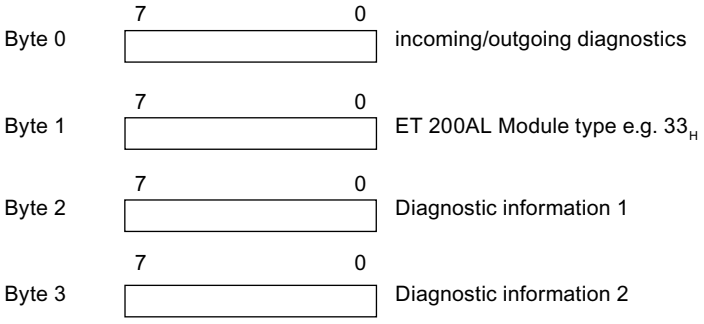


Figure 2-18 Structure of data record 0

The figure below shows the structure of data record 1.

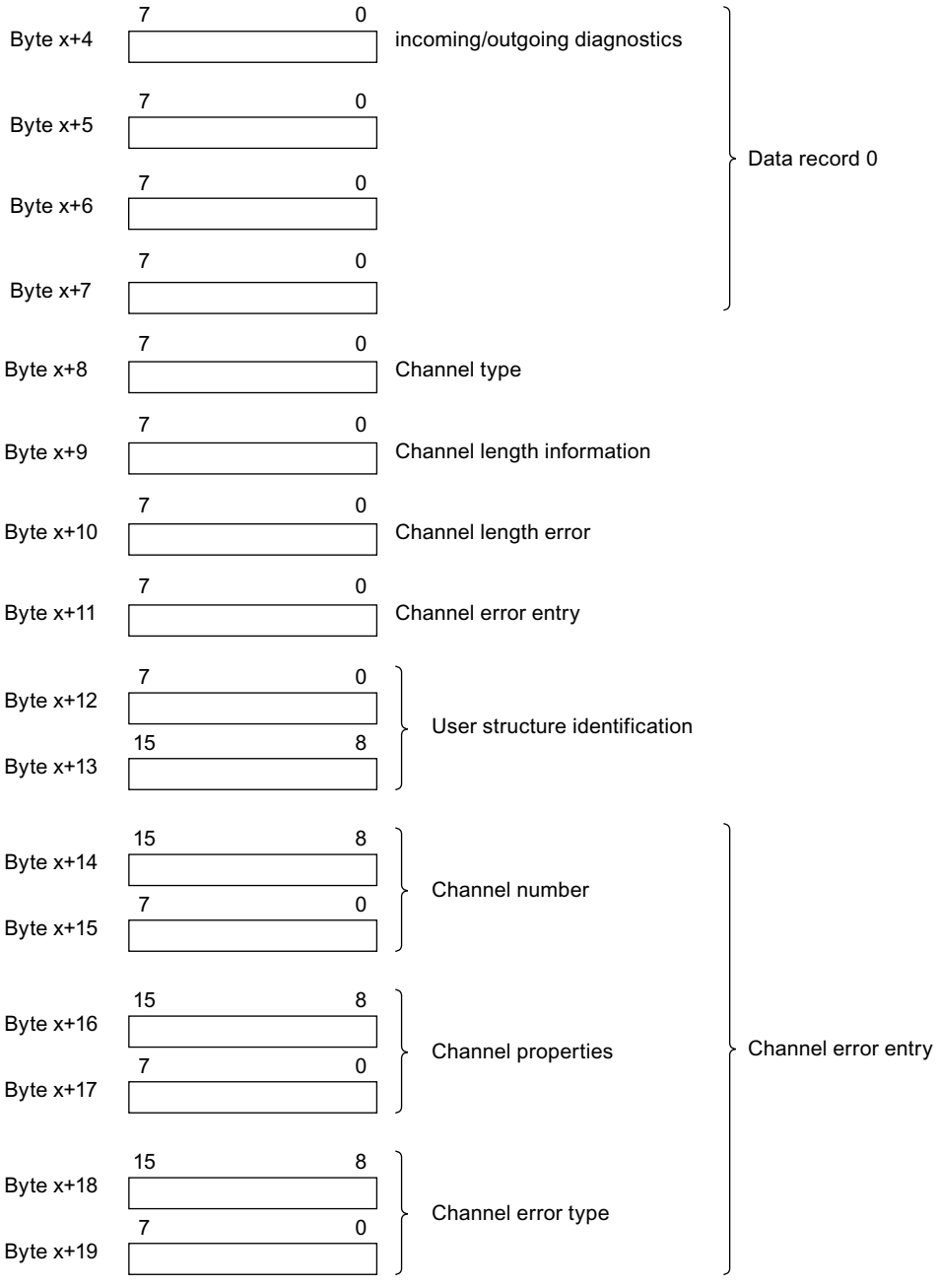


Figure 2-19 Structure of data record 1

Reading data records

You have the option to read out data records 0 and 1 via SFC 59 (RD_REC) or SFB 52 (RDREC). The data length of data record 1 is up to 240 bytes. In this case, data record 1 contains up to 38 channel fault entries.

Note the figures below in this section.

Contents

The contents of the interrupt information depend on the interrupt type:

- In the case of diagnostics interrupts, diagnostics data record 1 (up to 58 bytes) is sent as interrupt status information (starting from byte x+4).
- The length of the interrupt status information for hardware interrupts is 4 bytes.

Structure of interrupts

The figure below shows the structure of the interrupt section for the ET 200AL distributed I/O system.

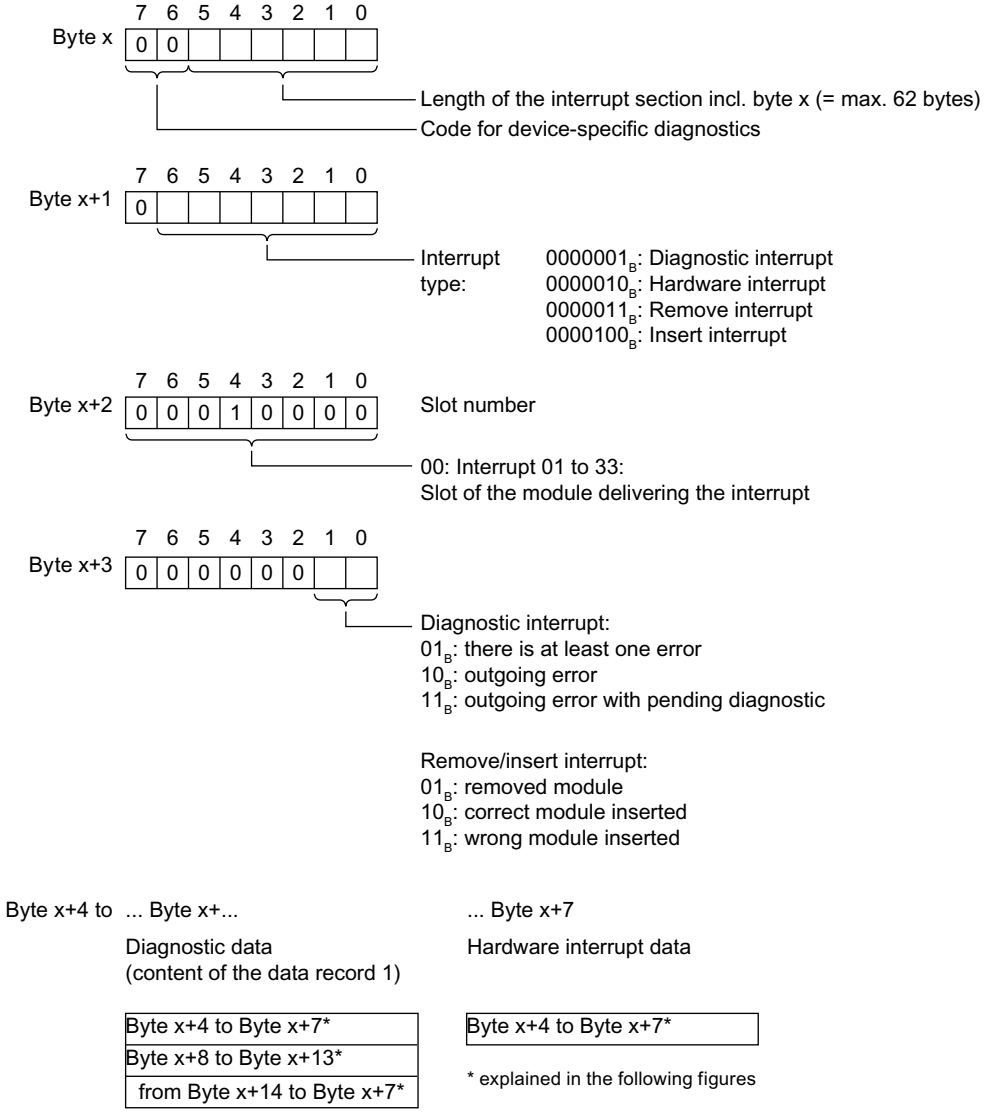


Figure 2-20 Structure of the interrupt status of the interrupt section

Diagnostics interrupt, byte x+4 to x+7

The figure below shows the structure of the diagnostics interrupt of byte x+4 to byte x+7.

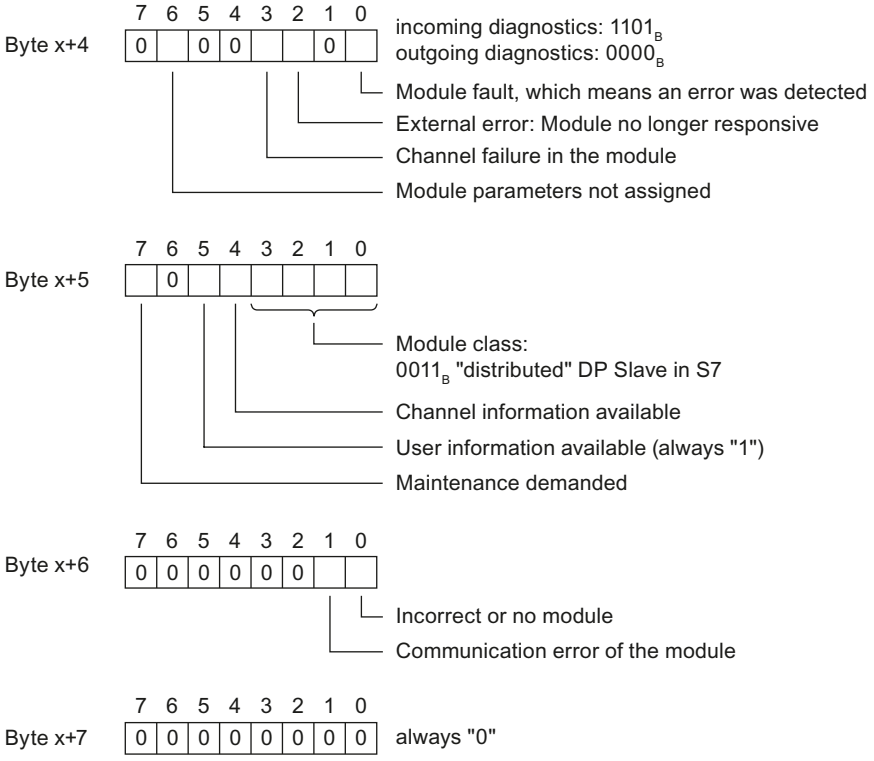


Figure 2-21 Structure of bytes x+4 to x+7 for diagnostics interrupt

Diagnostics interrupt, starting at byte x+8

The figure below shows the structure of the diagnostics interrupt starting at byte x+8.

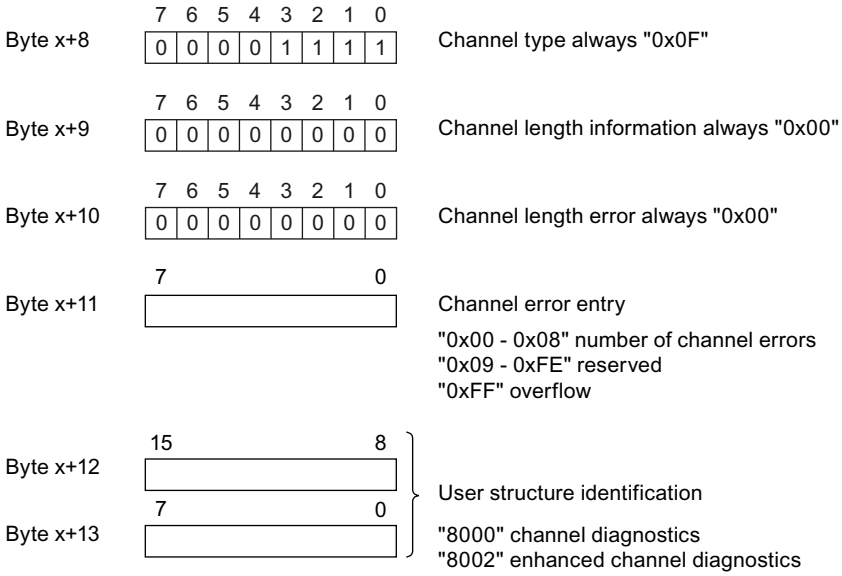


Figure 2-22 Structure starting at byte x+8

Diagnostics interrupt from the modules, starting at byte x+14

The channel error entries start from byte x+14. A channel fault entry is 6 bytes long and can follow 8 times starting at byte x+14.

If you read the channel faults with an SFB or SFC, then 38 channel diagnostics are possible.

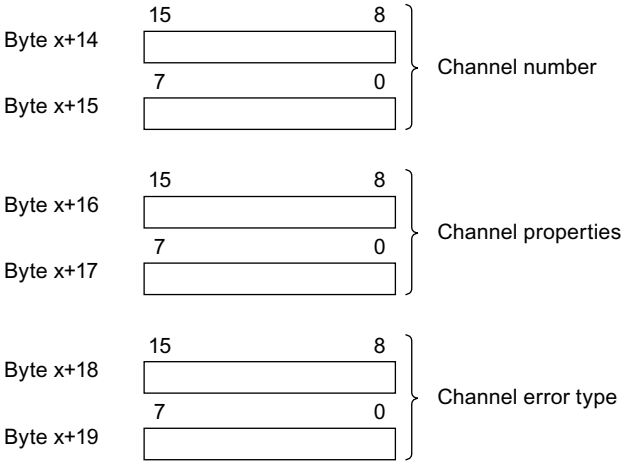


Figure 2-23 Structure starting from byte x+14

The following table is used to explain the channel error entries.

	Description	
Channel number	0 ... 63: Channel number for channel error 0x8000: Entire submodule	
Channel properties	Bits 0 to 7	00_H: Free data type 01_H: bit 02_H: 2 bit 03_H: 4 bit 04_H: byte 05_H: word 06_H: double word 07_H to FF_H: Reserved
	Bit 8	0: Channel 1: Channel group
	Bit 9, 10	00_H: Diagnostics 01_H: Maintenance demanded 02_H: Maintenance required 03_H: Reserved
	Bit 11, 12	00_H: Channel error-free 01_H: Incoming diagnostics 02_H: Outgoing diagnostics 03_H: Outgoing diagnostics, but other diagnostics are also pending on this channel
	Bits 13 to 15	00_H: Reserved 01_H: Input channel 02_H: Output channel 03_H: Input/output channel
Channel error type	Explanations are available in the device manuals, in the section "Diagnostic alarms".	

Example of a diagnostics interrupt

The figure below shows an example of a diagnostics interrupt.

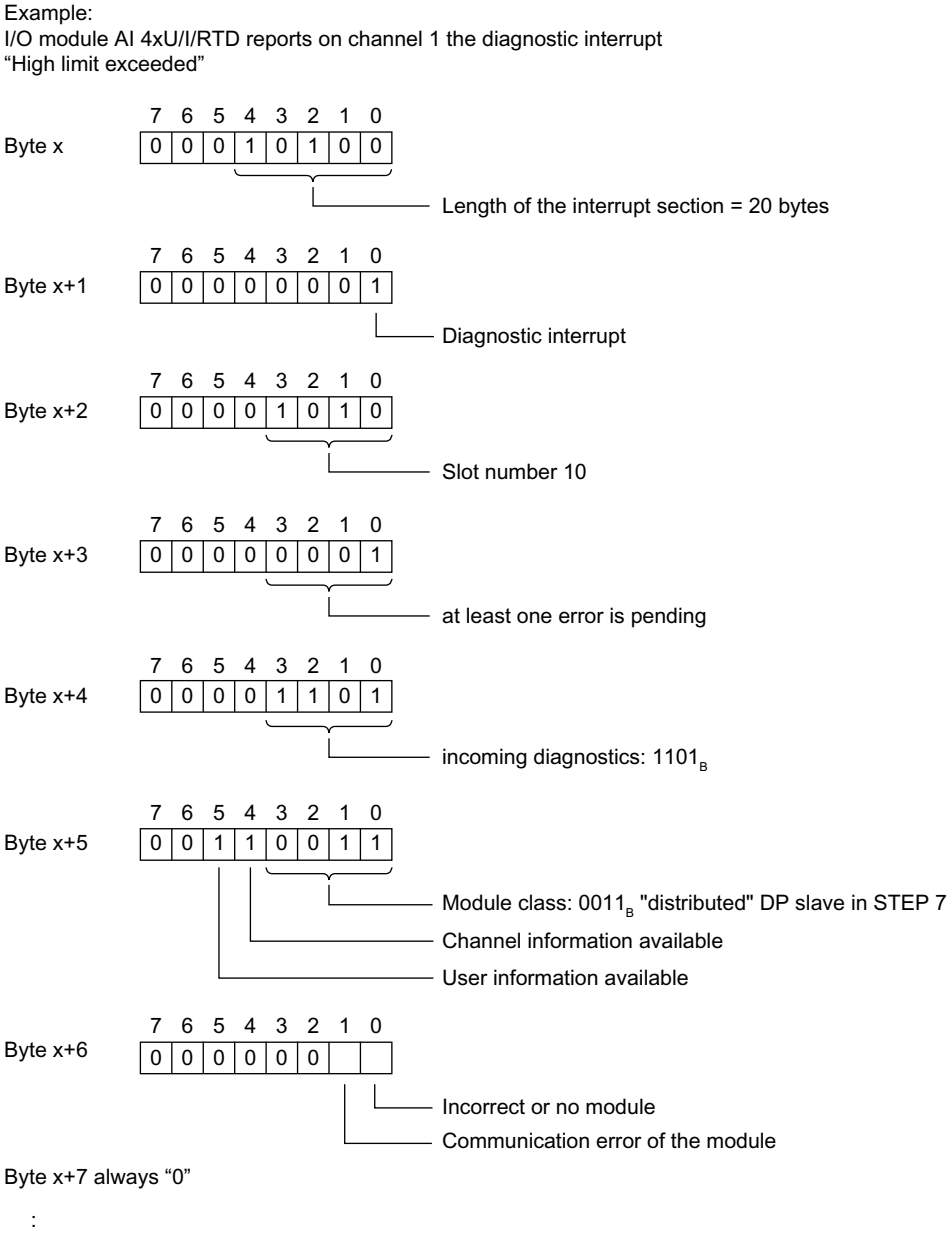


Figure 2-24 Example of a diagnostics interrupt (part 1)

:

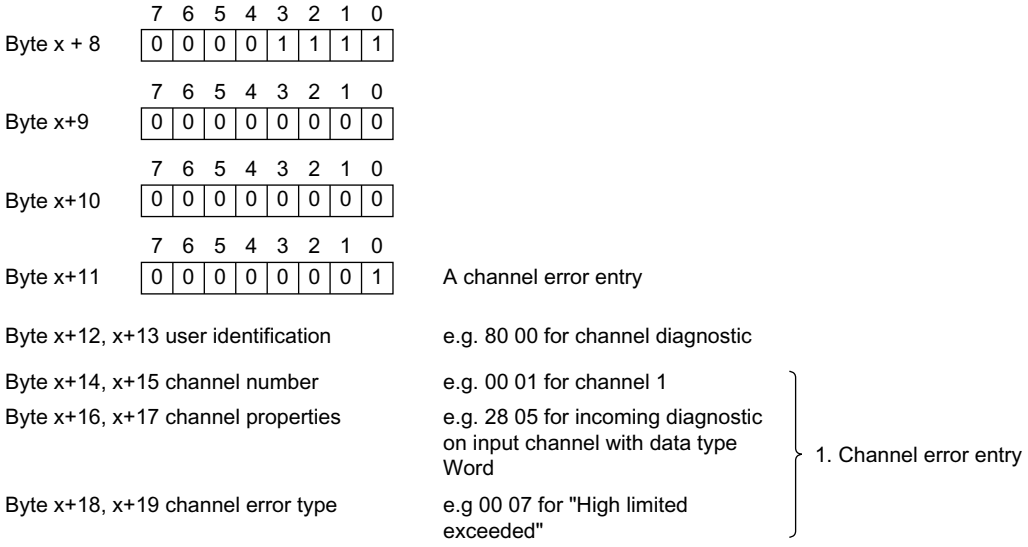


Figure 2-25 Example of a diagnostics interrupt (part 2)

Hardware interrupt of digital and analog input modules, bytes x+4 to x+7

The figure below shows the structure of a hardware interrupt.

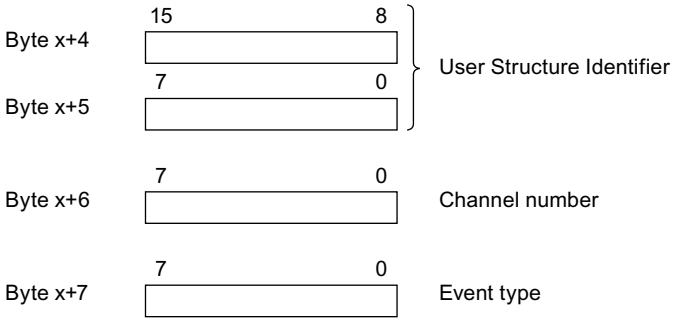


Figure 2-26 Structure as of Byte x+4 for hardware interrupt

NOTE

Byte x+4

You will find the event type in the device manual of the module that triggered the hardware interrupt.

5.3 Alarms

5.3.1 Diagnostics alarms

Actions after a diagnostics alarm in DPV1 mode

The error is entered in the channel diagnostics in the diagnostics frame:

- In DPV1 mode, diagnostics can be reported as diagnostics interrupts.
- After a diagnostics alarm, this is
  - entered in the diagnostics frame as a diagnostics interrupt block (always only one interrupt).
  - Stored in the diagnostics buffer of the CPU.
- The ERROR LED of the interface module flashes.
- OB 82 is called. If OB 82 is not available, the CPU goes into STOP mode.
- Acknowledgment of the diagnostics interrupt (a new interrupt is possible thereafter).

Length of the diagnostics frame

- The maximum frame length for the ET 200AL distributed I/O system with IM157-1 DP interface module (DPV1 mode) is 244 bytes.
- The minimum frame length is 6 bytes.

Reading out the diagnostics data

Table 2-33 Reading the diagnostics with STEP 7

Automation system with DP master	Application	See...
SIMATIC S7/M7	Slave diagnostics in plain text in "DP Slave Diagnostics" tab on STEP 7 interface	"Hardware diagnostics" in STEP 7 online help
	"DP NRM_DG" instruction (SFC 13) Reading out slave diagnostics (store in the data area of the user program)	SFC: see STEP 7 online help
	"RD_REC" instruction (SFC 59) Reading out data records of the S7 diagnostics data (store in the data area of the user program)	See System and Standard Functions reference manual
	"RDREC" instruction (SFC 52) Reading data records from the DP slave	SFB: refer to STEP 7 online help (system functions/function blocks)
	"RALRM" instruction (SFC 54) Receiving interrupts from the interrupt OBs	SFB: refer to STEP 7 online help (system functions/function blocks)

5.3.2 Slave diagnostics

The figure below shows the structure of the slave diagnostics.

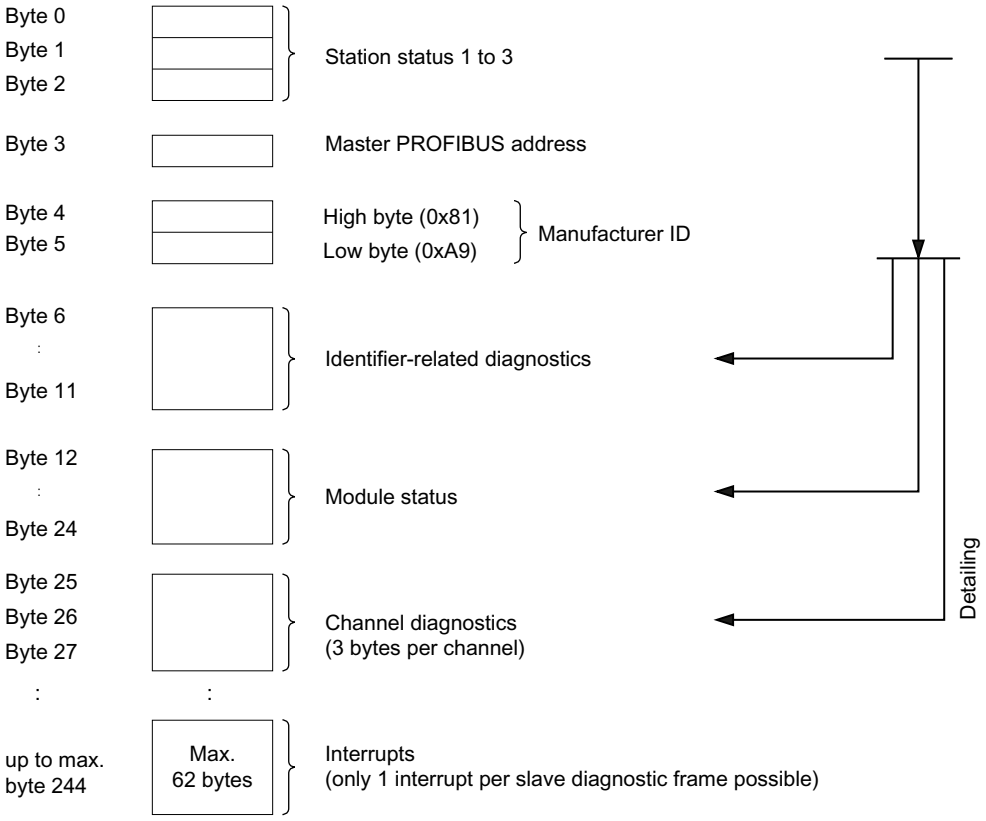


Figure 2-27 Structure of the slave diagnostics

NOTE

The length of the diagnostics frame varies with the IM 157-1 DP (depending on parameter assignment) between 6 and 244 bytes in DPV1 mode.

You can identify the length of the last received diagnostics frame in STEP 7 from the RET_VAL parameter in SFC 13.

5.3.3 Station statuses 1 to 3

The following tables show station status 1 to 3 and provide an overview of the status of a DP slave.

Structure of station status 1 (byte 0)

Table 2-34 Structure of station status 1 (byte 0)

Bit	Meaning	Cause/Solution
0	1: The DP slave is not responding to the DP master.	• Correct PROFIBUS address set on the DP slave? • Bus connector connected? • Is the DP slave connected to the voltage supply? • RS485 repeater properly configured?
1	1: The DP slave is not yet ready to exchange data.	• Wait; the DP slave is currently starting up.
2	1: The configuration data transferred from the DP master to the DP slave does not match the DP slave configuration.	• Has the correct station type or the correct DP slave configuration been entered in the configuration software?
3	1: External diagnostics is available. (Group diagnostics display)	• Evaluate the ID-specific diagnostics, the module status, and/or the channel diagnostics. As soon as all errors have been eliminated, bit 3 is reset. The bit is set again when there is a new diagnostics alarm in the bytes of the aforementioned diagnostics.
4	1: The requested function is not supported by the DP slave (e.g. changing the PROFIBUS address using software).	• Check the configuration.
5	1: The DP master cannot interpret the response of the DP slave.	• Check the bus configuration.
6	1: The DP slave type does not match the software configuration.	• Has the correct station type been entered in the configuration software?
7	1: Parameters have been assigned to the DP slave by a different DP master (not the one that currently has access to the DP slave).	• The bit is always 1, for example, if you access the DP slave with the programming device or another DP master. • The PROFIBUS address of the DP master that assigned parameters to the DP slave is located in the "Master PROFIBUS address" diagnostics byte.

Structure of station status 2 (byte 1)

Table 2-35 Structure of station status 2 (byte 1)

Bit	Meaning	
0	1:	The DP slave parameters need to be reassigned.
1	1:	A diagnostics alarm is pending. The DP slave will not operate until the problem is eliminated (static diagnostics alarm).
2	1:	The bit on the DP slave is always "1".

Bit	Meaning	
3	1:	The watchdog is activated for this DP slave.
4	1:	The DP slave has received the control command "FREEZE".[1]
5	1:	The DP slave has received the control command "SYNC".[1]
6	0:	Bit is always "0".
7	1:	The DP slave is disabled, that is, it has been removed from the processing in progress.
[1] The bit is updated only if another diagnostics alarm also changes.		

Structure of station status 3 (byte 2)

Table 2-36 Structure of station status 3 (byte 2)

Bit	Meaning	
0 to 6	0:	Bits are always set to "0".
7	1:	• There are more diagnostic alarms pending than the DP slave is able to store. • The DP master cannot enter all the diagnostics alarms sent by the DP slave in its (channel) diagnostics buffer.

5.3.4 Master PROFIBUS address

The following is stored in the diagnostic byte Master PROFIBUS address:

- The PROFIBUS address of the DP master that assigned the parameters to the DP slave.
- The PROFIBUS address of the DP master that has read and write access to the DP slave.

The master PROFIBUS address is found in byte 3 of the slave diagnostics.

5.3.5 Manufacturer ID

The manufacturer ID contains a code specifying the type of the DP slave.
The following table shows the structure of the manufacturer ID (bytes 4, 5).

Table 2-37 Description of the manufacturer ID

Byte 4	Byte 5	Manufacturer ID
81_H	$A9_H$	IM 157-1 DP interface module

5.3.6 Identifier-related diagnostics

The identifier-related diagnostics indicates whether modules of the ET 200AL distributed I/O system have errors or not. Identifier-related diagnostics starts at byte 6 and comprises 6 bytes.

The figure below shows how the identifier-related diagnostics for the ET 200AL distributed I/O system is structured with the IM 157-1 DP interface module.

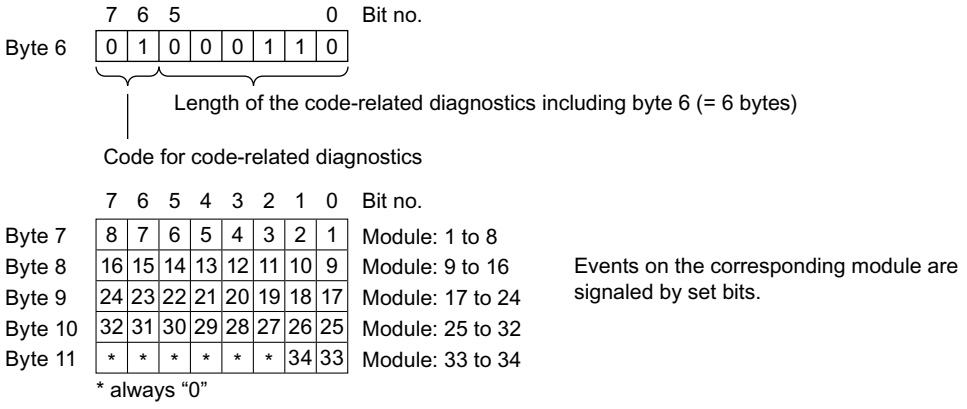


Figure 2-28 Structure of the identifier-related diagnostics

5.3.7 Module status

The module status indicates the status of the configured modules and provides more information on the identifier-related diagnostics with respect to the configuration. The module status begins after the identifier-related diagnostics and comprises 13 bytes.

The figure below shows how the module status for the ET 200AL distributed I/O system is structured with the IM 157-1 DP interface module.

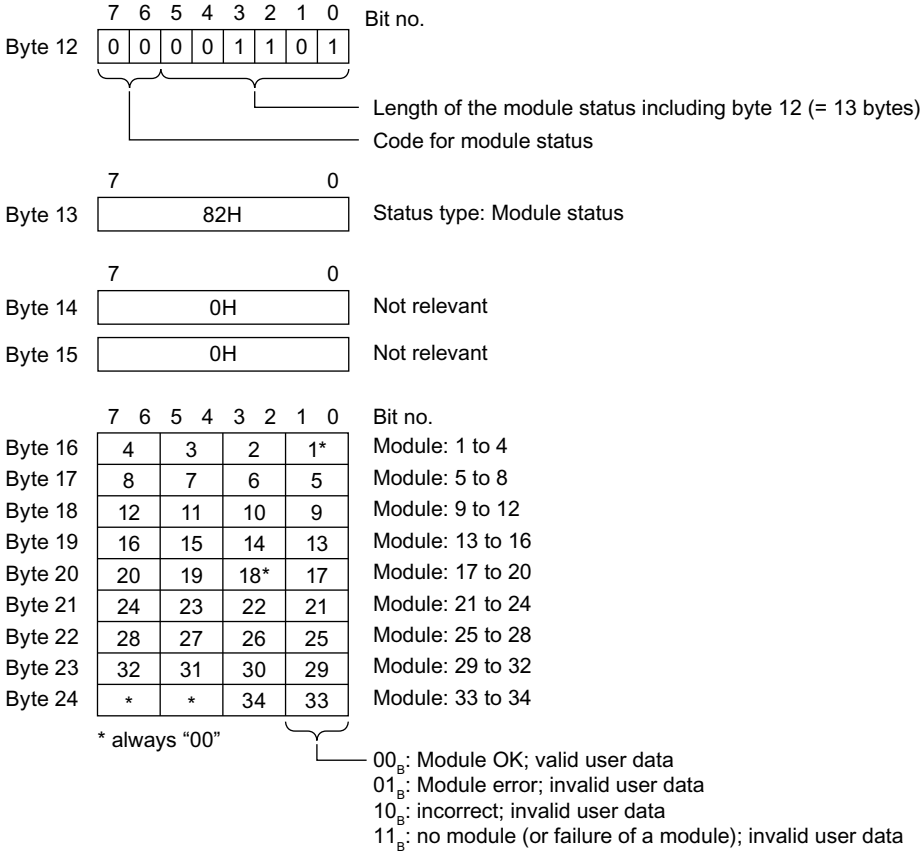


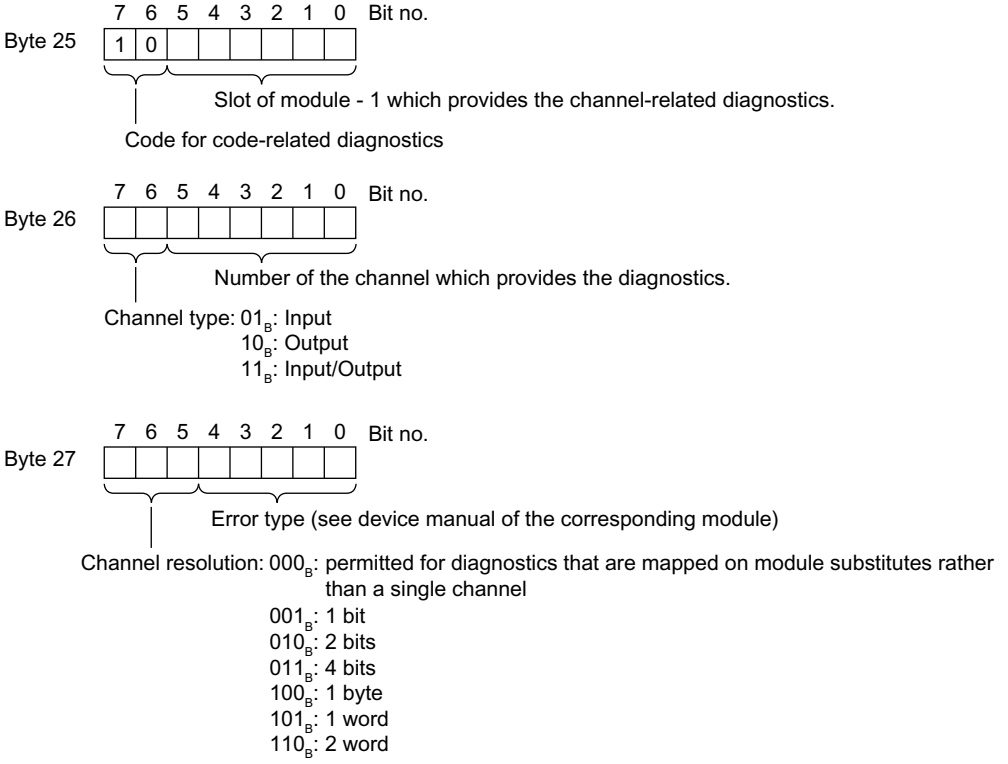
Figure 2-29 Module status structure

5.3.8 Channel diagnostics

Function

Channel diagnostics provides information about channel errors in modules and details of the identifier-related diagnostics. Channel diagnostics begins after the module status. Channel diagnostics does not affect the module status.

The figure below shows how the channel diagnostics for the ET 200AL distributed I/O system is structured with the IM 157-1 DP interface module.



Bytes 28 to 30 Next channel-related diagnostic alarm (assignment as with byte 25 to 27)

Max. byte 109 in DPV1 mode

Figure 2-30 Structure of channel diagnostics

Technical specifications

6

Technical specifications of the interface module IM 157-1 DP

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7157-1AA00-0AB0/td?dl=en).

Article number	6ES7157-1AA00-0AB0
General information	
Product type designation	IM 157-1 DP
HW functional status	FS02
Firmware version	V1.0.x
Vendor identification (VendorID)	81A9H
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	From V5.5 SP4 Hotfix 3
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
Configuration control	
via dataset	Yes
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Input current	
Current consumption (rated value)	50 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Power loss	
Power loss, typ.	1.7 W
Address area	
Address space per station	
• Address space per station, max.	244 byte
Interfaces	
Number of PROFIBUS interfaces	1
1. Interface	
Interface type	PROFIBUS DP
Interface types	
• RS 485	Yes

Article number	6ES7157-1AA00-0AB0
• M12 port	Yes; 2x M12 B-coded
Protocols	
• PROFIBUS DP slave	Yes
Interface types	
RS 485	
• Transmission rate, max.	12 Mbit/s
PROFIBUS DP	
Services	
– SYNC capability	Yes
– FREEZE capability	Yes
– Direct data exchange (slave-to-slave communication)	Yes
– DPV0	Yes
– DPV1	Yes
Interrupts/diagnostics/status information	
Diagnostics function	Yes
Alarms	
• Diagnostic alarm	Yes
Diagnostics indication LED	
• RUN LED	Yes; green LED
• ERROR LED	Yes; red LED
• MAINT LED	Yes; Yellow LED
• Connection display DP	Yes; green LED
Potential separation	
between the load voltages	Yes
between PROFIBUS DP and all other circuit components	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SILCL according to IEC 62061	SILCL 2
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Connection method	
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded

Article number	6ES7157-1AA00-0AB0
Dimensions	
Width	45 mm
Height	159 mm
Depth	46 mm
Weights	
Weight, approx.	211 g

Dimension drawing

A

The figure below shows the dimension drawing of the IM 157-1 DP interface module in the front and side view.

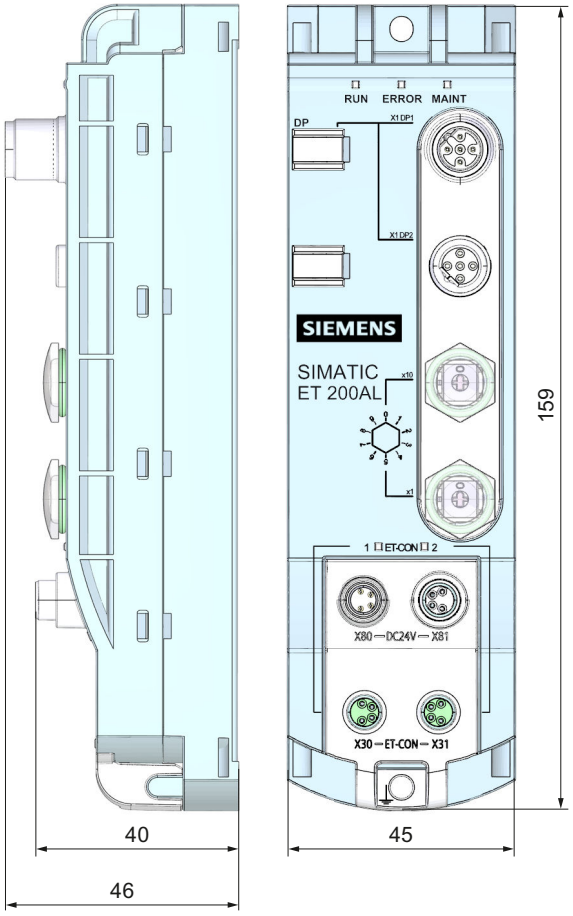


Figure 2-31 Dimension drawing

Cycle times

B

The following figure shows the cycle times at ET-Connection based on the number of I/O modules.

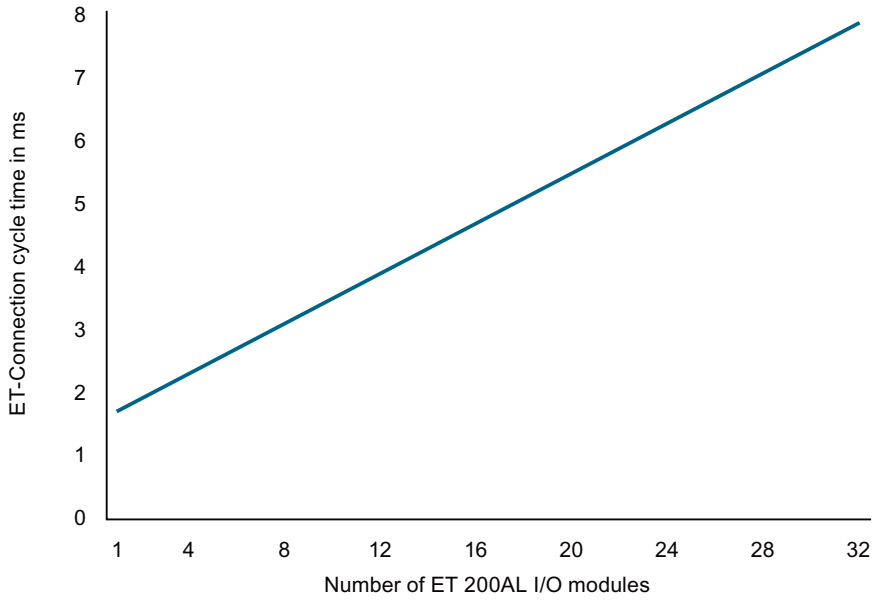


Figure 2-32 Cycle times

The cycle time is independent of the PROFIBUS transmission rate.

SIEMENS

SIMATIC

ET 200AL
IM 157-1 PN
(6ES7157-1AB00-0AB0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters 5

Interrupts, error messages, diagnostics and system alarms 6

Technical specifications 7

Dimension drawing A

Cycle times B

05/2025
A5E32347036-AF

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 4
1.1.1 Tool support 5
1.2 SIMATIC Technical Documentation 6

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 12

3.1 Properties 12
3.2 Operator controls and display elements 14
3.3 Functions 14
3.3.1 PROFINET IO 14
3.3.2 PROFIenergy 17
3.3.2.1 What is PROFIenergy? 17
3.3.2.2 Principle of operation 18
3.3.2.3 Parameter assignment 20
3.3.2.4 PROFIenergy control data records 22
3.3.3 Configuration control (option handling) 23

4 Wiring 24

4.1 Terminal and block diagram 24
4.2 Pin assignment 25

5 Parameters 27

5.1 Parameters 27
5.2 Explanation of the parameters 27

6 Interrupts, error messages, diagnostics and system alarms 28

6.1 Status and error displays 28
6.2 Interrupts 30
6.2.1 Evaluating interrupts 30
6.2.2 Trigger a diagnostics interrupt 31
6.2.3 Triggering a hardware interrupt 31
6.2.4 Triggering an insert/remove module interrupt 31
6.3 Alarms 32

6.3.1 Diagnostics alarms 32
6.3.2 Maintenance events 33
6.3.3 Channel diagnostics 33
6.3.4 Invalid configuration states of ET 200AL on the PROFINET IO 34
6.3.5 STOP of the IO controller and recovery of the IO device 34

7 Technical specifications 35

A Dimension drawing 38

B Cycle times 39

Introduction

1

Purpose of the documentation

This manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in this Equipment Manual, the System Manual, and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Changes compared to the previous version

This manual contains the following changes/additions compared to the previous version:

- Supplement to the Industrial cybersecurity (Page 9) section
- Adaptations in the Cycle times (Page 39) section
- Adaptations in the Technical specifications (Page 35) section

Conventions

Please also observe notes marked as follows:

NOTE
Indicates important product information to which particular attention should be paid.

1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.1 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)
     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:
     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the SIMATIC ET 200AL Distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965) System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-relevant information pertaining to your SIEMENS device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all cybersecurity-relevant information.

Topics with cybersecurity-relevant information	Reference
Operational application environment and security assumptions	
Requirements for the operational application environment of the system and security assumptions	You can find this section in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Security properties of the product	
Access protection	Note the information on access protection in the Protection chapter of the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Data integrity	The topic of data integrity is described in the "Industrial cybersecurity" section of the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Signed firmware update	The topic of signed firmware updates is described in the "Industrial cybersecurity" section of the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
PROFINET Security Class 1 • The device supports PROFINET Security Class 1. • With the introduction of PROFINET Security Class 1, additional security settings have been integrated into the PROFINET communication.	Detailed information about PROFINET Security Class 1 and the additional security settings can be found in the PROFINET with STEP 7 Function Manual (https://support.industry.siemens.com/cs/us/en/view/49948856)
Supported Ethernet services	Information about supported services can be found in the Technical specifications (Page 35) section. You can find detailed information on the supported Ethernet services in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Interfaces, ports, protocols and services	
Information on the following is security-relevant: • Communication layer and communication role • Default states • Enabling/disabling of ports and services	You can find detailed information on these topics in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Secure operation	
Recommendations for safe operation	You can find cross-system information on the safe operation of interface modules in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Corrective measures for known risks	Corrective measures for known risks are announced on the Siemens ProductCERT and Siemens CERT (https://siemens.com/productcert) web page. You can find more information on SIEMENS ProductCERT in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).

Topics with cybersecurity-relevant information	Reference
Security checks	You can find descriptions of specific security measures, such as cyclic checks of the configuration via checksums, in the Industrial cybersecurity section of the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).
Secure decommissioning Products that contain security-relevant data must be securely decommissioned before disposal or resale.	You can find information on secure decommissioning in the Secure operation of the system section in the System Manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).

Product overview

3

3.1 Properties

Article number

6ES7157-1AB00-0AB0

View of the module



Figure 2-33 View of the IM 157-1 PN interface module

Properties

The module has the following technical properties:

- Connects the ET 200AL distributed I/O system with PROFINET IO
- 24 V DC supply voltage
- Support for 2 ET-Connection lines
- Dimensions: 45 x 159 mm

The functions supported by the module are found in the chapter Functions (Page 14).

Maximum configuration

The module has the following maximum configuration:

- 1430 bytes input data
- 1430 bytes output data
- 32 I/O modules, up to 16 I/O modules can be connected for each ET-Connection line

NOTE

- In the case of a shared device configuration, the sum of the I/O data of all controllers that share the device applies.
- If more than two (max. four) controllers share the device, the maximum amount of I/O data including user data qualifier is limited to 360 bytes per controller.

Accessories

The following component is included with the module in the packaging:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

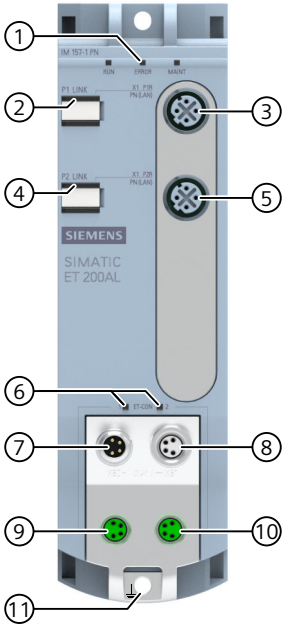
- Connectors
- Cables
- Stripping Tool for PROFINET
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You will find additional information on accessories and the other components in the Accessories/Spare parts section of the ET 200AL Distributed I/O System (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator control and display elements of the interface module IM 157-1 PN.



① RUN, ERROR, MAINT: LED indicators for the current operating state and diagnostic status
② P1 LINK: LED indicators for the current operating state of the 1st PROFINET interface
③ X1 P1 R: 1. PROFINET interface
④ P2 LINK: LED indicators for the current operating state of the 2nd PROFINET interface
⑤ X1 P2 R: 2. PROFINET interface
⑥ ET-CON1, ET-CON2: LED indicators for ET-Connection
⑦ X80: Connector for infeeding the supply voltage (POWER input)
⑧ X81: Socket for looping-through the supply voltage (POWER output)
⑨ X30: Socket for ET-Connection1
⑩ X31: Socket for ET-Connection2
⑪ Functional grounding (FE)

Figure 2-34 Operator controls and display elements

3.3 Functions

3.3.1 PROFINET IO

Introduction

The interface module supports the following PROFINET IO functions:

- Integrated switch with 2 ports
- Supported Ethernet services: ping, arp, network diagnostics (SNMP)/MIB-2, LLDP
- Port diagnostics
- Deactivating of ports

- Real-time communication
- Isochronous real-time communication
- Minimum update time 250 µs
- Media redundancy (MRP)
- Media redundancy with planned duplication (MRPD)
- Device replacement with topological configuration
- Device replacement without topological configuration
- Shared Device
- Identification data I&M0 to I&M4
- Firmware update via PROFINET IO
- Reset to factory settings via PROFINET IO
- PROFIenergy
- Configuration control (option handling)
- Value status (of I/O modules)

Requirements

The following table shows the software requirements for the use of PROFINET IO functions with the IM 157-1 PN interface module.

Table 2-38 Software requirements for PROFINET IO functions

PROFINET IO function	Configuration software	
	STEP 7 (TIA Portal) V13 or higher (with GSD file)	**STEP 7 V5.5 SP4 or higher (with GSD file)/Software from third-party manufacturer[2]**
Real-time communication	X	X
Isochronous real-time communication	X	X
Device replacement without programming device	X	X
Media redundancy	X	X
Shared device	X[1]	X

1 Use a S7-1500 CPU as a controller to use a shared device with STEP 7 (TIA Portal).

2 Systems of third-party manufacturers: Depending on the range of functions of the third-party system

Real-time communication

A transmission method for PROFINET IO based on a cyclic data exchange with a provider-consumer model.

Isochronous real-time communication

Synchronized transmission method for cyclic exchange of IRT data between PROFINET devices. A reserved bandwidth within the send clock is available for IRT data. The reserved bandwidth ensures that IRT data can be transferred at reserved synchronized intervals, without being influenced by other higher network loads (e.g., TCP/IP communication, or additional real-time communication).

A topological configuration is required for IRT.

NOTE

IO controller as sync master with IRT communication

We recommend that you also operate the IO controller as a sync master when configuring IRT communication.

Otherwise IRT and RT configured IO devices may fail if the sync master fails.

Device replacement without programming device

IO devices with this function can easily be replaced. You do not have to assign the device name with the PG.

The replaced IO device is assigned the device name by the IO controller and not by the programming device. The IO controller uses the configured topology and the neighboring relationships determined by the IO devices for this purpose. To do this, all devices involved must support the LLDP protocol (Link Layer Discovery Protocol). The configured target topology must match the actual topology.

IO devices which were already used in another configuration must be reset to factory settings before being reused.

Media redundancy

Function for safeguarding communication and plant availability. Redundant transmission lines (ring topology) ensure that another communication path is made available in the event of a transmission section failure.

Shared device

A shared device is an IO device that provides its data to up to four IO controllers.

The "Shared device" function allows the modules or submodules of an IO device to be divided up among different IO controllers. Thus allowing flexible automation concepts. You have, for example, the possibility of combining I/O modules lying near other into an IO device.

When operating as a shared device, there might be temporary delays in the update of the IO data when establishing or terminating additional communications relationships to an IO controller.

You can find additional information in the STEP 7 online help and the manual and in the function manual PROFINET with STEP 7 V14 (http://support.automation.siemens.com/WW/view/en/49948856).

Cabling with fixed connection setting

If you configure a fixed connection setting for the port in STEP 7, you also have to disable "Autonegotiation/Autocrossover". By disabling "Autonegotiation/Autocrossover" you speed up establishment of the communication path.

Replacement of an IM 157-1 PN

If you replace an interface module with an interface module that has already been used, you must reset this IO device to the delivery state with "Reset to factory settings".

You will find more information on "Resetting to factory settings" in the ET 200AL Distributed I/O System (http://support.automation.siemens.com/WW/view/en/89254965) system manual in the section "Resetting interface module (PROFINET) to factory settings".

Reference

You will find more information on the PROFINET IO functions in the PROFINET with STEP 7 V14 (http://support.automation.siemens.com/WW/view/en/49948856) Function Manual and in the STEP 7 online help.

3.3.2 PROFIenergy

3.3.2.1 What is PROFIenergy?

Introduction

PROFIenergy is a PROFINET-based data interface which makes it possible to switch off consumers in a coordinated and centrally controlled manner during break times regardless of the manufacturer or device. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

PROFINET devices are switched off with special commands in the user program of the PROFINET IO controller. Additional hardware is not needed: The PROFIenergy commands are interpreted by the PROFINET devices.

The device which provides PROFIenergy and supports the matching control data record owns the PE-Entity, the access point for these control data records. This PE-Entity represents I/O modules which do not have their own PE-Entity on the interface module. I/O modules that have their own PE-Entity are always addressed directly.

For the ET 200AL distributed I/O system, the PE-Entity is exclusively provided by the PROFINET interface module.

Procedure

To configure PROFIenergy, follow these steps:

1. Create the parameter data record, Index 3, in STEP 7.
2. Transfer the parameter data record to the interface module with the instruction "WRREC" - SFB 53.
3. Create the user program with the FBs to control the PROFIenergy commands ("PE_START_END" - FB 815, "PE_CMD" - FB 816).
4. Transfer the user program to the CPU.

Additional information

You will find more information on the Internet (http://www.profibus.com) under Common Application Profile PROFIenergy; Technical Specification for PROFINET; as well as in the following documentation:

- System manual ET 200AL Distributed I/O System (https://support.industry.siemens.com/cs/ww/en/view/89254965)
- Device manuals I/O modules (https://support.industry.siemens.com/cs/ww/en/ps/14247/man)
- System manual PROFINET System Description (https://support.industry.siemens.com/cs/ww/en/view/19292127)
- PROFINET with STEP 7 V14 (https://support.industry.siemens.com/cs/ww/en/view/49948856), function manual, section: Saving energy with PROFIenergy
- Application guide for implementation of shutdown concepts with PROFIenergy. (https://support.industry.siemens.com/cs/ww/en/view/96837137)
- Saving energy with SIMATIC S7 (STEP 7 as of V5.5) (https://support.industry.siemens.com/cs/ww/en/view/41986454)
- Saving energy with SIMATIC S7 and SIMATIC HMI (TIA Portal) (https://support.industry.siemens.com/cs/ww/en/view/58235225)
- SIMATIC S7 library for simple configuration of PROFIenergy. (https://support.industry.siemens.com/cs/ww/en/view/109478388)
- You will find additional information on the PROFIenergy FBs ("PE_START_END" - FB 815, "PE_CMD" - FB 816) in the online help for STEP 7 V5.5 SP2 and higher on System functions/system function blocks.

Application examples and manual information are also available online FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

3.3.2.2 Principle of operation

"Pause" control and "Pause" behavior

At the beginning/end of pauses, enable/disable the pause function on the system; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules. The module then interprets the content of the PROFIenergy command and turns it off or on again. The ET 200AL interface module is the PE-Entity for the PROFIenergy-capable I/O modules of the ET 200AL distributed I/O system in this case.

Device information can be called up using additional PROFIenergy commands during the pauses. You can use these commands to transfer the "Start_Pause" / "End_Pause" command in good time.

NOTE
A complete PROFIenergy sequence consists of the commands "Start_Pause" and "End_Pause". Always observe this sequence during programming.

LED displays

PROFIenergy generally has no effect on the LED display. Exceptions can be found in the device manuals of the I/O modules.

Response to error detection

All channels whose pause mode is set to "PE_MODE_PROCEED" report errors as in productive operation.

The following rules apply to channels which switch to a pause mode other than "PE_MODE_PROCEED":

- All errors that are unrelated to the switch to "Pause" are reported.
- If error recognition is possible during "Pause", these errors continue to be reported.
- All error messages which are caused by the switch to "Pause" are suppressed.
- The following applies if error recognition is not possible during the "Pause":
  - The status of errors already pending before the "Pause" is retained.
  - Incoming and outgoing errors are reported once the "Pause" has been ended.

NOTE
Switching to "Pause" and out of "Pause" may cause an error to be reported.

Additional information

Additional information on diagnostics can be found in the I/O module device manuals.

Hardware interrupt

Ending a "Pause" causes hardware interrupts to be detected again.

"Pause" behavior under certain operating conditions

A "Pause" is ended in the following cases:

Table 2-39 Ending a "Pause"

Ending a "Pause"	Explanation
The supply voltage 1L+ of the interface module module has failed.	The "pause" is exited and can be re-activated by re-sending the PROFIenergy parameter assignment followed by the "Start_Pause" command.
• Stop controller[1] • Controller failure (connection interrupted)[1] • Firmware update • Reset to factory settings • Deactivating the IO device[1]	
The I/O module was pulled and plugged	
Station stop[1] • Removing an I/O module	The "pause" is exited , the PROFIenergy parameter assignment is still on the I/O module and the "pause" can be re-activated by the "Start_Pause" command.
The supply voltage 1L+ of the I/O module has failed	
The parameter settings of the I/O module were changed during operation using data record 128	

[1] The substitute value behavior was activated.

3.3.2.3 Parameter assignment

Parameter assignment

Keep the following points in mind when assigning parameters for PROFIenergy:

- Parameters for PROFIenergy are assigned with the parameter data record (version 2), index 3. The interface module distributes the PROFIenergy parameters to the I/O modules.
- The parameter assignment of an additional pause behavior is possible immediately after the start of the previous "Pause". The required state for the following pause is activated with a new "Start_Pause" command.
- You can write the parameter assignment as often as needed.
- The interface module checks the distribution of the parameters to the I/O modules and returns the result as a return value of the write job. In the case of a negative return value, there are one or more I/O modules that have not accepted the parameter data record. In this case, the I/O modules respond according to their last PROFIenergy parameter assignment in case of an incoming "Start_Pause" command. "Start_Pause"/"End_Pause" commands can be executed as planned with a positive return value.

- In case of a failure of an I/O module or station outage, you must repeat the parameter assignment using the parameter data record.
- The ET 200AL distributed I/O system supports configuration of the behavior of **a** "pause". If a different response is required for an additional "Pause", you will have to assign parameters again.

NOTE

Effect: The response (switch-off) of the I/O modules to PROFIenergy is related to the slot, which means all channels in the slot behave accordingly.

Parameter data record

You specify in the parameter data record for PROFIenergy which I/O modules (slots) are controlled with the PROFIenergy commands.

The following table shows the content of the parameter data record for PROFIenergy, index 3, which you create yourself and can transfer to the interface module.

Table 2-40 Parameter data record for PROFIenergy (version 2), index 3

Byte	Element		Code	Explanation
0	Version		02_D	Cannot be modified
1	Number of blocks		01_D to 34_D	Slots 1 to 34 depending on the configuration of the distributed I/O system ET 200AL
2	Block 1	Slot number	00_D	Not assigned
			01_D to 34_D	I/O module slot with PROFIenergy
3		Mode	0_D: PE_MODE_PROCEED, proceed at "Pause" 1_D: PE_MODE_SHUTDOWN, shut down at "Pause" [1] 3_D: PE_MODE_LAST_VALUE, last output or measured value is retained 4_D: PE_MODE_SUBST_VALUE, substitute value "0" [2]	
:	:	:	:	
64	Block 32	Slot number	See Block 1	
65		Mode		

1 The specific behavior depends on the used I/O module (with a digital input module, for example, the sensor supply is turned off or the outputs are without power supply and voltage supply with an analog output module)

2 An analog output module (e. g. with the output range 0 mA to 20 mA, ± 20 mA) or a digital output module issues the value "0".

Error messages

The following table shows which error messages the feedback data record returns, if necessary:

Table 2-41 Error messages

Error code	Meaning	
$80B1_H$	Impermissible length	Check the length of the data record
$80E0_H$	Error in header information	Check the data record header information
$80E1_H$	Parameter error • at least one I/O module does not support PROFIenergy • A parameter value has been incorrectly encoded	Check the content of the data record and correct the parameter assignment error before starting the "Pause". Parameter assignment errors which are not corrected can result in incorrect I/O module shutdown behavior.

3.3.2.4 PROFIenergy control data records

PROFIenergy control data records

The control data record for PROFIenergy, Index $80A0_H$, supports the following services for the IM 157-1 PN interface module:

Table 2-42 Control data records for PROFIenergy

Service	Service ID	Meaning
Start pause [1]	01_H	Assuming the configured Pause behavior, suppressing all associated diagnostics data
End Pause	02_H	Leaving the pause
Query Modes	03_H	Reads the supported modes • Request List Energy Saving Modes • Request Get Mode (Energy Saving Mode Data)
PEM status	04_H	Reading the PROFIenergy status
PE_Identify	05_H	Reading the supported PROFIenergy services

[1] The minimum (configurable) pause time for the ET 200AL distributed I/O system is 10 s.

3.3.3 Configuration control (option handling)

Properties

Configuration control allows you to prepare your distributed I/O system for future extensions or options. Configuration control means that you can configure the planned maximum configuration of your distributed I/O system in advance and vary it later in a flexible manner by means of the user program.

Reference

You can find more information on configuration control

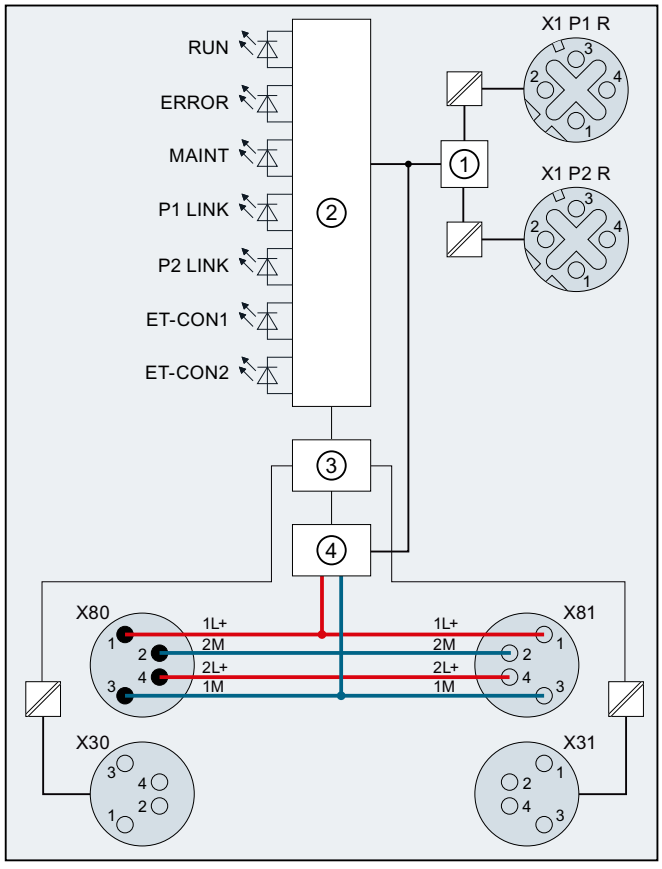
- In the system manual ET 200AL Distributed I/O System (https://support.industry.siemens.com/cs/ww/en/view/89254965)
- On the Internet under the following link: Application collection (https://support.industry.siemens.com/cs/ww/en/view/29430270).
- In the STEP 7 online help.

Wiring

4

4.1 Terminal and block diagram

The image below shows the terminal and block diagram of the IM 157-1 PN interface module.



①	Switch	1L+	Supply voltage 1L+ (non-switched)
②	Electronics	1M	Ground 1M (non-switched)
③	ET-Connection interface	2L+	Load voltage 2L+ (switched)
④	Internal supply voltage	2M	Ground 2M (switched)
X1 P1 R	1. PROFINET interface	RUN	LED operating state (green)
X1 P2 R	2. PROFINET interface	ERROR	LED diagnostics status (red)
X80	Infeed of supply voltages	MAINT	LED diagnostics status (yellow)
X81	Loop-through of supply voltages	P1 LINK, P2 LINK	PROFINET LEDs (green)
X30	Infeed of the ET-Connection	ET-CON1, ET-CON2	ET-Connection LEDs (green)
X31	Loop-through of the ET-Connection		

Figure 2-35 Terminal and block diagram

4.2 Pin assignment

NOTE

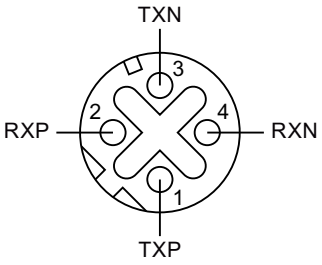
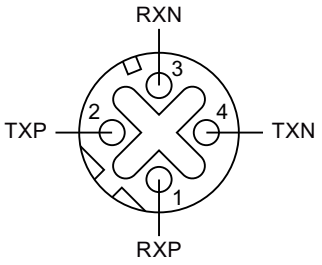
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for PROFINET

The following table shows the pin assignment of the two sockets for PROFINET.

Table 2-43 Pin assignment of the PROFINET sockets

Pin	Assignment		Front view of the sockets	
	X1 P1 R Socket	**X1 P2 R Socket**	**X1 P1 R**	**X1 P2 R**
1	TXP	RXP		
2	RXP	TXP		
3	TXN	RXN		
4	RXN	TXN		
Shield-ing	Functional earth FE			

NOTE

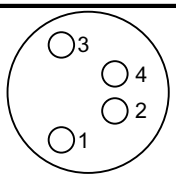
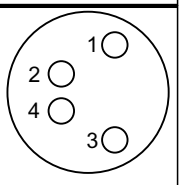
Pin assignments

If you disable "Autonegotiation" in STEP 7, you must pay attention to the different pin assignments of X1 P1 R and X1 P2 R.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

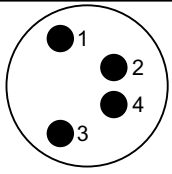
Table 2-44 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection1)	**X31 socket (ET-Connection2)**		**X30**	**X31**
1	RXP	RXP	Yellow		
2	TXP	TXP	White		
3	TXN	TXN	Blue		
4	RXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The following table shows the pin assignment for infeed of the supply voltage.

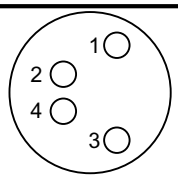
Table 2-45 Pin assignment of the supply voltage connector

Pin	Assignment X80 connector (power input)	Assignment of the wire color of the power line cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The following table shows the pin assignment for loop-through of the supply voltage.

Table 2-46 Pin assignment of the supply voltage socket

Pin	Assignment X81 Socket (power output)	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage

Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

⚠ CAUTION

PROFINET IO

Modules with PROFINET interfaces may only be operated under the following condition: All connected devices must be equipped with SELV/PELV power supplies.

Parameters

5

5.1 Parameters

The following table shows the parameters for the IM 157-1 PN interface module.

Table 2-47 Parameters (GSD file)

Parameters	Value range	Default	Efficiency range
Configuration control	• Disable • Enable	Disable	ET 200AL

5.2 Explanation of the parameters

Configuration control

You can use this parameter to enable the configuration control function in the ET 200AL distributed I/O system.

NOTE

If you configure the enable, the ET 200AL distributed I/O system requires a control data record 196 from the user program in order for the ET 200AL distributed I/O system to operate the I/O modules.

Reference

You will find more information in the section Configuration control (option handling) and in the STEP 7 online help.

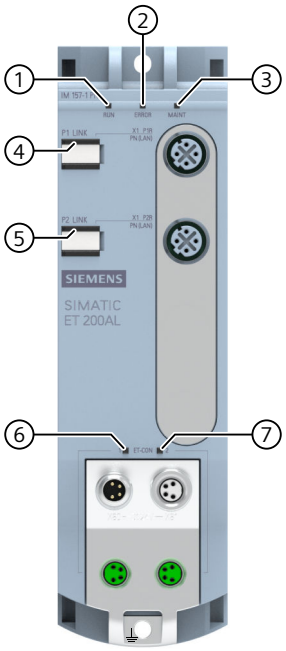
Interrupts, error messages, diagnostics and system alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the interface module IM 157-1 PN.



①	RUN	(green)
②	ERROR	(red)
③	MAINT	(yellow)
④	ET-CON1	(green)
⑤	ET-CON2	(green)
⑥	P2 LINK	(green)
⑦	P1 LINK	(green)

Figure 2-36 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 32).

LED RUN, LED ERROR, LED MAINT

Table 2-48 Status and error displays of the LEDs RUN, ERROR, MAINT

LEDs			Meaning	Solution
RUN	ERROR	MAINT		
Off	Off	Off	Missing or insufficient supply voltage on interface module.	Check the supply voltage or switch it on on the interface module.
On	On	On	Test of LEDs during startup: The three LEDs light up simultaneously for approximately 0.25 s.	---
Flashes	Off	Off	Interface module is deactivated.	Activate the interface module with the configuration software or the user program.
			Interface module is not configured.	Configure the interface module with the configuration software.
			ET 200AL starts up.	---
			ET 200AL is being assigned parameters.	
On	Not relevant	Not relevant	ET 200AL is currently exchanging data with the IO controller.	---
Not relevant	Flashes	Not relevant	Group error	Evaluate the diagnostics and eliminate the error.
			The preset configuration does not correspond to the actual configuration of the ET 200AL.	Check the configuration of the ET 200AL to see whether a module is missing, defective or if a module that is not configured is connected to ET-CON1 or ET-CON2 .
			Parameter assignment error in the I/O module	Evaluate the display of the module status in STEP 7 or in STEP 7 (TIA portal) and correct the errors in the I/O module.
Not relevant	Not relevant	On	Maintenance	See section Maintenance events (Page 33)
Flashes	Flashes	Flashes	The "Node flash test" is run (the LEDs P1 LINK and P2 LINK of the PROFINET interface also flash).	---
			Hardware or firmware defective (The LEDs P1 LINK and P2 LINK of the PROFINET interface do not flash).	Replace the interface module.
Flashes	Not relevant	Not relevant	Firmware is loading (all LEDs remain in their current state while the firmware update is being written)	---

LED P1 LINK, LED P2 LINK

Table 2-49 Status displays of the LEDs P1 LINK and P2 LINK

LEDs		Meaning	Solution
P1 LINK	P2 LINK		
☐ Off		There is no connection between the PROFINET interface of your PROFINET device and a communication partner (e.g., IO controller).	Check whether the bus cable to the switch or IO controller is disconnected.
■ On		There is no connection between the PROFINET interface of your PROFINET device and a communication partner (e.g., IO controller).	-
☼ Flashes		The "Node flash test" is run (the RUN, ERROR and MAINT LEDs also flash).	-

LED ET-CON1, LED ET-CON2

Table 2-50 Status displays of the LEDs ET-CON1 and ET-CON2

LEDs		Meaning	Solution
ET-CON1	ET-CON2		
☐ Off		There are no I/O modules available at the respective ET-Connection or the modules do not have supply voltage.	Check the wiring for the ET-Connection or the supply voltage for the I/O module.
■ On		A communications connection to at least one IO module at the corresponding ET-Connection is available.	-

6.2 Interrupts

6.2.1 Evaluating interrupts

Introduction

Interrupts are triggered by the IO device in case of errors. Interrupts are evaluated based on the I/O controller used.

Evaluating interrupts with I/O controllers

The ET 200AL distributed I/O system supports the following interrupts:

- Diagnostics interrupts
- Hardware interrupts
- Pull/plug module interrupt

In the event of an interrupt, interrupt OBs are automatically called in the CPU of the IO controller.

Information on the cause and class of the error is already available, based on the OB number and start information.

Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).

System diagnostics

In STEP 7 (TIA Portal), the updated system diagnostic is available for the modules of the S7-1500 automation system (IO controller CPU S7-1500) and ET 200AL (IO device). Independent of the cyclic user program, messages are made available on the display of the CPU S7-1500, the CPU web server and the HMI device.

You will find more information on systemic diagnostics in the Function Manual Diagnostics (http://support.automation.siemens.com/WW/view/en/59192926).

6.2.2 Trigger a diagnostics interrupt

For an incoming or outgoing event (for example, wire break on a channel of an I/O module), the interface module triggers a diagnostics interrupt if the parameters were assigned accordingly.

The CPU interrupts the processing of the user program and processes the diagnostics interrupt OB (OB 82). The event that triggered the interrupt is entered in the start information of the diagnostics interrupt OB.

6.2.3 Triggering a hardware interrupt

During a hardware interrupt, the CPU interrupts the processing of the user program and processes the hardware interrupt OB (e.g., OB 40). The event that triggered the interrupt is entered in the start information of the hardware interrupt OB.

NOTE

Diagnostics "Hardware interrupt lost" (from I/O module)

Avoid creating hardware interrupts cyclically.

If the hardware interrupt load is too high, hardware interrupts can get lost depending on the number of I/O modules and the communication load.

6.2.4 Triggering an insert/remove module interrupt

When an insert/remove module interrupt occurs, the CPU interrupts execution of the user program and processes the insert/remove module interrupt OB (OB 83). The event that triggered the interrupt is entered in the start information of the insert/remove OB.

The pull/plug OB (OB 83) is also triggered for all subsequent I/O modules, because the ET-Connection and/or the power supply is interrupted.

6.3 Alarms

6.3.1 Diagnostics alarms

Actions after a diagnostics alarm

There can be more than one diagnostic alarm at a given time. Actions initiated by diagnostics alarms:

- The ERROR LED of the interface module flashes.
- Diagnostic data is reported as diagnostics interrupts to the CPU of the IO controller and can be read via data records.
- Incoming diagnostics alarms are saved to the diagnostics buffer of the I/O controller.
- OB 82 is called. If OB 82 is not available, the I/O controller goes into STOP mode.

You can find more information on this topic in the STEP 7 online help.

Reading out the diagnostics data

Table 2-51 Reading the diagnostics with STEP 7

Automation system with IO controller	Application	See...
SIMATIC S7	Diagnostics as plain text in STEP 7 in online and diagnostics view	STEP 7 online help • STEP 7 V13 and higher Function Manual PROFINET with STEP 7 V13 (http://support.automation.siemens.com/WW/view/en/49948856) • STEP 7 V5.5 and higher System Manual PROFINET System Description (http://support.automation.siemens.com/WW/view/en/19292127)
	"RDREC" instruction (SFB 52) Reading data records from the IO device	
	"RALRM" instruction (SFB 54) Receiving alarms from the IO device	

Additional information on the data records for PROFINET IO

The structure of the diagnostics data records and programming examples can be found in the Programming Manual From PROFIBUS DP to PROFINET IO (http://support.automation.siemens.com/WW/view/en/19289930) and in the Application example (http://support.automation.siemens.com/WW/view/en/24000238).

Causes of error and troubleshooting

Causes of errors and corrective measures of diagnostics alarms are described in the device manuals of the I/O modules (http://support.automation.siemens.com/WW/view/en/89013554) in the section Interrupt, Error and System Messages.

6.3.2 Maintenance events

Triggering of a maintenance event

The PROFINET IO interfaces of the interface module support the diagnostics concept and maintenance concept in PROFINET IO according to standard IEC 61158-6-10. The goal is the early recognition and correction of potential disruptions.

For the interface module, maintenance events signal to the user when a network component must be checked or replaced.

The CPU interrupts user program execution and processes the diagnostic block OB 82. The event that triggered the maintenance event is entered in the start information of the OB 82.

The interface module signals a maintenance event to the higher-level diagnostics system in the case of the following event:

Table 2-52 Triggering of a maintenance event

Maintenance alarm	Event	Alarm/Meaning
Maintenance demanded LED MAINT is lit.	Synchronization loss	• No synchronization frame received. No synchronization message frame was received by the sync master within the timeout period after parameter assignment or during operation. • Successive synchronization frames are located outside permitted limits (jitter).

System alarms in STEP 7 (TIA Portal)

The maintenance information is generated in STEP 7 (TIA Portal) V12 SP1 and higher with the following system alarms:

- Maintenance demanded - indicated for each port by a yellow wrench icon in the device view or in the hardware configuration.

You can find more information on this topic in the STEP 7 online help.

6.3.3 Channel diagnostics

Function

Channel-related diagnostics provides information about channel faults in modules.

Channel faults are mapped as channel diagnostics data in IO diagnostics data records.

The data record is read with the "RDREC" instruction (SFB 52).

Structure of the diagnostics data records

The data records supported by the ET 200AL distributed I/O system are based on the PROFINET IO standard - Application Layer Service definition V2.2.

You can download the standard on the Internet (http://www.profibus.com) from home page of the PROFIBUS user organization free of charge.

Structure of the manufacturer-specific diagnostics data records

The structure of the diagnostics data records is differentiated by the BlockVersion. The following BlockVersion applies to the IM 157-1 PN interface modules:

Table 2-53 Structure of the manufacturer-specific diagnostics data records

IM 157-1 PN interface module	BlockVersion
6ES7157-1AB00-0AB0	W#16#0101

6.3.4 Invalid configuration states of ET 200AL on the PROFINET IO

Invalid configuration states

If the number of modules exceeds the maximum configuration limit, the extra modules are ignored by the system. No data exchange takes place.

6.3.5 STOP of the IO controller and recovery of the IO device

STOP of the SIMATIC IO controller

If diagnostics from the IO device are received by the IO controller in the STOP state, these diagnostics do not result in a start of the organization blocks after startup of the IO controller. You must read the data record $E00C_H$ in OB 100 with the "RDREC" instruction.

Return of the SIMATIC IO device

If you want to read out the diagnostics of a station after the station return, you must read the data record $E00C_H$ in OB 86 with the "RDREC" instruction.

Technical specifications

7

Technical specifications of the interface module IM 157-1 PN

The following table lists the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7157-1AB00-0AB0/td?dl=en).

Article number	6ES7157-1AB00-0AB0
General information	
Product type designation	IM 157-1 PN
HW functional status	FS02
Firmware version	V1.0.x
Vendor identification (VendorID)	002AH
Product function	
• I&M data	Yes; I&M0 to I&M4
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	From V5.5 SP4 Hotfix 3
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Configuration control	
via dataset	Yes
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Input current	
Current consumption (rated value)	100 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Power loss	
Power loss, typ.	2.9 W
Address area	
Address space per station	
• Address space per station, max.	1 430 byte
Interfaces	
Number of PROFINET interfaces	1
1. Interface	
Interface type	PROFINET

Article number	6ES7157-1AB00-0AB0
Interface types	
• M12 port	Yes; 2x M12 D-coded
• integrated switch	Yes
Protocols	
• PROFINET IO Device	Yes
• Open IE communication	Yes
Interface types	
M12 port	
• Transmission procedure	PROFINET with 100 Mbit/s full duplex (100BASE-TX)
• 10 Mbps	Yes; for Ethernet services
• 100 Mbps	Yes; PROFINET with 100 Mbit/s full duplex (100BASE-TX)
• Autonegotiation	Yes
• Autocrossing	Yes
Protocols	
Supports protocol for PROFINET IO	Yes
PROFIsafe	No
PROFIBUS	No
EtherNet/IP	No
PROFINET IO Device	
Services	
– IRT	Yes; 250 µs, 500 µs, 1 ms, 2 ms, 4 ms, 8 ms, 16 ms, 32 ms, 64 ms, 128 ms
– PROFIenergy	Yes
– Shared device	Yes
– Number of IO Controllers with shared device, max.	4
Redundancy mode	
Media redundancy	
– MRP	Yes
– MRPD	Yes
Open IE communication	
• TCP/IP	Yes
• SNMP	Yes
• LLDP	Yes
Interrupts/diagnostics/status information	
Diagnostics function	Yes
Alarms	
• Diagnostic alarm	Yes
Diagnostics indication LED	
• RUN LED	Yes; green LED
• ERROR LED	Yes; red LED
• MAINT LED	Yes; Yellow LED
• Connection display LINK TX/RX	Yes; 2x green LED

Article number	6ES7157-1AB00-0AB0
Potential separation	
between the load voltages	Yes
between PROFINET and all other circuits	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; from FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
Ambient conditions	
Ambient temperature during operation	
• min.	-25 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	263 g

Dimension drawing

A

The figure below shows the dimension drawing of the IM 157-1 PN interface module in the front and side view.

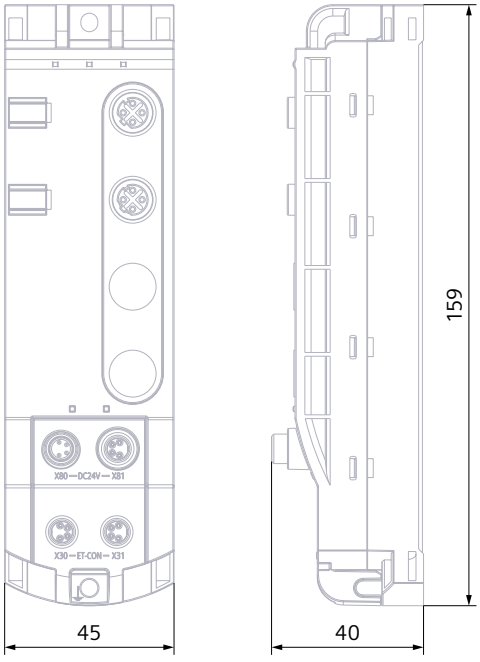
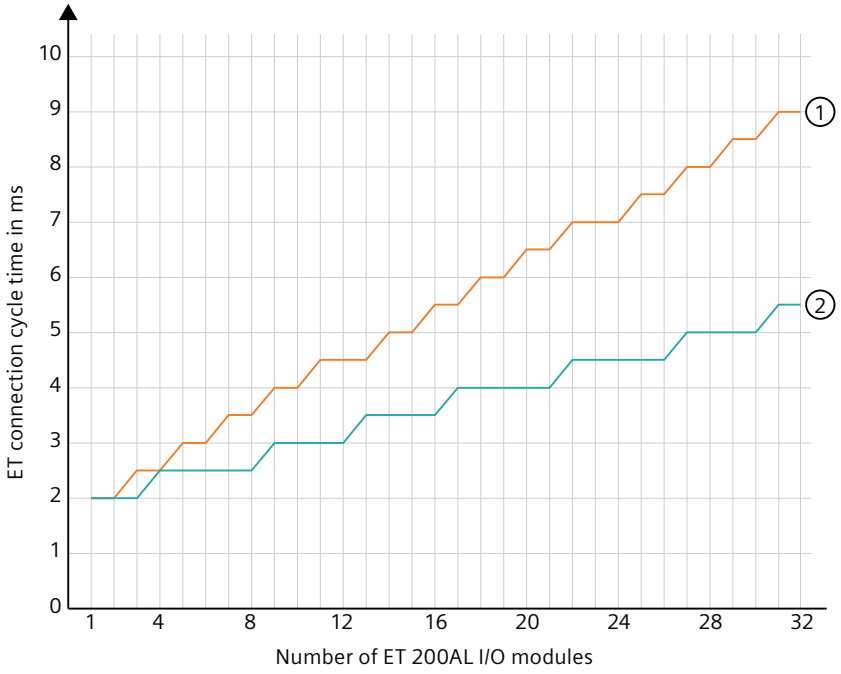


Figure 2-37 Dimension drawing

Cycle times

The figure below shows the cycle times at ET-Connection based on the number of I/O modules with a PN send clock of 0.5 ms.



① Cycle time for modules with firmware < V2.0.0

② Cycle time for modules with firmware ≥ V2.0.0

Figure 2-38 Cycle times

The cycle time at ET-Connection is synchronized with the PROFINET send clock. The input data of the I/O modules is transmitted via the ET-Connection via PROFINET without any further delay (waiting time in the interface module). The output data is also transmitted via PROFINET to the I/O modules without any further delay via the ET-Connection. The cycle time of the ET-Connection is always a multiple of the set PROFINET send clock and depends on the number of I/O modules.

The chart above shows the trend for a send clock of 0.5 ms. With larger send clocks, the gradation of the trend changes according to the send clock.

If there are modules with a firmware version < V2.0.0 and modules with a firmware version ≥ V2.0.0 present in the ET-Connection, then the cycle time is between trends ① and ②.

When using a larger number of IO-Link masters with a large I/O data configuration (> 32 bytes), there may be a slight increase in the cycle time at the ET connection.

SIEMENS

SIMATIC

ET 200AL
DI 8x24VDC 4xM12
(6ES7141-5AF00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostic alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

10/2024
A5E36680963-AC

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 14
4.2 Pin assignment 15

5 Parameters/address space 17

5.1 Parameters 17
5.2 Explanation of the parameters 17
5.3 Address space 17

6 Interrupts/diagnostic alarms 19

6.1 Status and error displays 19
6.2 Interrupts 20
6.3 Diagnostics alarms 21

7 Technical specifications 22

7.1 Technical specifications 22

8 PROFIenergy 25

8.1 Pause function 25
8.2 Behavior of the digital input module 26

A Dimension drawing 27

B Parameter data record 28

B.1 Structure of data record 128 for the module parameter assignment 28

B.2 Error transferring the data record 29

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7141-5AF00-0BA0

View of the module

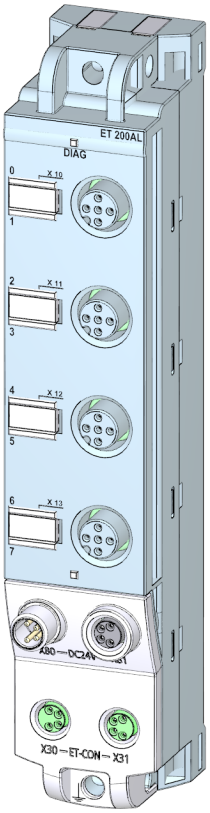


Figure 2-39 View of the DI 8x24VDC 4xM12 digital input module

Properties

The module has the following technical properties:

- 8 digital inputs
- M12 sockets for connection of sensors
- 24 V DC supply voltage
- Configurable diagnostics can be set for each module
- Typical input delay of 3 ms
- Suitable for switches and proximity switches
- Dimensions 30 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

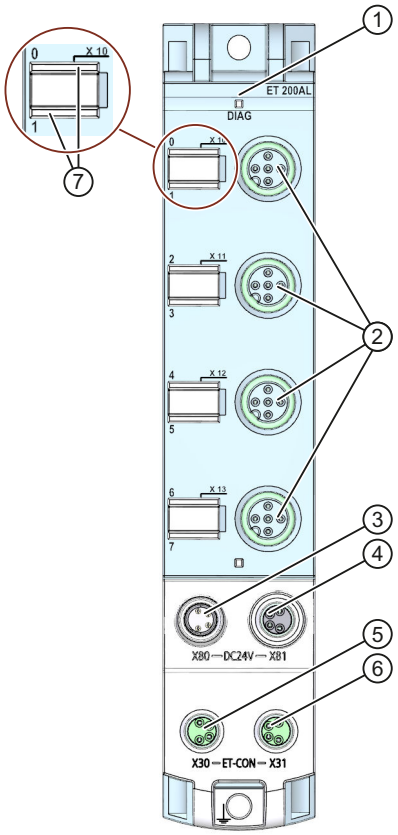
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DI 8x24VDC 4xM12 digital input module.



① DIAG: LED display for the diagnostic status
② X10 to X13: Sockets for the input signal
③ X80: Connector for infeed of the supply voltage (POWER input)
④ X81: Socket for loop-through of the supply voltage (POWER output)
⑤ X30: Socket for ET-Connection IN
⑥ X31: Socket for ET-Connection OUT
⑦ LED displays 0 to 7 for the channel status

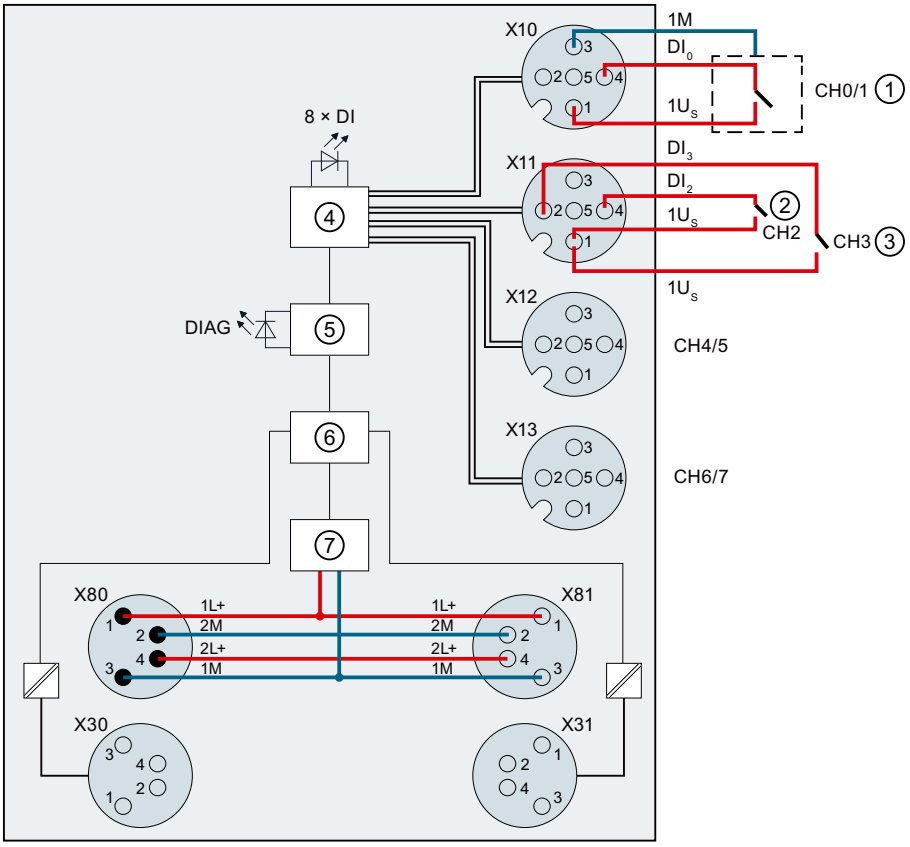
Figure 2-40 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The figure below shows an example of the pin assignment of signal inputs with 2-wire and 3-wire connection.



①	3-wire connection	X30	Infeed of the ET-Connection
②	2-wire connection	X31	Loop-through of the ET-Connection
③	2-wire connection	1L+	Supply voltage 1L+ (non-switched)
④	DI circuit	1M	Ground 1M (non-switched)
⑤	Microcontroller	2L+	Load voltage 2L+ (switched)
⑥	ET-Connection interface	2M	Ground 2M (switched)
⑦	Internal supply voltage	$1U_S$	24 V encoder supply
X10 to X13	Channels 0 to 7	DI_n	Input signal
X80	Infeed of supply voltages	DI	Channel status LEDs (0 to 7) (green)
X81	Loop-through of supply voltages	DIAG	LED diagnostic status (red/green)

Figure 2-41 Terminal and block diagram

4.2 Pin assignment

NOTE

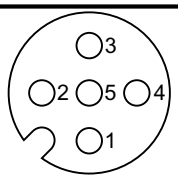
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital inputs

The table below shows the pin assignment of the 4 sockets for the connection of digital inputs.

Table 2-54 Pin assignment for digital inputs

Pin	Assignment	Front view of the sockets
	X10 to X13 sockets for digital inputs	
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)	
2	Input signal DI_1: Connector X10 Input signal DI_3: Connector X11 Input signal DI_5: Connector X12 Input signal DI_7: Connector X13	
3	Encoder supply ground 1M	
4	Input signal DI_0: Connector X10 Input signal DI_2: Connector X11 Input signal DI_4: Connector X12 Input signal DI_6: Connector X13	
5	Functional earth FE	

NOTICE

24 V encoder supply $1U_S$

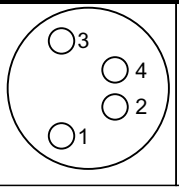
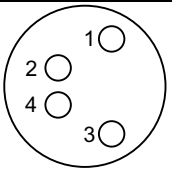
Use only the 24 V encoder supply $1U_S$ provided by the digital input module to supply power to the encoder.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

Table 2-55 Pin assignment for ET-Connection

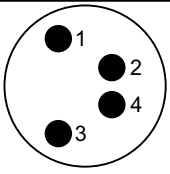
Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

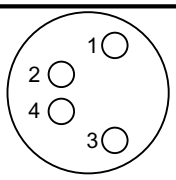
Table 2-56 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-57 Pin assignment of the supply voltage socket

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the socket
	X81 socket (POWER output)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The table below shows the parameters for the DI 8x24VDC 4xM12 digital input module.

Table 2-58 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module

5.2 Explanation of the parameters

Diagnostics: Short-circuit to ground

Enabling of the diagnostics if a short-circuit of the encoder supply to ground occurs.

5.3 Address space

The table below shows the assignment of the address space for the digital input module DI 8x24VDC 4xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-59 Address space for the digital input module DI 8x24VDC 4xM12 with value status

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image inputs (PII)									
IB x									Input values on channels 0 ... 7
IB x +1									Value status (QI) for inputs on channels 0 ... 7*

* 0 = Value read in at channel is incorrect

Configuration options of the DI 8x24VDC 4xM12 digital input module

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

One additional byte is occupied in the input address space if you enable the value status for the digital input module. Bits 0 to 7 in this byte are assigned to a channel and return information about the validity of the digital input value.

Bit = 1: No error on channel.

Bit = 0: Error on channel.

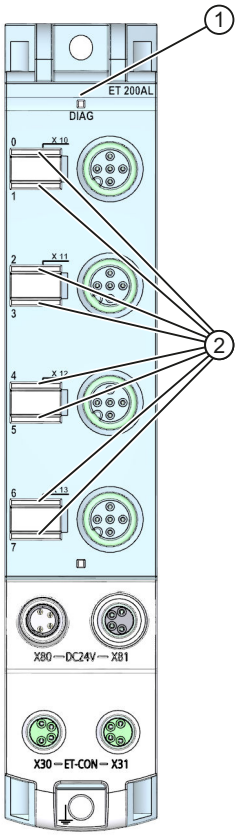
Interrupts/diagnostic alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DI 8x24VDC 4xM12 digital input module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 7) (green)

Figure 2-42 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in section Diagnostics alarms (Page 21).

DIAG LED

Table 2-60 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
On	Module parameters assigned and no module diagnostics
Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-61 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

6.2 Interrupts

The DI 8x24VDC 4xM12 digital input module supports diagnostic interrupts.

Diagnostic interrupt

The digital input module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-62 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit	1_H	Short-circuit encoder supply to ground	Eliminate the short-circuit
Security event: Firmware has been successfully downloaded and activated for installation.[1]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[1]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 A diagnostics alarm is output for a signed firmware update.

Technical specifications

7

7.1 Technical specifications

Technical specifications of the DI 8x24VDC 4xM12 digital input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7141-5AF00-0BA0/td?dl=en).

Article number	6ES7141-5AF00-0BA0
General information	
Product type designation	DI 8x24VDC
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 Hotfix 7 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	25 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	4
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders
Power loss	
Power loss, typ.	1.9 W

Article number	**6ES7141-5AF00-0BA0**
Digital inputs	
Number of digital inputs	8
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	8
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-30 to +5 V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3.2 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Sensor supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67

Article number	6ES7141-5AF00-0BA0
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. The majority of the energy is saved by the process itself; the PROFINET device itself only contributes a few watts of saving potential. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input module is explained in the following section.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 Behavior of the digital input module

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-63 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] As there is only one encoder supply U_S for all channels, the supply can only be switched off at "pause" if no channel is configured in PE_MODE_PROCEED.

Dimension drawing

A

The figure below shows the dimension drawing of the DI 8x24VDC 4xM12 digital input module in front and side view.

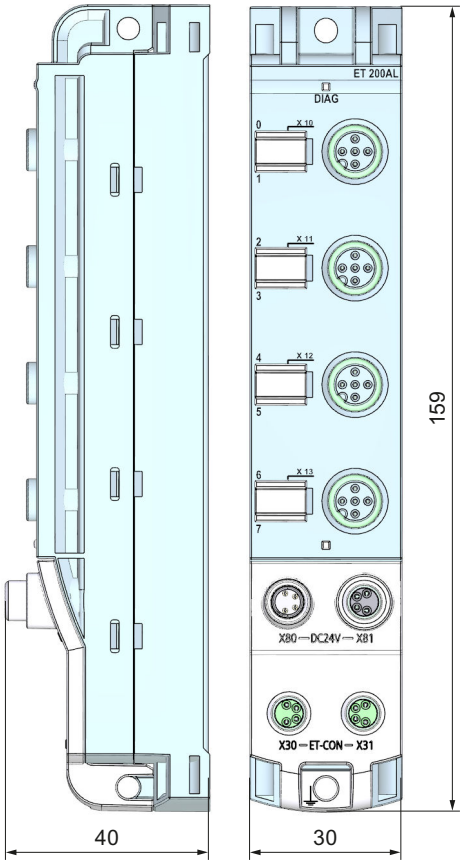


Figure 2-43 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 1_D ($0000\ 0001_B$)							

[1] Reserved bits must be set to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	**Parameter**							
2	Reserved[1]					Diagnostics: Short-circuit to ground 0_B: Disable 1_B: Enable	Reserved[1]	

[1] Reserved bits must be set to 0

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 21) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-64 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
DI 8x24VDC 8xM8
(6ES7141-5BF00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostics alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

10/2024
A5E32349579-AE

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 14
4.2 Pin assignment 15

5 Parameters/address space 17

5.1 Parameters 17
5.2 Explanation of the parameters 17
5.3 Address space 17

6 Interrupts/diagnostics alarms 19

6.1 Status and error displays 19
6.2 Interrupts 20
6.3 Diagnostics alarms 21

7 Technical specifications 22

8 PROFIenergy 25

8.1 Pause function 25
8.2 Behavior of the digital input module 26

A Dimension drawing 27

B Parameter data record 28

B.1 Structure of data record 128 for the module parameter assignment 28

B.2 Error transferring the data record 29

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7141-5BF00-0BA0

View of the module

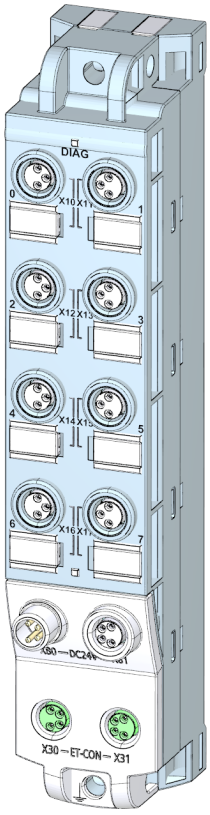


Figure 2-44 View of the DI 8x24VDC 8xM8 digital input module

Properties

The module has the following technical properties:

- 8 digital inputs
- M8 sockets for connection of sensors
- 24 V DC supply voltage
- Configurable diagnostics can be set for each module
- Typical input delay of 3 ms
- Suitable for switches and proximity switches
- Dimensions 30 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

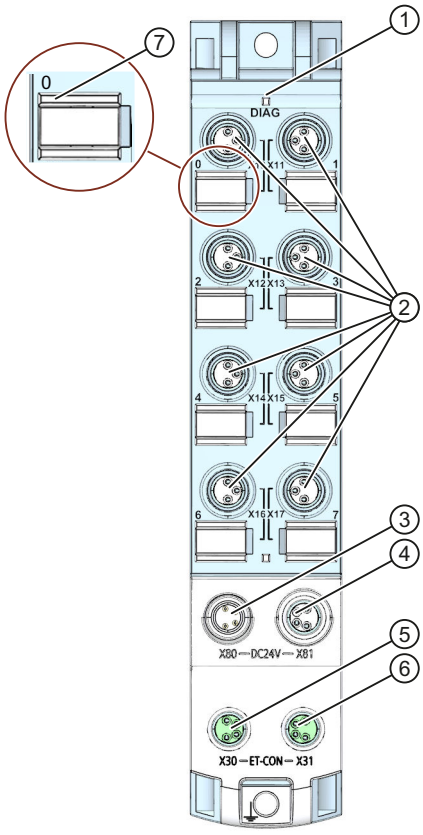
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The following figure shows the operator controls and display elements of the DI 8x24VDC 8xM8 digital input module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input signal
③ X80: Connector for infeed of the supply voltage (POWER input)
④ X81: Socket for loop-through of the supply voltage (POWER output)
⑤ X30: Socket for ET-Connection IN
⑥ X31: Socket for ET-Connection OUT
⑦ LED displays 0 to 7 for the channel status

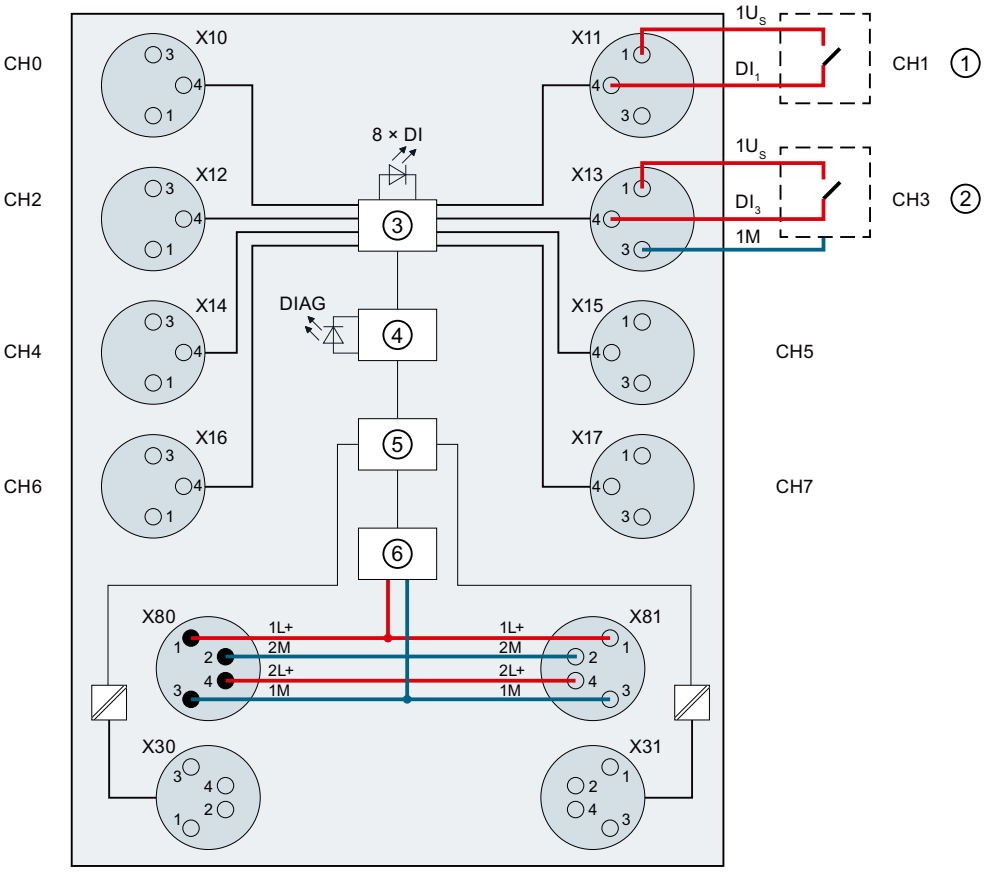
Figure 2-45 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The following figure shows an example of the pin assignment of signal outputs with 2- and 3-wire connection.



①	2-wire connection	X30	Infeed of the ET-Connection
②	3-wire connection	X31	Loop-through of the ET-Connection
③	DI circuit	1L+	Supply voltage 1L+ (non-switched)
④	Microcontroller	1M	Ground 1M (non-switched)
⑤	ET-Connection interface	2L+	Load voltage 2L+ (switched)
⑥	Internal supply voltage	2M	Ground 2M (switched)
X10 to X17	Channels 0 to 7	1U$_S$	24 V encoder supply
X80	Infeed of supply voltages	DI$_n$	Input signal
X81	Loop-through of supply voltages	DI	Channel status LEDs (0 to 7) (green)
		DIAG	LED diagnostic status (red/green)

Figure 2-46 Terminal and block diagram

4.2 Pin assignment

NOTE

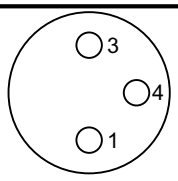
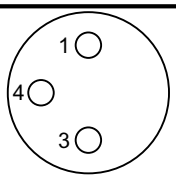
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital inputs

The table below shows the pin assignment of the 8 sockets for the connection of digital inputs.

Table 2-65 Pin assignment for digital inputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 sockets for digital inputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
3	Encoder supply ground 1M		
4	Input signal DI_0: Connector X10 Input signal DI_1: Connector X11 Input signal DI_2: Connector X12 Input signal DI_3: Connector X13 Input signal DI_4: Connector X14 Input signal DI_5: Connector X15 Input signal DI_6: Connector X16 Input signal DI_7: Connector X17		

NOTICE

24 V encoder supply $1U_S$

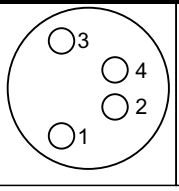
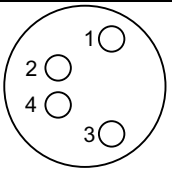
Use only the 24 V encoder supply $1U_S$ provided by the digital input module to supply power to the encoder.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

Table 2-66 Pin assignment for ET-Connection

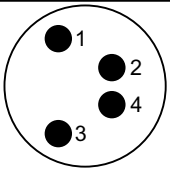
Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	**X31 socket (ET-Connection OUT)**		**X30**	**X31**
1	TXP	RXP	Yellow		
2	RXP	TXP	White		

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

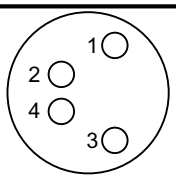
Table 2-67 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-68 Pin assignment of the supply voltage socket

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the socket
	X81 socket (POWER output)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The following table shows the parameters for the DI 8x24VDC 8xM8 digital input module.

Table 2-69 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module

5.2 Explanation of the parameters

Diagnostics: Short-circuit to ground

Enabling of the diagnostics if a short-circuit of the encoder supply to ground occurs.

5.3 Address space

The table below shows the assignment of the address space for the digital input module DI 8x24VDC 8xM8 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-70 Address space for the digital input module DI 8x24VDC 8xM8 with value status

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image inputs (PII)									
IB x									Input values on channels 0 ... 7
IB x +1									Value status (QI) for inputs on channels 0 ... 7*

* 0 = Value read in at channel is incorrect

Configuration options of the DI 8x24VDC 8xM8 digital input module

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

One additional byte is occupied in the input address space if you enable the value status for the digital input module. Bits 0 to 7 in this byte are assigned to a channel and provide information on the validity of the digital input value.

Bit = 1: No error on channel.

Bit = 0: Error on channel.

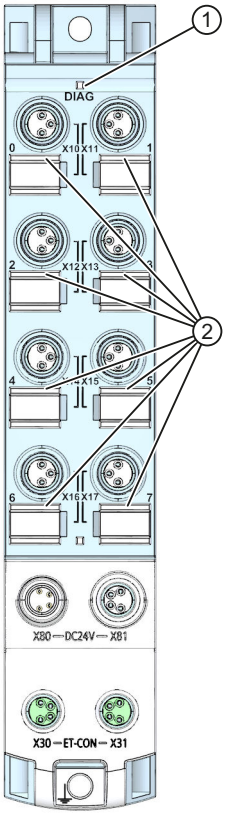
Interrupts/diagnostics alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DI 8x24VDC 8xM8 digital input module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 7) (green)

Figure 2-47 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 21).

DIAG LED

Table 2-71 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
On	Module parameters assigned and no module diagnostics
Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-72 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

6.2 Interrupts

The DI 8x24VDC 8xM8 digital input module supports diagnostic interrupts.

Diagnostic interrupt

The digital input module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-73 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit	1_H	Short-circuit encoder supply to ground	Eliminate the short-circuit
Security event: Firmware has been successfully downloaded and activated for installation.[1]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[1]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 A diagnostics alarm is output for a signed firmware update.

Technical specifications

7

Technical specifications of the DI 8x24VDC 8xM8 digital input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7141-5BF00-0BA0/td?dl=en).

Article number	6ES7141-5BF00-0BA0
General information	
Product type designation	DI 8x24VDC
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	From V5.5 SP4 Hotfix 3
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	25 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	8
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders
Power loss	
Power loss, typ.	1.9 W
Digital inputs	
Number of digital inputs	8
Input characteristic curve in accordance with IEC 61131, type 3	Yes

Article number	6ES7141-5BF00-0BA0
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	8
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-30 to +5 V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3.2 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Sensor supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01

Article number	6ES7141-5BF00-0BA0
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M8, 3-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input module is explained in the following section.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (http://support.automation.siemens.com/WW/view/en/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 Behavior of the digital input module

Requirement

You can use the PROFIenergy function when you use the internal encoder supply.

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-74 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] As there is only one encoder supply U_S for all channels, the supply can only be switched off at "pause" if no channel is configured in PE_MODE_PROCEED.

Dimension drawing

A

The figure below shows the dimension drawing of the DI 8x24VDC 8xM8 digital input module in front and side view.

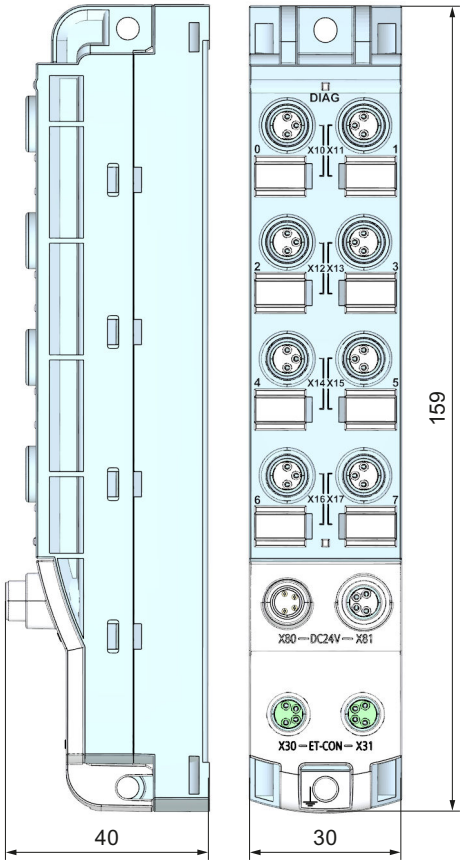


Figure 2-48 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 1_D ($0000\ 0001_B$)							

[1] Reserved bits must be set to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	Parameter							
2	Reserved[1]					Diagnostics: Short-circuit to ground 0_B: Disable 1_B: Enable	Reserved[1]	

1 Reserved bits must be set to 0

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 21) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-75 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
DI 16x24VDC 8xM12
(6ES7141-5AH00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostic alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

10/2024
A5E36681813-AC

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 14
4.2 Pin assignment 15

5 Parameters/address space 18

5.1 Parameters 18
5.2 Explanation of the parameters 18
5.3 Address space 18

6 Interrupts/diagnostic alarms 20

6.1 Status and error displays 20
6.2 Interrupts 21
6.3 Diagnostics alarms 22

7 Technical specifications 23

7.1 Technical specifications 23

8 PROFIenergy 26

8.1 Pause function 26
8.2 Behavior of the digital input module 27

A Dimension drawing 28

B Parameter data record 29

B.1 Structure of data record 128 for the module parameter assignment 29

B.2 Error transferring the data record 30

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7141-5AH00-0BA0

View of the module

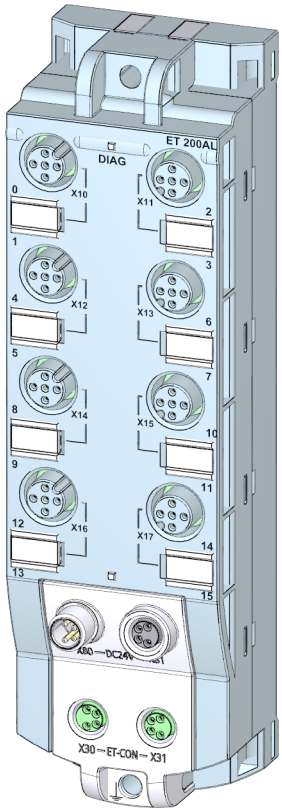


Figure 2-49 View of the DI 16x24VDC 8xM12 digital input module

Properties

The module has the following technical properties:

- 16 digital inputs
- M12 sockets for connection of sensors
- 24 V DC supply voltage
- Configurable diagnostics can be set for each module
- Typical input delay of 3 ms
- Suitable for switches and proximity switches
- Dimensions 45 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

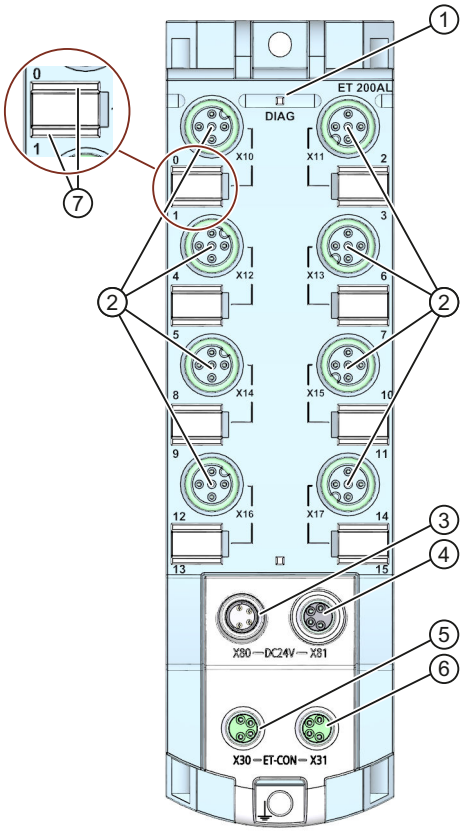
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DI 16x24VDC 8xM12 digital input module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input signal
③ X80: Connector for infeed of the supply voltage (POWER input)
④ X81: Socket for loop-through of the supply voltage (POWER output)
⑤ X30: Socket for ET-Connection IN
⑥ X31: Socket for ET-Connection OUT
⑦ LED displays 0 to 15 for the channel status

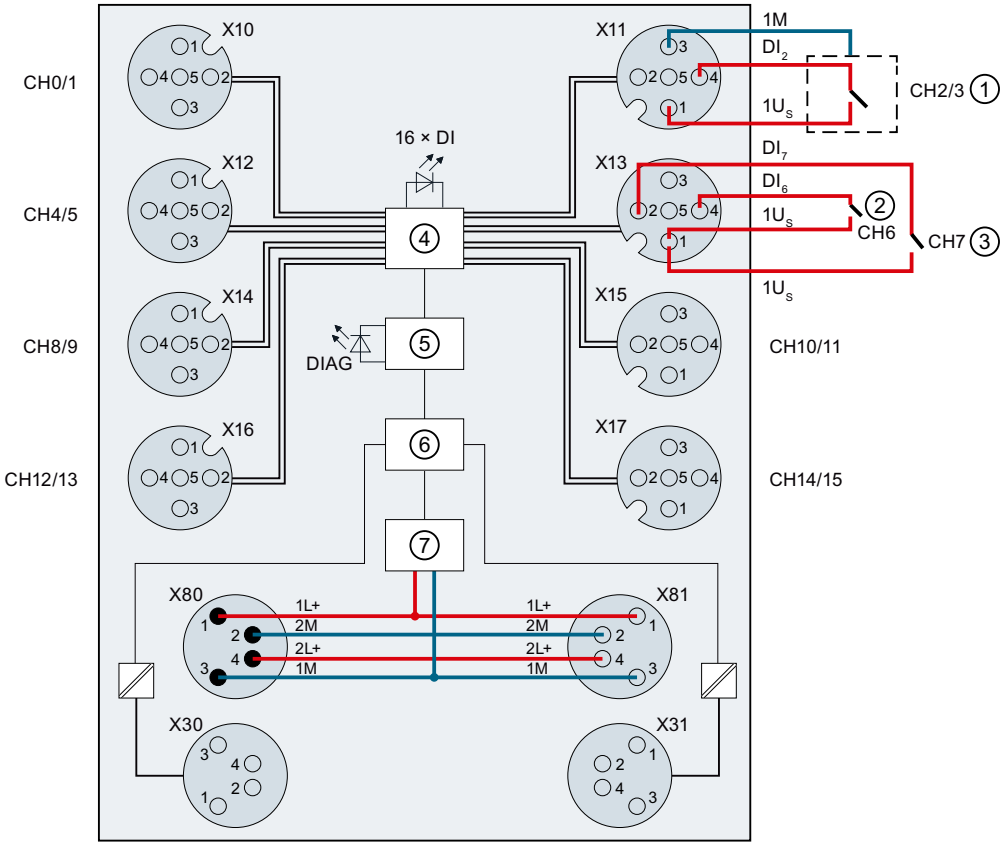
Figure 2-50 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The figure below shows an example of the pin assignment of signal inputs with 2-wire and 3-wire connection.



①	3-wire connection	X30	Infeed of the ET-Connection
②	2-wire connection	X31	Loop-through of the ET-Connection
③	2-wire connection	1L+	Supply voltage 1L+ (non-switched)
④	DI circuit	1M	Ground 1M (non-switched)
⑤	Microcontroller	2L+	Load voltage 2L+ (switched)
⑥	ET-Connection interface	2M	Ground 2M (switched)
⑦	Internal supply voltage	$1U_S$	24 V encoder supply
X10 to X17	Channels 0 to 7	DI_n	Input signal
X80	Infeed of supply voltages	DI	Channel status LEDs (0 to 15) (green)
X81	Loop-through of supply voltages	DIAG	LED diagnostic status (red/green)

Figure 2-51 Terminal and block diagram

4.2 Pin assignment

NOTE

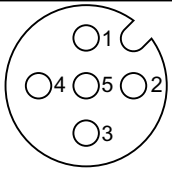
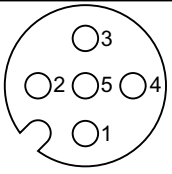
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital inputs

The table below shows the pin assignment of the 8 sockets for the connection of digital inputs.

Table 2-76 Pin assignment for digital inputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 sockets for digital inputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Input signal DI_1: Connector X10 Input signal DI_3: Connector X11 Input signal DI_5: Connector X12 Input signal DI_7: Connector X13 Input signal DI_9: Connector X14 Input signal DI_{11}: Connector X15 Input signal DI_{13}: Connector X16 Input signal DI_{15}: Connector X17		
3	Encoder supply ground 1M		
4	Input signal DI_0: Connector X10 Input signal DI_2: Connector X11 Input signal DI_4: Connector X12 Input signal DI_6: Connector X13 Input signal DI_8: Connector X14 Input signal DI_{10}: Connector X15 Input signal DI_{12}: Connector X16 Input signal DI_{14}: Connector X17		
5	Functional earth FE		

NOTICE

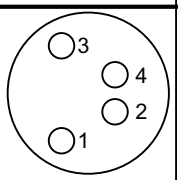
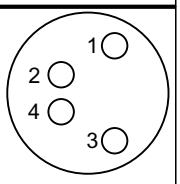
24 V encoder supply $1U_S$

Use only the 24 V encoder supply $1U_S$ provided by the digital input module to supply power to the encoder.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

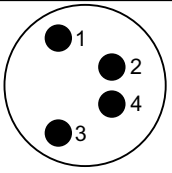
Table 2-77 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

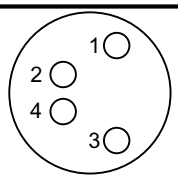
Table 2-78 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-79 Pin assignment of the supply voltage socket

Pin	Assignment **X81 socket (POWER output)**	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The table below shows the parameters for the DI 16x24VDC 8xM12 digital input module.

Table 2-80 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module

5.2 Explanation of the parameters

Diagnostics: Short-circuit to ground

Enabling of the diagnostics if a short-circuit of the encoder supply to ground occurs.

5.3 Address space

The table below shows the assignment of the address space for the digital input module DI 16x24VDC 8xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-81 Address space for the digital input module DI 16x24VDC 8xM12 with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image inputs (PII)									
IB x									Input values on channels 0 ... 7
IB x +1									Input values on channels 8 ... 15
IB x +2									Value status (QI) for inputs on channels 0 ... 7*
IB x +3									Value status (QI) for inputs on channels 8 ... 15*

* 0 = Value read in at channel is incorrect

Configuration options of the DI 16x24VDC 8xM12 digital input module

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

An additional 2 bytes are occupied in the input address space if you enable the value status for the digital input module. Bits 0 to 7 in these bytes are assigned to a channel and return information about the validity of the digital input value.

Bit = 1: No error on channel.

Bit = 0: Error on channel.

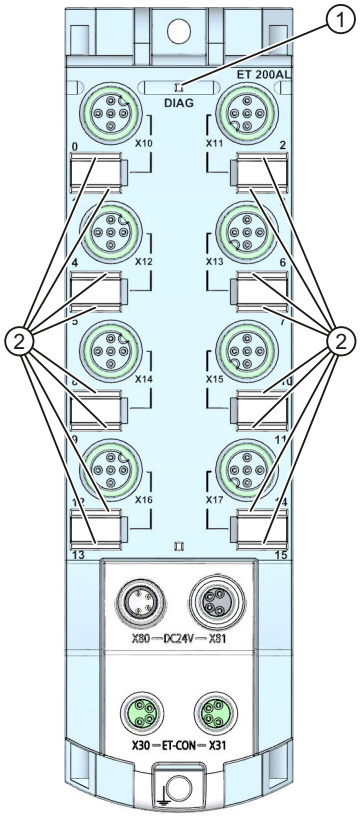
Interrupts/diagnostic alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DI 16x24VDC 8xM12 digital input module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 15) (green)

Figure 2-52 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in section Diagnostics alarms (Page 22).

DIAG LED

Table 2-82 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
On	Module parameters assigned and no module diagnostics
Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-83 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

6.2 Interrupts

The DI 16x24VDC 8xM12 digital input module supports diagnostic interrupts.

Diagnostic interrupt

The digital input module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-84 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit	1_H	Short-circuit encoder supply to ground	Eliminate the short-circuit
Security event: Firmware has been successfully downloaded and activated for installation.[1]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[1]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

[1] A diagnostics alarm is output for a signed firmware update.

Technical specifications

7

7.1 Technical specifications

Technical specifications of the DI 16x24VDC 8xM12 digital input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7141-5AH00-0BA0/td?dl=en).

Article number	6ES7141-5AH00-0BA0
General information	
Product type designation	DI 16x24VDC
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 Hotfix 7 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	30 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	8
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	1.4 A; Total current of all encoders
Power loss	
Power loss, typ.	2.7 W

Article number	6ES7141-5AH00-0BA0
Digital inputs	
Number of digital inputs	16
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	16
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-30 to +5 V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3.2 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Sensor supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67

Article number	**6ES7141-5AH00-0BA0**
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	184 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input module is explained in the following section.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 Behavior of the digital input module

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-85 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] As there is only one encoder supply U_S for all channels, the supply can only be switched off at "pause" if no channel is configured in PE_MODE_PROCEED.

Dimension drawing

A

The figure below shows the dimension drawing of the DI 16x24VDC 8xM12 digital input module in front and side view.

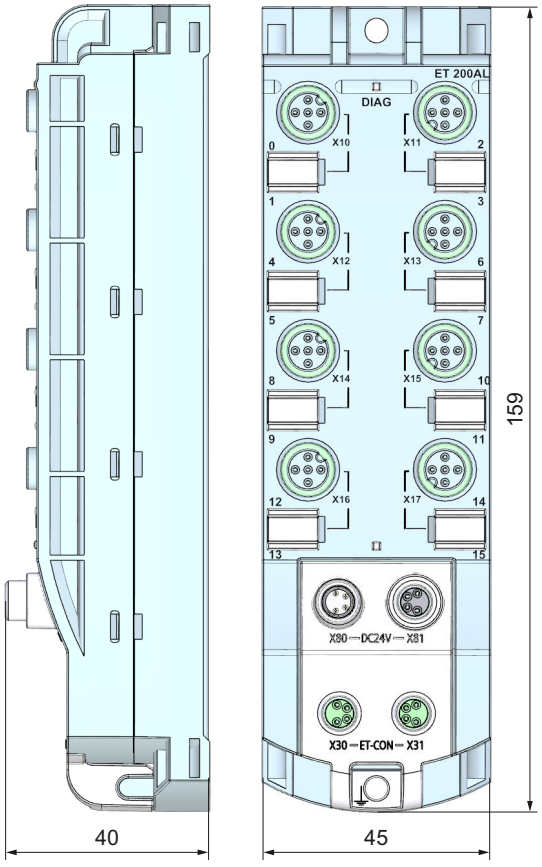


Figure 2-53 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 1_D ($0000\ 0001_B$)							

[1] Reserved bits must be set to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	**Parameter**							
2	Reserved[1]					Diagnostics: Short-circuit to ground 0_B: Disable 1_B: Enable	Reserved[1]	

1 Reserved bits must be set to 0

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 22) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-86 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
Digital output module DQ 8x24VDC/2A 8xM12 (6ES7142-5AF00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostic alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

10/2024
A5E36683723-AC

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 14
4.2 Pin assignment 15

5 Parameters/address space 17

5.1 Parameters 17
5.2 Explanation of the parameters 17
5.3 Address space 18

6 Interrupts/diagnostic alarms 19

6.1 Status and error displays 19
6.2 Interrupts 20
6.3 Diagnostics alarms 21

7 Technical specifications 22

7.1 Technical specifications 22

8 PROFIenergy 25

8.1 Pause function 25
8.2 Behavior of the digital output module 26

A Dimension drawing 27

B Parameter data record 28

B.1 Structure of data record 128 for the module parameter assignment 28

B.2 Error transferring the data record 29

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7142-5AF00-0BA0

View of the module

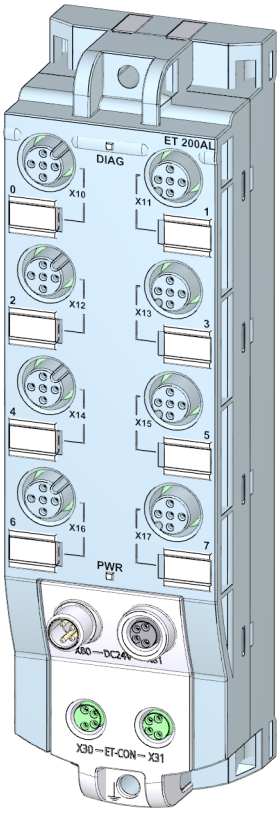


Figure 2-54 View of the DQ 8x24VDC/2A 8xM12 digital output module

Properties

The module has the following technical properties:

- 8 digital outputs
  - Channels 0 to 3 connected to 1L+ (non-switched)
  - Channels 4 to 7 connected to 2L+ (switched)
- M12 sockets for connection of actuators
- Rated load voltage 24 V DC
- Suitable for solenoid valves, DC contactors, and indicator lights
- Output current per output 2 A
- Configurable diagnostics can be set for each module
- Dimensions 45 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

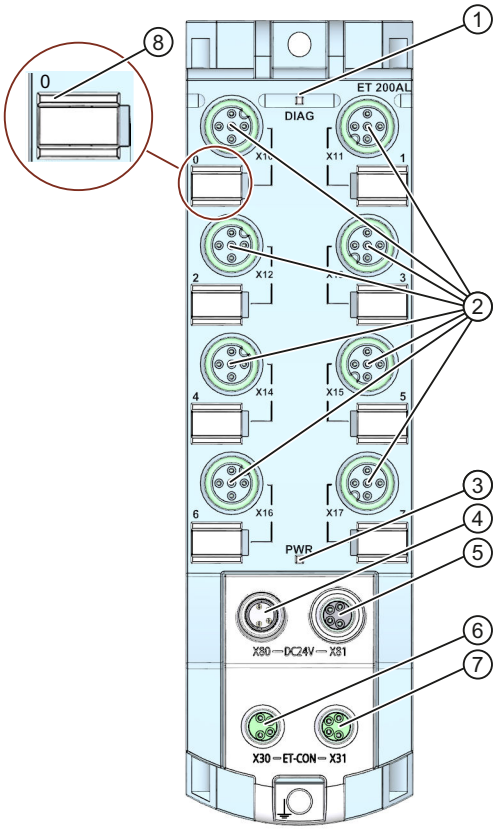
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DQ 8x24VDC/2A 8xM12 digital output module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the output signal
③ PWR: LED display for load voltage 2L+
④ X80: Connector for infeed of the supply voltage (POWER input)
⑤ X81: Socket for loop-through of the supply voltage (POWER output)
⑥ X30: Socket for ET-Connection IN
⑦ X31: Socket for ET-Connection OUT
⑧ LED displays 0 to 7 for the channel status

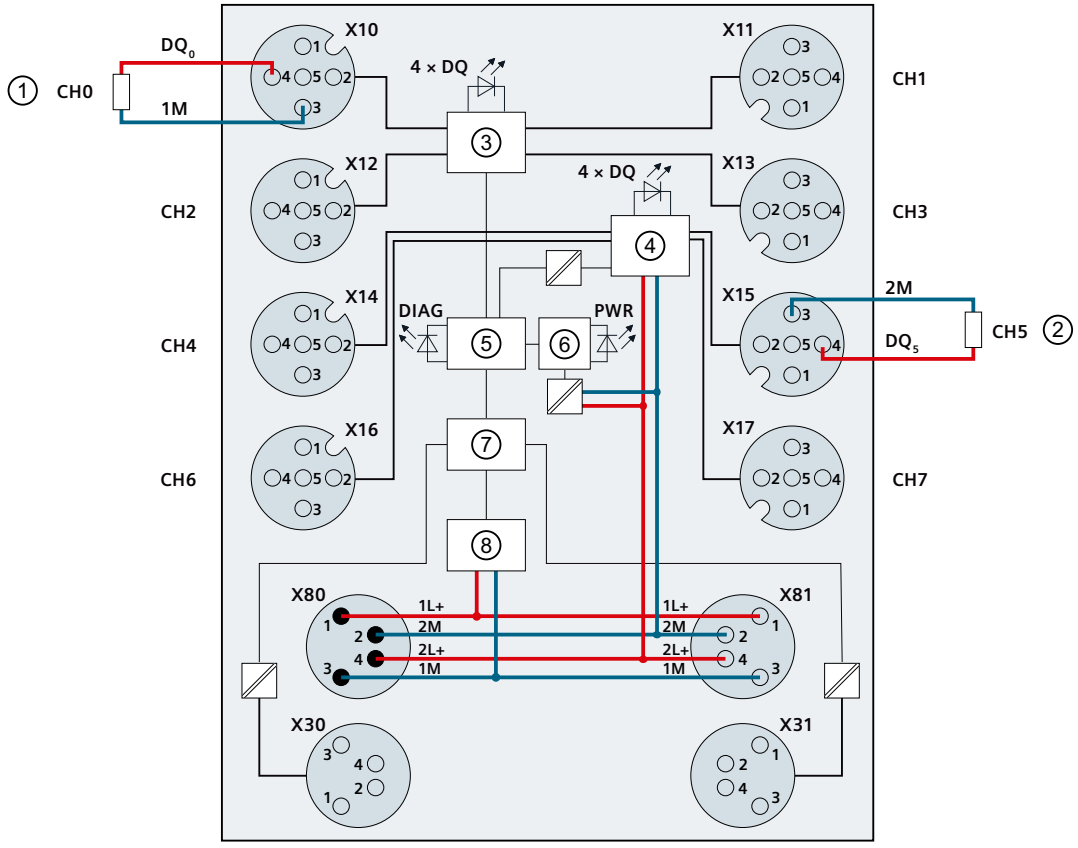
Figure 2-55 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The example in the figure below shows the pin assignment of signal outputs.



①	Output to 1L+	X10 to X17	Channels 0 to 7
②	Output to 2L+	X30	Infeed of the ET-Connection
③	DQ circuit 1L+	X31	Loop-through of the ET-Connection
④	DQ circuit 2L+	1L+	Supply voltage 1L+ (non-switched)
⑤	Microcontroller	1M	Ground 1M (non-switched)
⑥	Monitoring	2L+	Load voltage 2L+ (switched)
⑦	ET-Connection interface	2M	Ground 2M (switched)
⑧	Internal supply voltage	$1U_S$	24 V encoder supply
X80	Infeed of supply voltages	DQ_n	Output signal
X81	Loop-through of supply voltages	DQ	Channel status LEDs (0 to 7) (green)

Figure 2-56 Terminal and block diagram

4.2 Pin assignment

NOTE

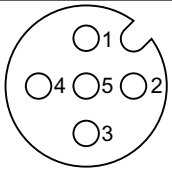
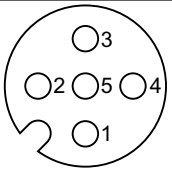
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital outputs

The tables below show the pin assignments of the 8 sockets for connection of the digital outputs.

Table 2-87 Pin assignment for digital outputs

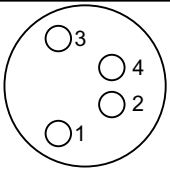
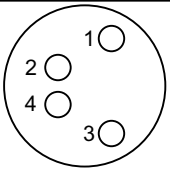
Pin	Assignment	Front view of the sockets	
	X10 to X17 sockets for digital outputs	X10, X12, X14, X16	X11, X13, X15, X17
1	Unassigned		
2	Unassigned		
3	X10 - X13: Ground 1M X14 - X17: Ground 2M		
4 *	Output signal DQ_0: Connector X10 Output signal DQ_1: Connector X11 Output signal DQ_2: Connector X12 Output signal DQ_3: Connector X13 Output signal DQ_4: Connector X14 Output signal DQ_5: Connector X15 Output signal DQ_6: Connector X16 Output signal DQ_7: Connector X17		
5	Functional earth FE		

* The outputs DQ_0 to DQ_3 are connected to 1L+; the outputs DQ_4 to DQ_7 are connected to 2L+.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

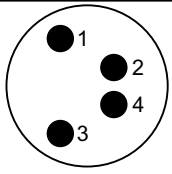
Table 2-88 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

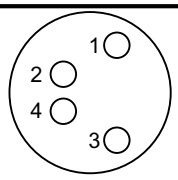
Table 2-89 Pin assignment of the supply voltage connector

Pin	Assignment **X80 connector (POWER input)**	Assignment of the wire color of the power line cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-90 Pin assignment of the supply voltage socket

Pin	Assignment **X81 socket (POWER output)**	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage

Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The table below shows the parameters for the DQ 8x24VDC/2A 8xM12 digital output module.

Table 2-91 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of the output to ground)
Reaction to CPU/master STOP	• Shut down • Keep last value • Output substitute value	Shut down	Module
Substitute value channel 0 ... 7	• 0 • 1	0	Channel

5.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics for short-circuit of the output to ground.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the digital outputs of the module after a CPU/master STOP:

- Shut down: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel 0 ... 7

With this parameter, you set substitute values for the digital outputs.

5.3 Address space

The tables below shows the assignment of the address space for the digital output module DQ 8x24VDC/2A 8xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-92 Address space for the digital output module DQ 8x24VDC/2A 8xM12 with value status

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Value status (QI) for outputs on channels 0 ... 7*
Assignment in the process image output (PIQ)									
QB x									Output values on channels 0 ... 7

* 0 = Value read in at channel is incorrect

Configuration options of the digital output module DQ 8x24VDC/2A 8xM12

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

One additional byte is occupied in the input address space if you enable the value status for the digital output module. The value status of the outputs is assigned to bits 0 to 7 in input byte x. This additional information provides information regarding the validity of the digital values or channel status.

Bit = 1: No error on channel.

Bit = 0: Error on channel.
This means:

- Short-circuit of output to ground or
- Parameter error or
- For channels 4 ... 7: Missing load voltage 2L+

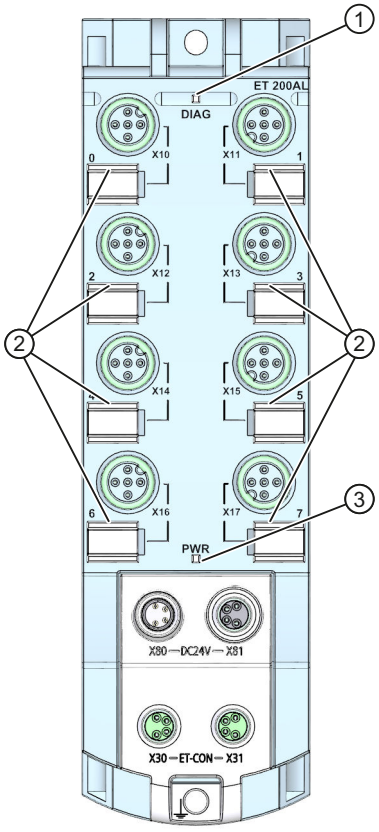
Interrupts/diagnostic alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital output module DQ 8x24VDC/2A 8xM12.



①	Diagnostic status (DIAG)	(red/green)
②	Channel status (0 to 7)	(green)
③	Load voltage 2L+ (PWR)	(green)

Figure 2-57 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic alarms can be found in the section Diagnostics alarms (Page 21).

DIAG LED

Table 2-93 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
On	Module parameters assigned and no module diagnostics
Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-94 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

PWR LED

Table 2-95 Status display of the PWR LED

PWR LED	Meaning
Off	Load voltage 2L+ is missing or too low
On	Load voltage 2L+ present

6.2 Interrupts

The digital output module DQ 8x24VDC/2A 8xM12 supports diagnostics interrupts.

Diagnostic interrupt

The digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of outputs to ground
- Load voltage 2L+ missing or too low

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital output module. You can read out the diagnostics alarms, for example, from the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-96 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit	1_H	Short-circuit of outputs to ground	• Eliminate the short-circuit
Load voltage 2L+ missing[1]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Security event: Firmware has been successfully downloaded and activated for installation.[2]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[2]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostics alarm "Load voltage missing" is displayed.

2 A diagnostics alarm is output for a signed firmware update.

Technical specifications

7

7.1 Technical specifications

Technical specifications of the DQ 8x24VDC/2A 8xM12 digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7142-5AF00-0BA0/td?dl=en).

Article number	6ES7142-5AF00-0BA0
General information	
Product type designation	DQ 8x24VDC/2A
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 Hotfix 7 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction; load increasing
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction; load increasing
Input current	
Current consumption (rated value)	40 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Power loss	
Power loss, typ.	4 W

Article number	**6ES7142-5AF00-0BA0**
Digital outputs	
Number of digital outputs	8
• in groups of	4; 2 load groups for 4 outputs each
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	2.8 A
Limitation of inductive shutdown voltage to	2L+ (-47 V)
Switching capacity of the outputs	
• on lamp load, max.	10 W
Load resistance range	
• lower limit	12 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	2 A
• for signal "1" permissible range, max.	2 A; with inductive load to IEC 60947-5-1, DC-13 / AC-15
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.1 Hz; 0.25 Hz at 25 °C
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per group, max.	4 A; For inductive load max. 2 channels per group
Cable length	
• unshielded, max.	30 m
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Outputs to ground; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels, in groups of	4
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No; 4 channels are non-isolated and 4 channels are isolated from supply voltage 1L+
Isolation	
Isolation tested with	707 V DC (type test)

Article number	**6ES7142-5AF00-0BA0**
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	192 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital output module is explained in the following sections.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 Behavior of the digital output module

Display

The channel status LEDs are directly affected by the signal level at the socket.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-97 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

Dimension drawing

The figure below shows the dimension drawing of the DQ 8x24VDC/2A 8xM12 digital output module in front and side views.

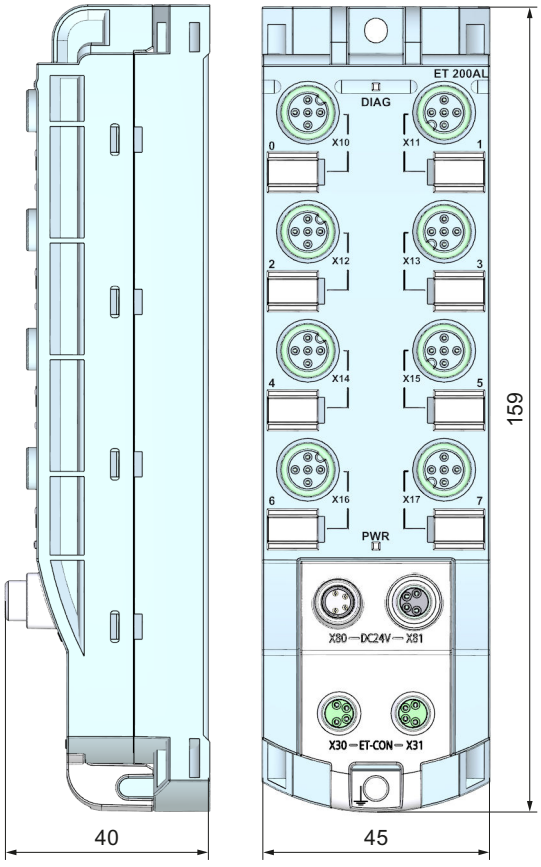


Figure 2-58 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 3_D ($0000\ 0011_B$)							
2...4	**Parameter**							
2	Reserved[1]					Diagnostics: Short-circuit to ground	Diagnostics: Missing load voltage 2L+	Reserved[1]

[1] Reserved bits must be set to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	Reserved[1]					0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	Reserved[1]
3	Reserved[1]		Response at CPU/master STOP[1] 00_B: Shut down 10_B: Keep last value 11_B: Output substitute value		Reserved[1]			
4	Substitute value channel 7 0_B: 0 1_B: 1	Substitute value channel 6 0_B: 0 1_B: 1	Substitute value channel 5 0_B: 0 1_B: 1	Substitute value channel 4 0_B: 0 1_B: 1	Substitute value channel 3 0_B: 0 1_B: 1	Substitute value channel 2 0_B: 0 1_B: 1	Substitute value channel 1 0_B: 0 1_B: 1	Substitute value channel 0 0_B: 0 1_B: 1

[1] Reserved bits must be set to 0

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 21) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-98 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
Digital input/digital output module DIQ 4+DQ 4x24VDC/0.5A 4xM12 (6ES7143-5AF00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostic alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

10/2024
A5E36683613-AC

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 15
4.2 Pin assignment 16

5 Parameters/address space 19

5.1 Parameters 19
5.2 Explanation of the parameters 19
5.3 Address space 20

6 Interrupts/diagnostic alarms 22

6.1 Status and error displays 22
6.2 Interrupts 24
6.3 Diagnostics alarms 24

7 Technical specifications 25

7.1 Technical specifications 25

8 PROFIenergy 29

8.1 Pause function 29
8.2 DI operating mode 30
8.3 DQ operating mode 31

A Dimension drawing 32

B Parameter data record 33

B.1 Structure of data record 128 for the module parameter assignment 33

B.2 Error transferring the data record 34

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7143-5AF00-0BA0

View of the module

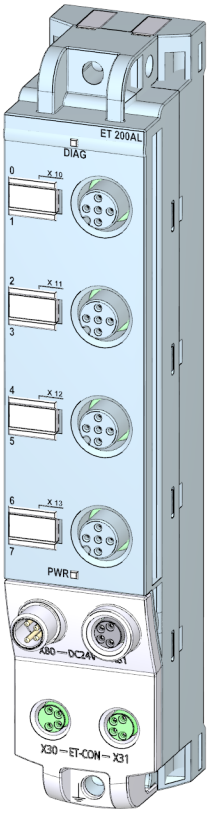


Figure 2-59 View of the DIQ 4+DQ 4x24VDC/0.5A 4xM12 digital input/digital output module

Properties

The module has the following technical properties:

- 4 digital inputs or digital outputs and 4 digital outputs, depending on parameter assignment
  - DIQ signals connected to 1L+ (non-switched)
  - DQ signals connected to 2L+ (switched)
- M12 sockets for connection of sensors and actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Configurable diagnostics can be set for each module
  - Typical input delay of 3 ms
  - Suitable for switches and proximity switches
- Digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current per output 0.5 A
  - Configurable diagnostics can be set for each module
- Dimensions 30 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

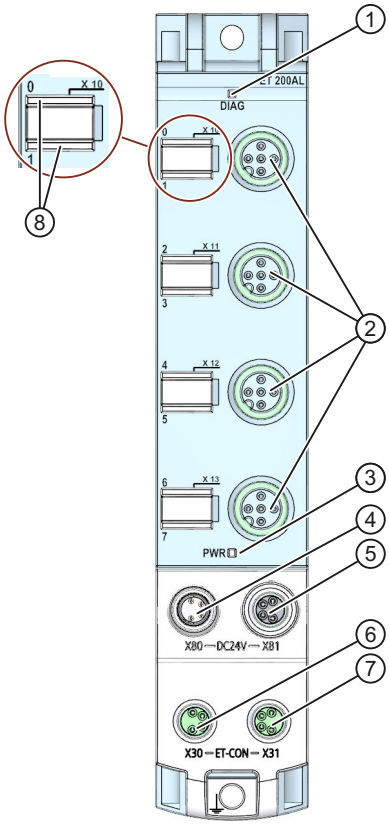
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DIQ 4+DQ 4x24VDC/0.5A 4xM12 digital input/digital output module.



① DIAG: LED display for the diagnostic status
② X10 to X13: Sockets for the input/output signal
③ PWR: LED display for load voltage 2L+
④ X80: Connector for infeed of the supply voltage (POWER input)
⑤ X81: Socket for loop-through of the supply voltage (POWER output)
⑥ X30: Socket for ET-Connection IN
⑦ X31: Socket for ET-Connection OUT
⑧ LED displays 0 to 7 for the channel status

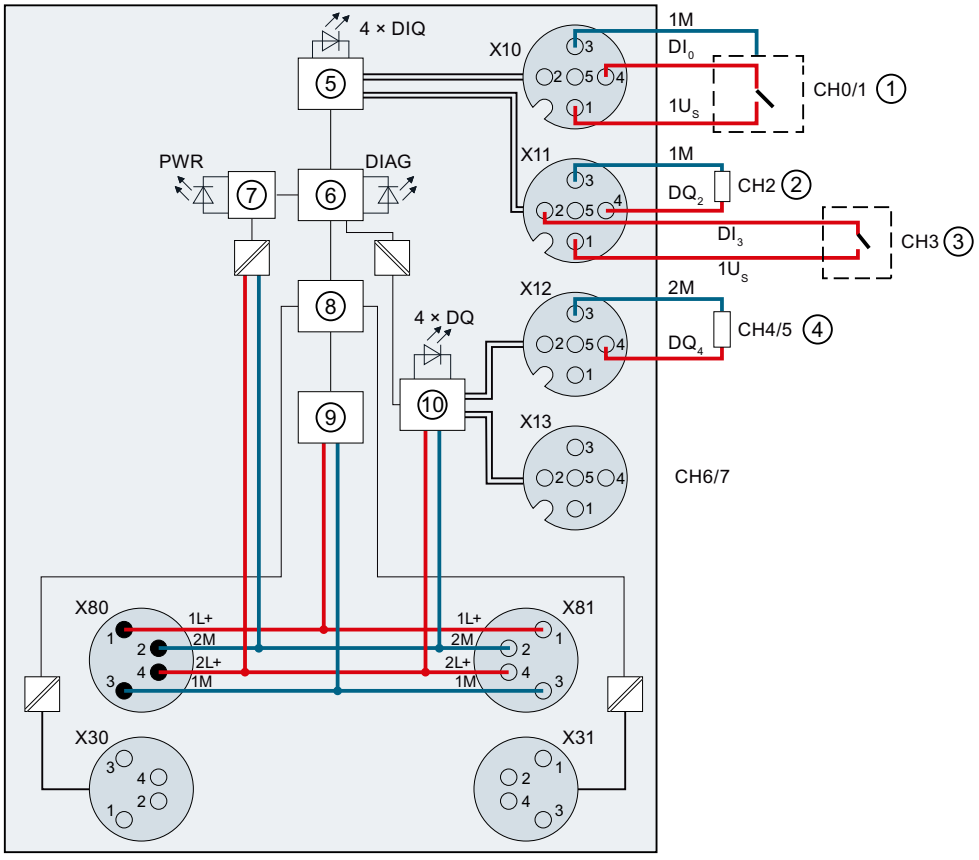
Figure 2-60 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The figure below shows an example of the pin assignment of signal inputs with 2-wire and 3-wire connection as well as signal outputs.



①	Configured as input: 3-wire connection	X30	Infeed of the ET-Connection
②	Configured as output	X31	Loop-through of the ET-Connection
③	Configured as input: 2-wire connection	1L+	Supply voltage 1L+ (non-switched)
④	Output	1M	Ground 1M (non-switched)
⑤	DI/DQ circuit	2L+	Load voltage 2L+ (switched)
⑥	Microcontroller	2M	Ground 2M (switched)
⑦	Monitoring	$1U_S$	24 V encoder supply
⑧	ET-Connection interface	DIQ_n	Input/output signal
⑨	Internal supply voltage	DQ_n	Output signal
⑩	DQ circuit	DIQ	LEDs channel status (0, 1, 2 and 3) (green)
X10 to X13	Channels 0 to 7	DQ	LEDs channel status (4, 5, 6 and 7) (green)
X80	Infeed of supply voltages	DIAG	LED diagnostic status (red/green)
X81	Loop-through of supply voltages	PWR	LED supply voltage 2L+ (green)

Figure 2-61 Terminal and block diagram

4.2 Pin assignment

NOTE

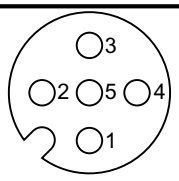
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital inputs/digital outputs

The tables below show the pin assignments of the 4 sockets for connection of the digital inputs/digital outputs.

Table 2-99 Pin assignment for digital inputs/digital outputs

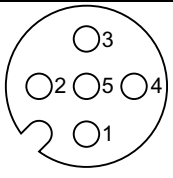
Pin	Assignment	Front view of the sockets
	X10 and X11 - sockets for digital inputs/digital outputs	**X10, X11**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)	
2	Input/output signal DIQ_1: Connector X10 Input/output signal DIQ_3: Connector X11	
3	Encoder supply ground 1M	
4	Input/output signal DIQ_0: Connector X10 Input/output signal DIQ_2: Connector X11	
5	Functional earth FE	

NOTICE

24 V encoder supply $1U_S$

Use only the 24 V encoder supply $1U_S$ provided by the digital input/digital output module to supply power to the encoder.

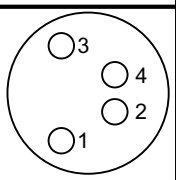
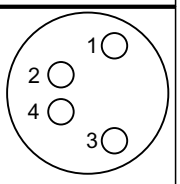
Table 2-100 Pin assignment for digital outputs

Pin	Assignment	Front view of the sockets
	X12 and X13 sockets for digital outputs	**X12, X13**
1	Unassigned	
2	Output signal DQ_5: Connector X12 Output signal DQ_7: Connector X13	
3	Ground 2M	
4	Output signal DQ_4: Connector X12 Output signal DQ_6: Connector X13	
5	Functional earth FE	

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

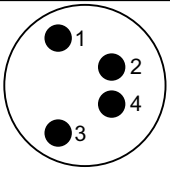
Table 2-101 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

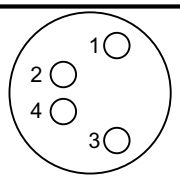
Table 2-102 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-103 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The table below shows the parameters for the DIQ 4+DQ 4x24VDC/0.5A 4xM12 digital input/digital output module.

Table 2-104 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of encoder supply or of the output to ground)
Freely assignable channel 0 ... 3	• DI • DQ	DI	Channel
Reaction to CPU/master STOP	• Shut down • Keep last value • Output substitute value	Shut down	Module (digital outputs)
Substitute value channel 0 ... 7	• 0 • 1	0	Channel (digital outputs)

5.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics for short-circuit of the encoder supply or output to ground.

Freely assignable channel n

With this parameter, you set whether the channel is to be operated as an input or output.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the digital outputs of the digital input/ digital output module after a CPU/master STOP:

- Shut down: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel 0 ... 7

With this parameter, you set substitute values for the digital outputs.

5.3 Address space

The table below shows the assignment of the address space for the digital input/output module DIQ 4+DQ 4x24VDC/0.5A 4xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-105 Address space for the digital input/output module DIQ 4+DQ 4x24VDC/0.5A 4xM12 with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x	0	0	0	0					Input values on channels 0 ... 3
IB x +1	0	0	0	0					Value status (QI) for inputs on channels 0 ... 3*
IB x +2									Value status (QI) for outputs on channels 0 ... 7*
Assignment in the process image output (PIQ)									
QB x									Output values on channels 0 ... 7

* 0 = Value read in at channel is incorrect

NOTE

Parameter assignment of the channels

Parameters for the first four channels can be freely assigned.

For the channels 0 ... 3 that are configured as input, the corresponding values in the output data do not trigger any reaction.

For the channels 0 ... 3 that are configured as output, the input value in the process image is 0.

Configuration options of the digital input/digital output module DIQ 4+DQ 4x24VDC/0.5A 4xM12

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

An additional 2 bytes are occupied in the input address space if you enable the value status for the digital input/digital output module. The value status of the inputs is assigned to bits 0 to 3 in input byte x + 1. The value status of the outputs is assigned to bits 0 to 7 in input byte x + 2. This additional information provides information regarding the validity of the digital values or channel status.

Bit = 1: No error on channel.

Bit = 0: Error on channel.
If the channel is configured as input, this means:

- Short-circuit to ground at sensor supply or
- Parameter error

If the channel is configured as output, this means:

- Short-circuit of output to ground or
- Parameter error or
- For channels 4 ... 7: Missing load voltage 2L+

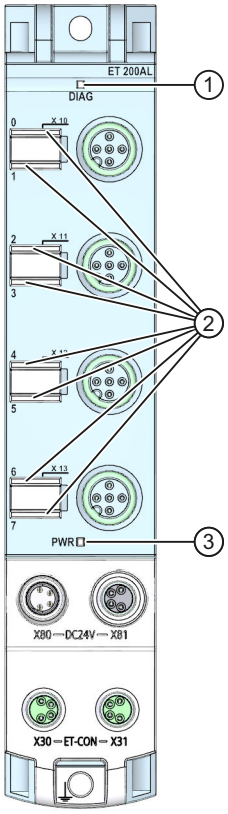
Interrupts/diagnostic alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital input/ digital output module DIQ 4+DQ 4x24VDC/0.5A 4xM12.



①	Diagnostic status (DIAG)	(red/green)
②	Channel status (0 to 7)	(green)
③	Load voltage 2L+ (PWR)	(green)

Figure 2-62 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic alarms can be found in the section Diagnostics alarms (Page 24).

DIAG LED

Table 2-106 Error display of the DIAG LED

DIAG LED	Meaning
□ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-107 LED channel status display

LED channel status	Meaning
□ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-108 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

6.2 Interrupts

The DIQ 4+DQ 4x24VDC/0.5A 4xM12 digital input/digital output module supports diagnostic interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground
- Short-circuit of outputs to ground
- Load voltage 2L+ missing or too low

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input/output module. You can read out the diagnostics alarms, for example, from the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-109 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short circuit[1]	1_H	Short-circuit encoder supply to ground	Eliminate the short-circuit
		Short-circuit of outputs to ground	
Load voltage 2L+ missing[2]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Security event: Firmware has been successfully downloaded and activated for installation.[3]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[3]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 If a short-circuit of the encoder supply to ground is detected, the diagnostics alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.

2 If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostics alarm "Load voltage missing" is displayed

3 A diagnostics alarm is output for a signed firmware update.

NOTE

Channel type

The digital input/digital output module is always signaled as a mixed module (channel type "Input/Output") in the case of diagnostic events, even if you have configured the digital input/digital output module exclusively as an output module.

Technical specifications

7

7.1 Technical specifications

Technical specifications of the DIQ 4+DQ 4x24VDC/0.5A 4xM12 digital input/digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7143-5AF00-0BA0/td?dl=en).

Article number	6ES7143-5AF00-0BA0
General information	
Product type designation	DIQ 4+DQ 4x24VDC/0.5A
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 Hotfix 7 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction; load increasing
Input current	
Current consumption (rated value)	40 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value

Article number	6ES7143-5AF00-0BA0
Encoder supply	
Number of outputs	4
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders
Power loss	
Power loss, typ.	2.5 W
Digital inputs	
Number of digital inputs	4; Parameterizable as DIQ
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	4
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3.2 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Digital outputs	
Number of digital outputs	8; 4 DQ fixed, 4 DIQ parameterizable
• in groups of	4; 2 load groups for 4 outputs each
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	0.7 A
Limitation of inductive shutdown voltage to	2L+ (-47 V)
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA

Article number	6ES7143-5AF00-0BA0
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per group, max.	2 A
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Outputs to M; encoder supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels, in groups of	4; DIQ channels are isolated from DQ channels
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No; DIQ channels are non-isolated and DQ channels are isolated from supply voltage 1L+
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198632

Article number	6ES7143-5AF00-0BA0
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input/digital output module is explained in the following sections.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 DI operating mode

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-110 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] As there is only one encoder supply U_S for all channels, the supply can only be switched off at "pause" if all channels are configured to switch off.

8.3 DQ operating mode

Display

The channel status LEDs are directly affected by the signal level at the socket.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-111 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

Dimension drawing

A

The figure below shows the dimension drawing of the DIQ 4+DQ 4x24VDC/0.5A 4xM12 digital input/digital output module in front and side views.

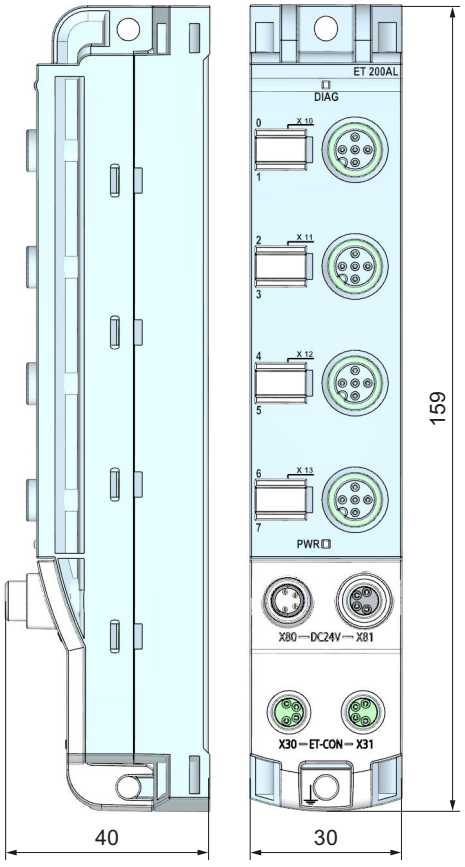


Figure 2-63 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 3_D ($0000\ 0011_B$)							
2...4	**Parameter**							
2	Reserved[1]					Diagnostics: Short-circuit to ground	Diagnostics: Missing load voltage 2L+	Reserved[1]

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	Reserved[1]					0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	Reserved[1]
3	Reserved[1]		Response at CPU/master STOP[2] 00_B: Shut down 10_B: Keep last value 11_B: Output substitute value		Configuration mode channel 3 0_B: DI 1_B: DQ	Configuration mode channel 2 0_B: DI 1_B: DQ	Configura-tion mode channel 1 0_B: DI 1_B: DQ	Configuration mode channel 0 0_B: DI 1_B: DQ
4	Substitute value channel 7[2] 0_B: 0 1_B: 1	Substitute value channel 6[2] 0_B: 0 1_B: 1	Substitute value channel 5[2] 0_B: 0 1_B: 1	Substitute value channel 4[2] 0_B: 0 1_B: 1	Substitute value channel 3[2] 0_B: 0 1_B: 1	Substitute value channel 2[2] 0_B: 0 1_B: 1	Substitute value channel 1[2] 0_B: 0 1_B: 1	Substitute value channel 0[2] 0_B: 0 1_B: 1

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 24) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-112 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL Digital input/digital output module DIQ 4+DQ 4x24VDC/0.5A 8xM8 (6ES7143-5BF00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostics alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

10/2024
A5E32349882-AE

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 15
4.2 Pin assignment 16

5 Parameters/address space 19

5.1 Parameters 19
5.2 Explanation of the parameters 19
5.3 Address space 20

6 Interrupts/diagnostics alarms 22

6.1 Status and error displays 22
6.2 Interrupts 24
6.3 Diagnostics alarms 25

7 Technical specifications 26

8 PROFIenergy 30

8.1 Pause function 30
8.2 DI operating mode 31
8.3 DQ operating mode 32

A Dimension drawing 33

B Parameter data record 34
B.1 Structure of data record 128 for the module parameter assignment 34
B.2 Error transferring the data record 35

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7143-5BF00-0BA0

View of the module

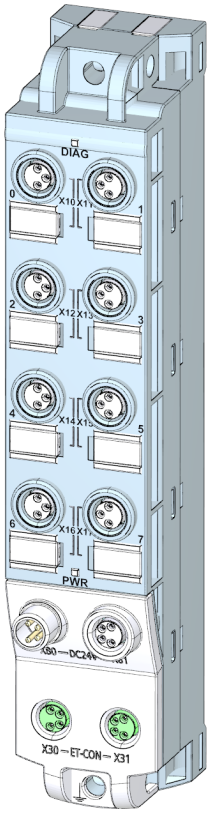


Figure 2-64 View of the DIQ 4+DQ 4x24VDC/0,5A 8xM8 digital input/digital output module

Properties

The module has the following technical properties:

- 4 digital inputs or digital outputs and 4 digital outputs, depending on parameter assignment
  - DIQ signals connected to 1L+ (non-switched)
  - DQ signals connected to 2L+ (switched)
- M8 sockets for connection of sensors and actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Configurable diagnostics can be set for each module
  - Typical input delay of 3 ms
  - Suitable for switches and proximity switches
- Digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current 0.5 A per output
  - Configurable diagnostics can be set for each module
- Dimensions 30 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

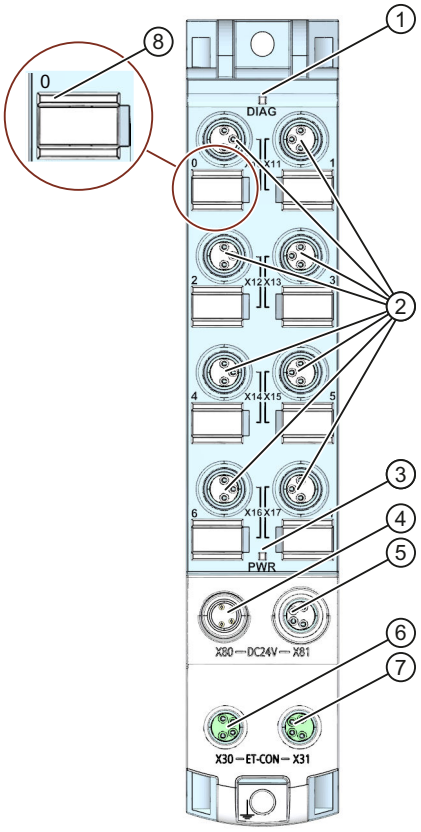
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The following figure shows the operator controls and display elements of the DIQ 4+DQ 4x24VDC/0.5A 8xM8 digital input/digital output module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input/output signal
③ PWR: LED display for the load voltage 2L+
④ X80: Connector for infeed of the supply voltage (POWER input)
⑤ X81: Socket for loop-through of the supply voltage (POWER output)
⑥ X30: Socket for ET-Connection IN
⑦ X31: Socket for ET-Connection OUT
⑧ LED displays 0 to 7 for the channel status

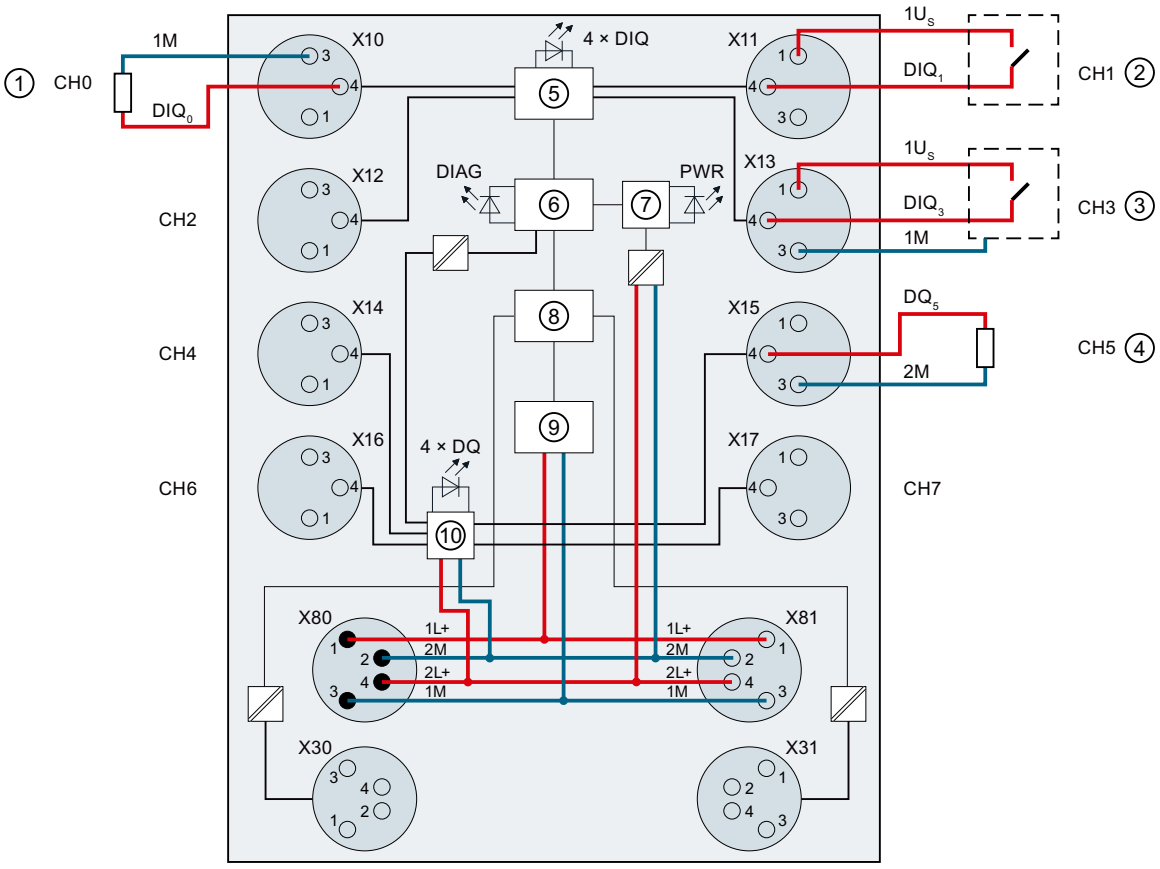
Figure 2-65 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The following figure shows an example of the pin assignment of signal inputs with 2- and 3-wire connection as well as signal outputs.



①	Configured as output	X30	Infeed of the ET-Connection
②	Configured as input: 2-wire connection	X31	Loop-through of the ET-Connection
③	Configured as input: 3-wire connection	1L+	Supply voltage 1L+ (non-switched)
④	Output	1M	Ground 1M (non-switched)
⑤	DI/DQ circuit	2L+	Load voltage 2L+ (switched)
⑥	Microcontroller	2M	Ground 2M (switched)
⑦	Monitoring	$1U_S$	24 V encoder supply
⑧	ET-Connection interface	DIQ_n	Input/output signal
⑨	Internal supply voltage	DQ_n	Output signal
⑩	DQ circuit	DIQ	LEDs channel status (0, 1, 2 and 3) (green)
X10 to X17	Channels 0 to 7	DQ	LEDs channel status (4, 5, 6 and 7) (green)
X80	Infeed of supply voltages	DIAG	LED diagnostic status (red/green)
X81	Loop-through of supply voltages	PWR	LED supply voltage 2L+ (green)

Figure 2-66 Terminal and block diagram

4.2 Pin assignment

NOTE

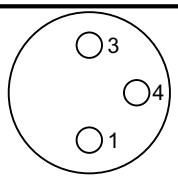
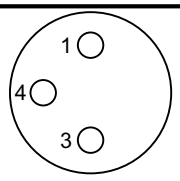
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital inputs/digital outputs

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs.

Table 2-113 Pin assignment for digital inputs/digital outputs

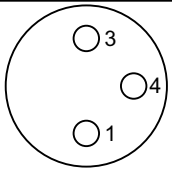
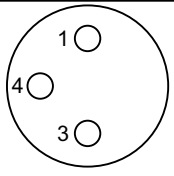
Pin	Assignment	Front view of the sockets	
	X10 to X13 sockets for digital inputs/ digital outputs	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
3	Encoder supply ground 1M		
4	Input/output signal DIQ_0: Connector X10 Input/output signal DIQ_1: Connector X11 Input/output signal DIQ_2: Connector X12 Input/output signal DIQ_3: Connector X13		

NOTICE

24 V encoder supply $1U_S$

Use only the 24 V encoder supply $1U_S$ provided by the digital input/digital output module to supply power to the encoder.

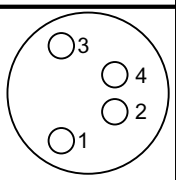
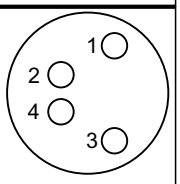
Table 2-114 Pin assignment for digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 sockets for digital outputs	**X14, X16**	**X15, X17**
1	Unassigned		
3	Ground 2M		
4	Output signal DQ_4: Connector X14 Output signal DQ_5: Connector X15 Output signal DQ_6: Connector X16 Output signal DQ_7: Connector X17		

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

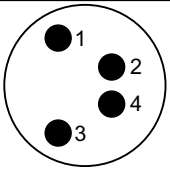
Table 2-115 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

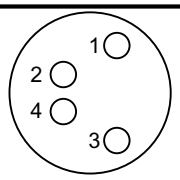
Table 2-116 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-117 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The following table shows the parameters for the DIQ 4+DQ 4x24VDC/0.5A 8xM8 digital input/digital output module.

Table 2-118 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of encoder supply or of the output to ground)
Freely assignable channel 0 ... 3	• DI • DQ	DI	Channel
Reaction to CPU/master STOP	• Shut down • Keep last value • Output substitute value	Shut down	Module (digital outputs)
Substitute value channel 0 ... 7	• 0 • 1	0	Channel (digital outputs)

5.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics for short-circuit of the encoder supply or output to ground.

Freely assignable channel n

With this parameter, you set whether the channel is to be operated as an input or output.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the digital outputs of the digital input/ digital output module after a CPU/master STOP:

- Shut down: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel 0 ... 7

With this parameter, you set substitute values for the digital outputs.

5.3 Address space

The table below shows the assignment of the address space for the digital input/output module DIQ 4+DQ 4x24VDC/0.5A 8xM8 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-119 Address space for the digital input/output module DIQ 4+DQ 4x24VDC/0.5A 8xM8 with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x	0	0	0	0					Input values on channels 0 ... 3
IB x +1	0	0	0	0					Value status (QI) for inputs on channels 0 ... 3*
IB x +2									Value status (QI) for outputs on channels 0 ... 7*
Assignment in the process image output (PIQ)									
QB x									Output values on channels 0 ... 7

* 0 = Value read in at channel is incorrect

NOTE

Parameter assignment of the channels

Parameters for the first four channels can be freely assigned.

For the channels 0 ... 3 that are configured as input, the corresponding values in the output data do not trigger any reaction.

For the channels 0 ... 3 that are configured as output, the input value in the process image is 0.

Configuration options of the digital input/digital output module DIQ 4+DQ 4x24VDC/0.5A 8xM8

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

An additional 2 bytes are occupied in the input address space if you enable the value status for the digital input/digital output module. The value status of the inputs is assigned to bits 0 to 3 in input byte x + 1. The value status of the outputs is assigned to bits 0 to 7 in input byte x + 2. This additional information provides information regarding the validity of the digital values or channel status.

Bit = 1: No error on channel.

Bit = 0: Error on channel.
If the channel is configured as input, this means:

- Short-circuit to ground at sensor supply or
- Parameter error

If the channel is configured as output, this means:

- Short-circuit of output to ground or
- Parameter error or
- For channels 4 ... 7: Missing load voltage 2L+

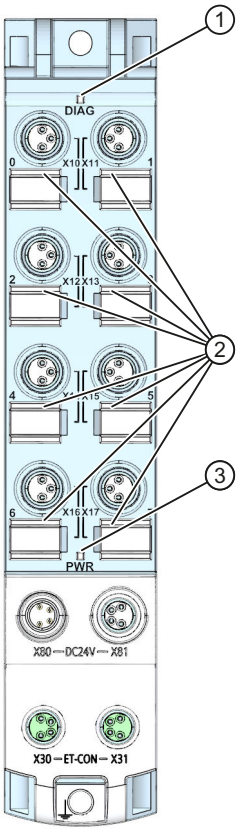
Interrupts/diagnostics alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital input/ digital output module DIQ 4+DQ 4x24VDC/0.5A 8xM8.



①	Diagnostic status (DIAG)	(red/green)
②	Channel status (0 to 7)	(green)
③	Load voltage 2L+ (PWR)	(green)

Figure 2-67 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 25).

DIAG LED

Table 2-120 Error display of the DIAG LED

DIAG LED	Meaning
□ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-121 LED channel status display

LED channel status	Meaning
□ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-122 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

6.2 Interrupts

The DIQ 4+DQ 4x24VDC/0.5A 8xM8 digital input/digital output module supports diagnostic interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground
- Short-circuit of outputs to ground
- Load voltage 2L+ missing or too low

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input/output module.
You can read out the diagnostics alarms, for example, from the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-123 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short circuit[1]	1_H	Short-circuit encoder supply to ground	• Eliminate the short-circuit
		Short-circuit of outputs to ground	
Load voltage 2L+ missing[2]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Security event: Firmware has been successfully downloaded and activated for installation.[3]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[3]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 If a short-circuit of the encoder supply to ground is detected, the diagnostics alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.

2 If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostics alarm "Load voltage missing" is displayed

3 A diagnostics alarm is output for a signed firmware update.

NOTE

Channel type

The digital input/digital output module is always signaled as a mixed module (channel type "Input/Output") in the case of diagnostic events, even if you have configured the digital input/digital output module exclusively as an output module.

Technical specifications

7

Technical specifications of the DIQ 4+DQ 4x24VDC/0.5A 8xM8 digital input/digital output module

Article number	6ES7143-5BF00-0BA0
General information	
Product type designation	DIQ 4+DQ 4x24VDC/0.5A
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	From V5.5 SP4 Hotfix 3
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction; load increasing
Input current	
Current consumption (rated value)	40 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	4
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders
Power loss	
Power loss, typ.	2.5 W

Article number	6ES7143-5BF00-0BA0
Digital inputs	
Number of digital inputs	4; Parameterizable as DIQ
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	4
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3.2 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Digital outputs	
Number of digital outputs	8; 4 DQ fixed, 4 DIQ parameterizable
• in groups of	4; 2 load groups for 4 outputs each
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	0.7 A
Limitation of inductive shutdown voltage to	2L+ (-47 V)
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per group, max.	2 A

Article number	6ES7143-5BF00-0BA0
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Outputs to M; encoder supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels, in groups of	4; DIQ channels are isolated from DQ channels
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No; DIQ channels are non-isolated and DQ channels are isolated from supply voltage 1L+
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C

Article number	6ES7143-5BF00-0BA0
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M8, 3-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7143-5BF00-0BA0/td?dl=en).

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input/digital output module is explained in the following sections.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (http://support.automation.siemens.com/WW/view/en/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 DI operating mode

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-124 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] As there is only one encoder supply U_S for all channels, the supply can only be switched off at "pause" if all channels are configured to switch off.

8.3 DQ operating mode

Display

The channel status LEDs are directly affected by the signal level at the socket.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-125 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

Dimension drawing

A

The following figure shows the dimension drawing of the DIQ 4+DQ 4x24VDC/0.5A 8xM8 digital input/digital output module in front and side views.

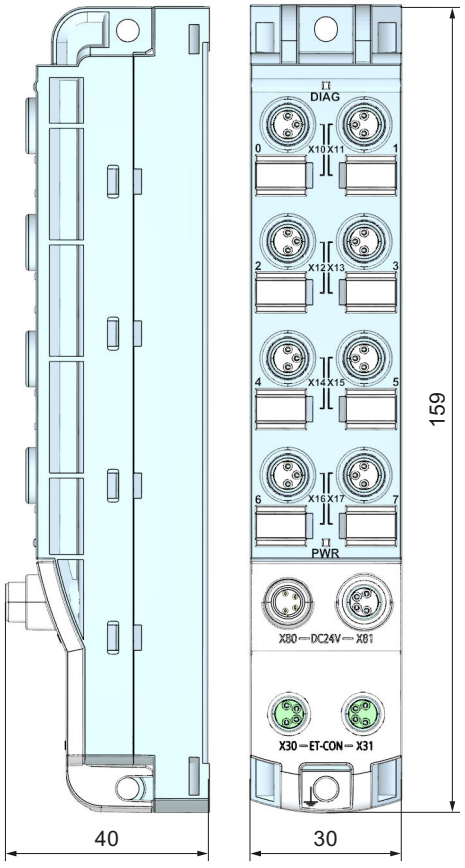


Figure 2-68 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 3_D ($0000\ 0011_B$)							
2...4	**Parameter**							
2	Reserved[1]					Diagnostics: Short-circuit to ground	Diagnostics: Missing load voltage 2L+	Reserved[1]

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	Reserved[1]					0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	Reserved[1]
3	Reserved[1]		Response at CPU/master STOP[2] 00_B: Shut down 10_B: Keep last value 11_B: Output substitute value		Configuration mode channel 3 0_B: DI 1_B: DQ	Configuration mode channel 2 0_B: DI 1_B: DQ	Configuration mode channel 1 0_B: DI 1_B: DQ	Configuration mode channel 0 0_B: DI 1_B: DQ
4	Substitute value channel 7[2] 0_B: 0 1_B: 1	Substitute value channel 6[2] 0_B: 0 1_B: 1	Substitute value channel 5[2] 0_B: 0 1_B: 1	Substitute value channel 4[2] 0_B: 0 1_B: 1	Substitute value channel 3[2] 0_B: 0 1_B: 1	Substitute value channel 2[2] 0_B: 0 1_B: 1	Substitute value channel 1[2] 0_B: 0 1_B: 1	Substitute value channel 0[2] 0_B: 0 1_B: 1

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 25) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-126 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
Digital input / digital output module DIQ 8x24VDC/0.5A 8xM8 (6ES7143-5BF50-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostics alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Parameter data record B

02/2026
A5E53727253-AB

Table of contents

1 Introduction 3
1.1 ET 200AL Documentation Guide 3
1.2 SIMATIC Technical Documentation 5

2 Industrial cybersecurity 7
2.1 Introduction to industrial cybersecurity 7
2.2 Cybersecurity information 7
2.3 Cybersecurity-relevant information 8

3 Product overview 9
3.1 Properties 9
3.2 Operator controls and display elements 11

4 Wiring 12
4.1 Terminal and block diagram 12
4.2 Pin assignment 13

5 Parameters/address space 15
5.1 Parameters 15
5.2 Explanation of the parameters 15
5.3 Address space 16

6 Interrupts/diagnostics alarms 18
6.1 Status and error displays 18
6.2 Interrupts 20
6.3 Diagnostics alarms 20

7 Technical specifications 22

8 PROFIenergy 26
8.1 Pause function 26
8.2 DI operating mode 27
8.3 DQ operating mode 28

A Dimension drawing 29

B Parameter data record 30
B.1 Structure of data record 128 for the module parameter assignment 30
B.2 Error transferring the data record 31

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://www.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7143-5BF50-0BA0

View of the module



Figure 2-69 View of the DIQ 8x24VDC/0.5A 8xM8 digital input/digital output module

Properties

The module has the following technical properties:

- 8 digital inputs or digital outputs, depending on configuration and parameter assignment
  - DIQ signals connected to 2L+ (switched)
- M8 sockets for connection of sensors and actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Configurable diagnostics can be set for each module
  - Typical input delay of 3 ms
  - Suitable for switches and proximity switches

- Digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current 0.5 A per output
  - Configurable diagnostics can be set for each module
- Dimensions 30 x 159 mm

The module supports the following functions:

- Signed firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

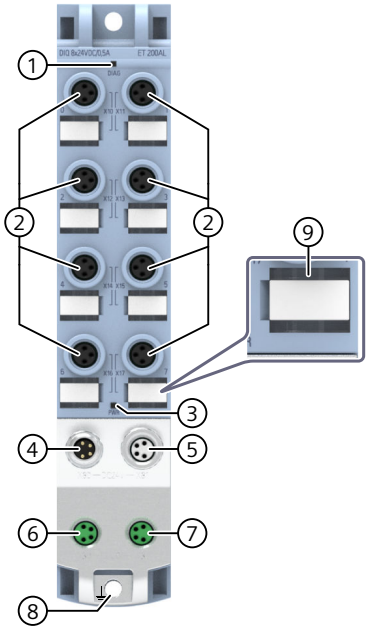
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DIQ 8x24VDC/0.5A 8xM8 digital input/digital output module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input/output signal
③ PWR: LED display for load voltage 2L+
④ X80: Connector for infeed of the supply voltage (POWER input)
⑤ X81: Socket for loop-through of the supply voltage (POWER output)
⑥ X30: Socket for ET-Connection IN
⑦ X31: Socket for ET-Connection OUT
⑧ Functional ground
⑨ LED displays 0 to 7 for the channel status

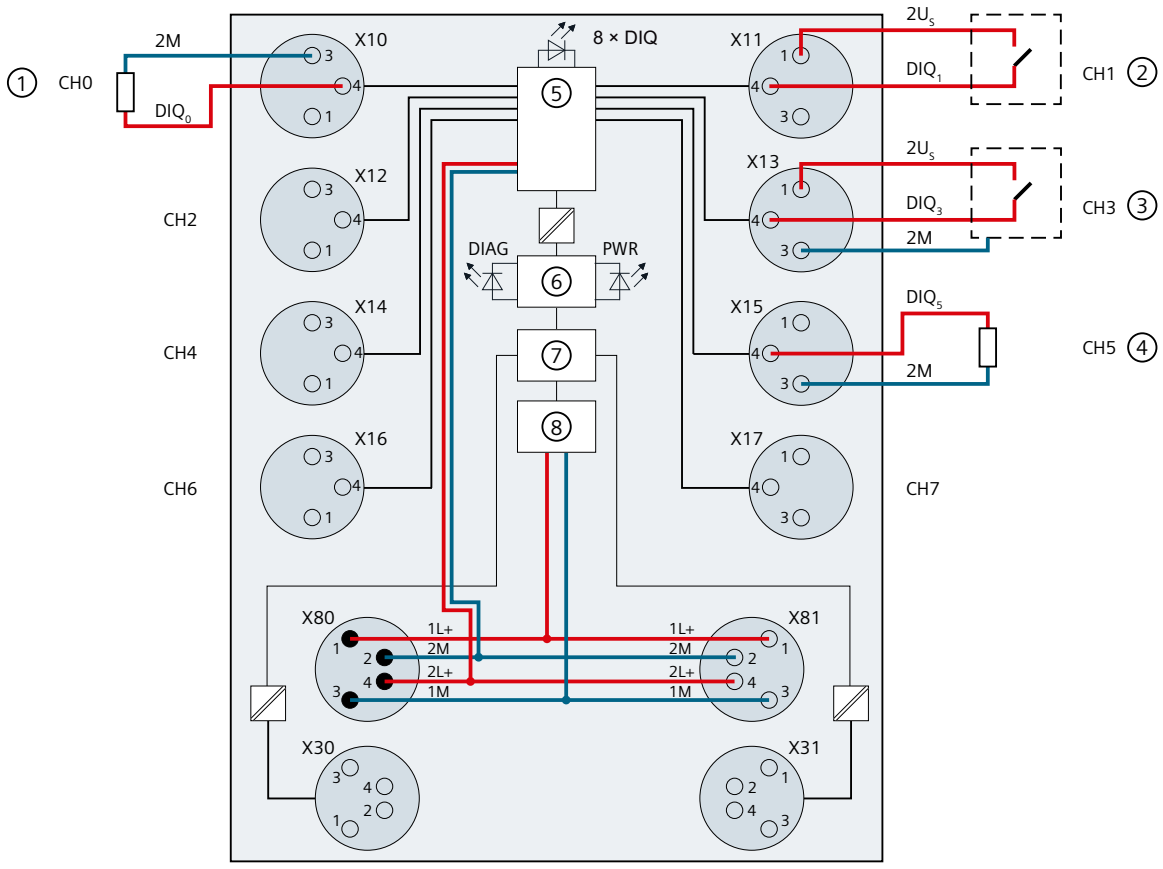
Figure 2-70 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The following figure shows an example of the pin assignment of signal inputs with 2- and 3-wire connection as well as signal outputs.



① + ④	Configured as output	X30	Infeed of the ET-Connection
②	Configured as input: 2-wire connection	X31	Loop-through of the ET-Connection
③	Configured as input: 3-wire connection	1L+	Supply voltage 1L+ (non-switched)
⑤	DI/DQ circuit	1M	Ground 1M (non-switched)
⑥	Microcontroller	2L+	Load voltage 2L+ (switched)
⑦	ET-Connection interface	2M	Ground 2M (switched)
⑧	Internal supply voltage	$2U_S$	24 V encoder supply
X10 to X17	Channels 0 to 7	DIQ_n	Input/output signal
X80	Infeed of supply voltages	DIQ	LEDs channel status (green)
X81	Loop-through of supply voltages	DIAG	LED diagnostic status (red/green)
		PWR	LED supply voltage 2L+ (green)

Figure 2-71 Terminal and block diagram

4.2 Pin assignment

NOTE

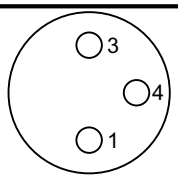
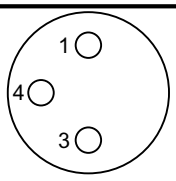
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for digital inputs/digital outputs

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs.

Table 2-127 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 - sockets for digital inputs/ digital outputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
3	Sensor supply ground 2M		
4	Input/output signal DIQ_0: Connector X10 Input/output signal DIQ_1: Connector X11 Input/output signal DIQ_2: Connector X12 Input/output signal DIQ_3: Connector X13 Input/output signal DIQ_4: Connector X14 Input/output signal DIQ_5: Connector X15 Input/output signal DIQ_6: Connector X16 Input/output signal DIQ_7: Connector X17		

NOTICE

24 V encoder supply $2U_S$

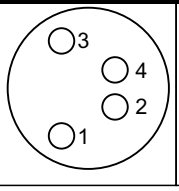
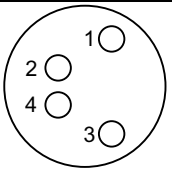
Use only the 24 V encoder supply $2U_S$ provided by the digital input/digital output module to supply power to the encoder.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

Table 2-128 Pin assignment for ET-Connection

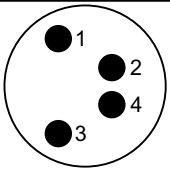
Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	**X31 socket (ET-Connection OUT)**		**X30**	**X31**
1	TXP	RXP	Yellow		
2	RXP	TXP	White		

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

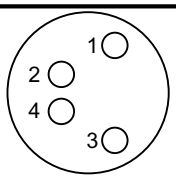
Table 2-129 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-130 Pin assignment of the supply voltage socket

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the socket
	X81 socket (POWER output)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Parameters

The following table shows the parameters for the DIQ 8x24VDC/0.5A 8xM8 digital input/digital output module.

Table 2-131 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of encoder supply or of the output to ground)
Freely configurable channel n	• DI • DQ	DI	Channel
Reaction to CPU/master STOP	• Shut down • Keep last value • Output substitute value	Shut down	Module (digital outputs)
Substitute value channel 0 ... 7	• 0 • 1	0	Channel (digital outputs)

5.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics for short-circuit of the encoder supply or output to ground.

Freely assignable channel n

With this parameter, you set whether the channel is to be operated as an input or output.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the digital outputs of the digital input/ digital output module after a CPU/master STOP:

- Shut down: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel 0 ... 7

With this parameter, you set substitute values for the digital outputs.

5.3 Address space

The tables below shows the assignment of the address space for the digital input / output module DIQ 8x24VDC/0.5A 8xM8 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses are available for the value status. The value status is not available for PROFIBUS.

Table 2-132 Assignment in the process image input (PII)

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
IB x									Input values at channels 0 ... 7
IB x +1									Value status (QI) for inputs at channels 0 ... 7*
IB x +2									Value status (QI) for outputs at channels 0 ... 7*

* 0 = Value read in at channel is incorrect

Table 2-133 Assignment in the process image output (PIQ)

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
QB x									Output values at channels 0 ... 7

NOTE

Parameter assignment of the channels

If a channel is parameterized as an input, this channel does not result in a response in the output data.

If a channel is parameterized as an output, the input value in the process image is 0 for this channel.

Configuration options of the digital input/digital output module DIQ 8x24VDC/0.5A 8xM8

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

An additional two bytes are occupied in the input address space if you enable the value status for the digital input/digital output module. The value status of the inputs is assigned to bits 0 to 7 in input byte x + 1. The value status of the outputs is assigned to bits 0 to 7 in input byte x + 2. This additional information provides information regarding the validity of the digital values or channel status.

Bit = 1: No error on channel.

Bit = 0: Error on channel.
If the channel is parameterized as an input, this can mean:

- Short-circuit to ground at transducer supply
- Parameter error

If the channel is parameterized as an output, this can mean:

- Short-circuit of the output to ground
- Parameter error
- Missing load voltage 2L+

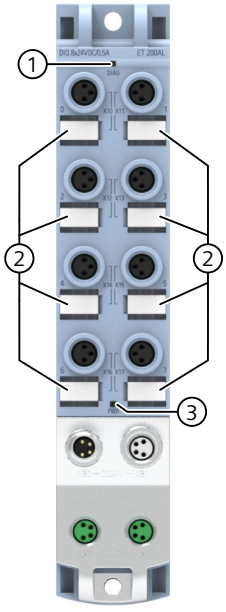
Interrupts/diagnostics alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital input/ digital output module DIQ 8x24VDC/0.5A 8xM8.



①	Diagnostic status (DIAG)	(red/green)
②	Channel status (0 to 7)	(green)
③	Load voltage 2L+ (PWR)	(green)

Figure 2-72 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 20).

DIAG LED

Table 2-134 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-135 LED channel status display

LED channel status	Meaning
☐ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-136 Status display of the PWR LED

PWR LED	Meaning
☐ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

6.2 Interrupts

The DIQ 8x24VDC/0.5A 8xM8 digital input/digital output module supports diagnostic interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground
- Short-circuit of outputs to ground
- Load voltage 2L+ missing or too low

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input/output module. You can read out the diagnostics messages, for example, from the diagnostic buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-137 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Remedy
Short circuit[1]	1_H	Short-circuit encoder supply to ground	Eliminate the short-circuit
		Short-circuit of outputs to ground	
Parameterization error	10_H	• The module cannot evaluate parameters for the channel • Incorrect parameter assignment	Correct the parameter assignment.
Load voltage 2L+ missing[2]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Security event: Firmware has been successfully downloaded and activated for installation.[3]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[3]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 If a short-circuit of the encoder supply to ground is detected, the diagnostics alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.

2 If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostics alarm "Missing supply voltage" is displayed

3 A diagnostics alarm is output for a signed firmware update.

NOTE

Channel type

The digital input/digital output module is always signaled as a mixed module (channel type "Input/Output") in the case of diagnostic events, even if you have configured the digital input/digital output module exclusively as an output module.

Technical specifications

7

Technical specifications of the DIQ 8x24VDC/0.5A 8xM8 digital input/digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7143-5BF50-0BA0/td?dl=en).

Article number	6ES7143-5BF50-0BA0
General information	
Product type designation	DIQ 8x24VDC/0.5A, 8xM8
HW functional status	From FS03
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M4
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V18 or higher
• STEP 7 configurable/integrated from version	V5.6 and higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.4.x
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up
Input current	
Current consumption (rated value)	20 mA; 20 mA (1L+) / 40 mA (2L+); without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	8

Article number	6ES7143-5BF50-0BA0
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	1.4 A; Total current of all encoders
Power loss	
Power loss, typ.	2.6 W
Digital inputs	
Number of digital inputs	8; Parameterizable as DIQ
Sourcing/sinking input	P-reading
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	8
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	2.4 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Digital outputs	
Number of digital outputs	8
Current-sourcing	Yes
output type acc. to IEC 61131, type 0.5	Yes
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	0.7 A
Limitation of inductive shutdown voltage to	2L+ (-47 V)
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA

Article number	6ES7143-5BF50-0BA0
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per module, max.	4 A
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Outputs to M; encoder supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; from FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/document/39198632
Security	
signed firmware update	Yes
data integrity	Yes

Article number	**6ES7143-5BF50-0BA0**
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
Connection method	
Design of electrical connection for the inputs and outputs	M8, 3-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input/digital output module is explained in the following sections.

Additional information

You can find more information on working with PROFIenergy in the PROFIenergy section of the Equipment Manual Interface module IM 157-1 PN (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of the Function Manual PROFINET with STEP 7 (http://support.automation.siemens.com/WW/view/en/49948856) .

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 DI operating mode

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-138 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltage U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] As there is only one encoder supply U_S for all channels, the supply can only be switched off at "pause" if all channels are configured to switch off.

8.3 DQ operating mode

Display

The channel status LEDs are directly affected by the signal level at the socket.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-139 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

Dimension drawing

A

The figure below shows the dimension drawing of the DIQ 8x24VDC/0.5A 8xM8 digital input/digital output module in front and side views.

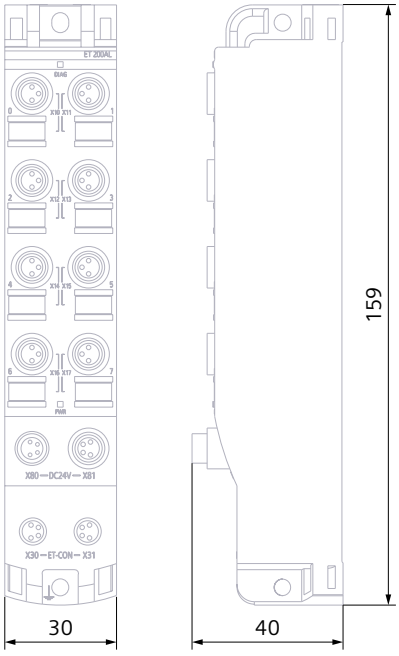


Figure 2-73 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 4_D ($0000\ 0100_B$)							
2...5	**Parameter**							
2	Reserved[1]					Diagnostics: Short-circuit to ground	Diagnostics: Missing load voltage 2L+	Reserved[1]

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2	Reserved[1]					0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	Reserved[1]
3	Reserved[1]		Response at CPU/master STOP[2] 00_B: Shut down 10_B: Keep last value 11_B: Output substitute value		Reserved[1]			
4	Operating mode channel 7	Operating mode channel 6	Operating mode channel 5	Operating mode channel 4	Operating mode channel 3	Operating mode channel 2	Operating mode channel 1	Operating mode channel 0
	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ
5	Substitute value channel 7[2]	Substitute value channel 6[2]	Substitute value channel 5[2]	Substitute value channel 4[2]	Substitute value channel 3[2]	Substitute value channel 2[2]	Substitute value channel 1[2]	Substitute value channel 0[2]
	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 20) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-140 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	Byte 1	Byte 2	Byte 3			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL Digital input/Digital output module DIQ 16x24VDC/0.5A 8xM12 (6ES7143-5AH00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Configuration modes for digital inputs/outputs 4

Counting 5

Technical specifications 6

PROFIenergy 7

Dimension drawing A

Parameter data record B

10/2024
A5E38688112-AE

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 14

4 Configuration modes for digital inputs/outputs 15

4.1 Overview 15
4.2 Wiring 16
4.2.1 Terminal and block diagram 16
4.2.2 Pin assignment 17
4.3 Parameters/address space 22
4.3.1 Parameters 22
4.3.2 Explanation of the parameters 23
4.3.3 Address space 24
4.4 Interrupts/diagnostic alarms 27
4.4.1 Status and error displays 27
4.4.2 Interrupts 29
4.4.3 Diagnostics alarms 29

5 Counting 31

5.1 Configuration method 2xCount 33
5.1.1 Wiring 33
5.1.1.1 Terminal and block diagram 33
5.1.1.2 Pin assignment 34
5.1.2 Parameters/address space 37
5.1.2.1 Parameters 37
5.1.2.2 Explanation of the parameters 39
5.1.2.3 Assignment of the control interface 43
5.1.2.4 Explanations on the control interface 44

5.1.2.5 Assignment of the feedback interface ... 45
5.1.2.6 Explanations for the feedback interface ... 46
5.1.3 Interrupts/diagnostic alarms ... 48
5.1.3.1 Status and error displays ... 48
5.1.3.2 Interrupts ... 50
5.1.3.3 Diagnostics alarms ... 51
5.2 Configuration method 4xCount ... 52
5.2.1 Wiring ... 52
5.2.1.1 Terminal and block diagram ... 52
5.2.1.2 Pin assignment ... 53
5.2.2 Parameters/address space ... 55
5.2.2.1 Parameters ... 55
5.2.2.2 Explanation of the parameters ... 57
5.2.2.3 Assignment of the control interface ... 60
5.2.2.4 Explanations on the control interface ... 61
5.2.2.5 Assignment of the feedback interface ... 62
5.2.2.6 Explanations for the feedback interface ... 63
5.2.3 Interrupts/diagnostic alarms ... 65
5.2.3.1 Status and error displays ... 65
5.2.3.2 Interrupts ... 67
5.2.3.3 Diagnostics alarms ... 68
5.3 Examples of counting ... 68

6 Technical specifications ... 74

7 PROFIenergy ... 78

7.1 Pause function ... 78
7.2 Behavior of the digital inputs ... 79
7.3 Behavior of the digital outputs ... 80
7.4 Behavior of the digital inputs of the counters ... 81

A Dimension drawing ... 83

B Parameter data record ... 84

B.1 Structure of data record 128 for the module parameter assignment ... 84
B.2 Error transferring the data record ... 87

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7143-5AH00-0BA0

View of the module

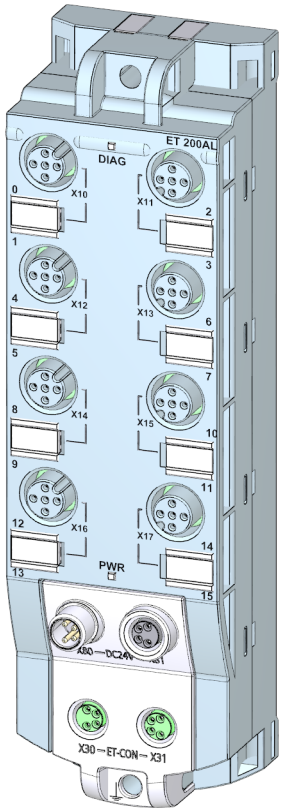


Figure 2-74 View of the digital input/digital output module DIQ 16x24VDC/0.5A 8xM12

Properties

The module has the following technical properties:

- 16 digital inputs or digital outputs, depending on configuration and parameter assignment
  - 8 DIQ signals connected to 1L+ (non-switched)
  - 8 DQ signals connected to 2L+ (switched)
- M12 sockets for connection of sensors and actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Suitable for switches and proximity switches
  - Input delay configurable
  - Configurable diagnostics can be set for each module
- Digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current per output 0.5 A
  - Configurable diagnostics can be set for each module
- Counters:
  - Configuration method 2xCount or 4xCount with 2 or 4 counters
  - Counting frequency 2 kHz
  - Counting width 32 bits
  - Counting direction parameterizable or controllable via direction input
  - GATE function controllable via the control interface or via control input
  - Configurable diagnostics and hardware interrupts can be set for each module
  - Input delay configurable
- Dimensions 45 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

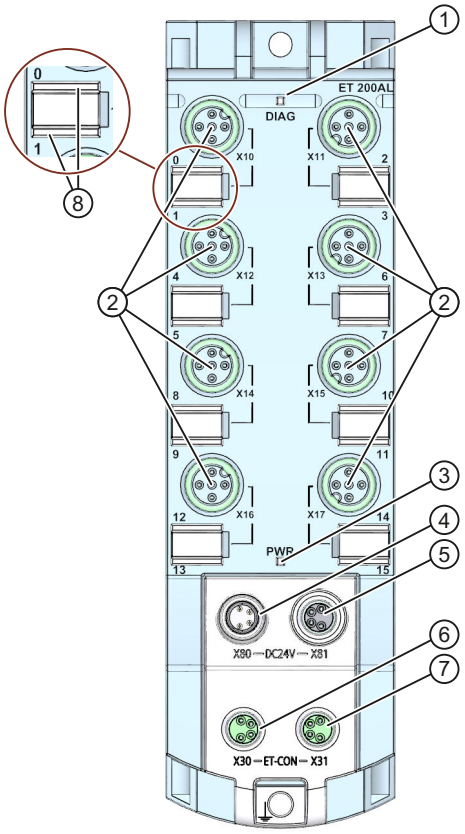
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) system manual.

3.2 Operator controls and display elements

The following figure shows the operator controls and display elements of the digital input/digital output module DIQ 16x24VDC/0.5A 8xM12.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input/output signal
③ PWR: LED display for load voltage 2L+
④ X80: Connector for infeed of the supply voltage (POWER input)
⑤ X81: Socket for loop-through of the supply voltage (POWER output)
⑥ X30: Socket for ET-Connection IN
⑦ X31: Socket for ET-Connection OUT
⑧ LED displays 0 to 15 for the channel status

Figure 2-75 Operator controls and display elements

Configuration modes for digital inputs/outputs

4

4.1 Overview

Introduction

With the configuration modes for digital inputs and outputs, you can configure each channel of the module as an input or output consistent with your application.

You use the available configuration modes to specify how the channels will be used:

- DIQ:
  You can use each channel as an input or output through a corresponding parameter assignment.
- DIQ with value status:
  You can use each channel as an input or output through a corresponding parameter assignment. Additionally, the value status gives you information about the validity of the digital values and the channel status.
- DQ16:
  All channels (0..15) are configured as outputs.
- DI8/DQ8:
  Channels 0..7 are configured as inputs, and channels 8..15 are configured as outputs.
- DIQ MIX:
  The channels 0, 2, 4, 6, 8, 10, 12, 14 and 16 have a fixed configuration as outputs, the channels 1, 3, 5, 7, 9, 11, 13 and 15 have a fixed configuration as inputs.

NOTE

Project engineering configuration mode DIQ MIX

Note that you can only use the configuration mode DIQ MIX when configuring via GSD file and in connection with the interface modules IM 157-1 PN and IM 157-1 DP.

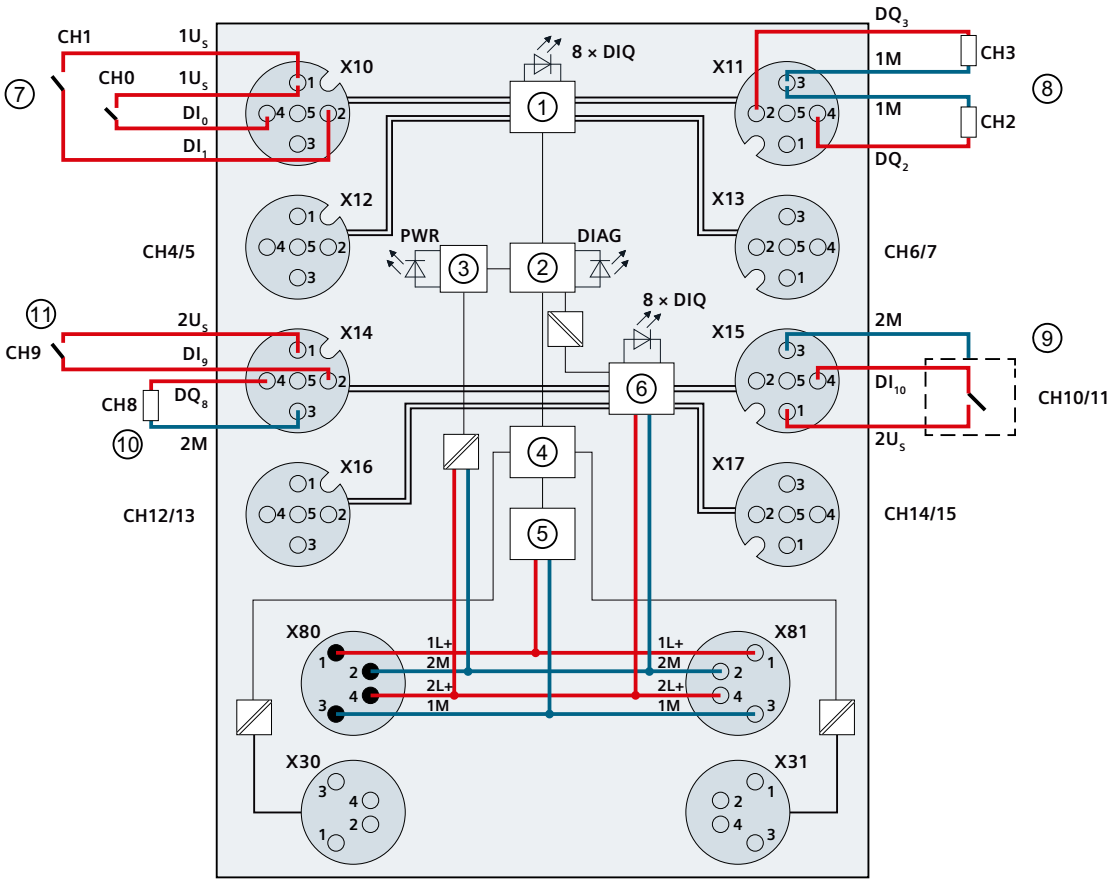
Benefits

The address space occupied by the module is significantly reduced in the DQ16, DI8/DQ8 and DIQ MIX configuration modes compared with the DIQ configuration modes.
This reduction offers you advantages if you have already assigned the available address space of your plant for other processes.

4.2 Wiring

4.2.1 Terminal and block diagram

The figure below shows an example of the pin assignment of signal inputs with 2-wire and 3-wire connection and of signal outputs in the configuration modes for digital inputs and outputs.



①	DI/DQ circuit (1L+ non-switched)	X81	Loop-through of supply voltages
②	Microcontroller	X30	Infeed of the ET-Connection
③	Monitoring	X31	Loop-through of the ET-Connection
④	ET-Connection interface	1L+	Supply voltage 1L+ (non-switched)
⑤	Internal supply voltage	1M	Ground 1M (non-switched)
⑥	DI/DQ circuit (2L+ switched)	2L+	Load voltage 2L+ (switched)
⑦	Parameterized as inputs: 2-wire connection	2M	Ground 2M (switched)
⑧	Parameterized as outputs	$1U_S$	24 V encoder supply
⑨	Configured as input: 3-wire connection	$2U_S$	24 V encoder supply
⑩	Configured as output	DIQ_n	Input/output signal
⑪	Configured as input: 2-wire connection	DIQ	LEDs channel status (0..15) (green)
X10 to X17	Channels 0 to 15	DIAG	Diagnostic status LED (red/green)
X80	Infeed of supply voltages	PWR	LED supply voltage 2L+ (green)

Figure 2-76 Wiring and block diagram of configuration modes for digital inputs and outputs

4.2.2 Pin assignment

NOTE

Color coding
The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

NOTICE
24 V encoder supply $1U_S$ / $2U_S$ Use only the 24 V encoder supplies $1U_S$ and $2U_S$ provided by the digital input/digital output module to supply power to the encoder.

Pin assignment of the sockets for digital inputs/digital outputs in the configuration modes DIQ and DIQ with value status

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs.

Table 2-141 Pin assignment for digital inputs/digital outputs

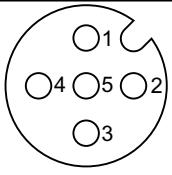
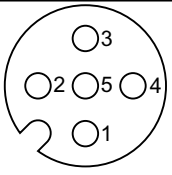
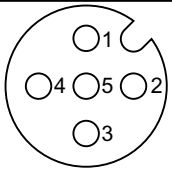
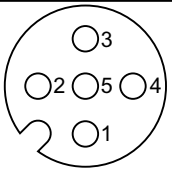
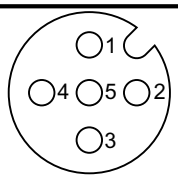
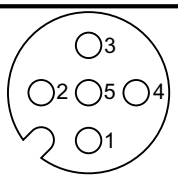
Pin	Assignment	Front view of the sockets	
	X10 to X13 sockets for digital inputs / outputs	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Input/output signal DIQ_1: Connector X10 Input/output signal DIQ_3: Connector X11 Input/output signal DIQ_5: Connector X12 Input/output signal DIQ_7: Connector X13		
3	Ground 1M		
4	Input/output signal DIQ_0: Connector X10 Input/output signal DIQ_2: Connector X11 Input/output signal DIQ_4: Connector X12 Input/output signal DIQ_6: Connector X13		
5	Functional earth FE		

Table 2-142 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Input/output signal DIQ_9: Connector X14 Input/output signal DIQ_{11}: Connector X15 Input/output signal DIQ_{13}: Connector X16 Input/output signal DIQ_{15}: Connector X17		
3	Ground 2M		
4	Input/output signal DIQ_8: Connector X14 Input/output signal DIQ_{10}: Connector X15 Input/output signal DIQ_{12}: Connector X16 Input/output signal DIQ_{14}: Connector X17		

Pin	Assignment	Front view of the sockets	
	X14 to X17 sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
5	Functional earth FE		

Pin assignment of the sockets for digital inputs/digital outputs in the configuration mode DQ16

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs in the configuration mode DQ16.
In this configuration mode, socket pins 2 and 4 are always permanently assigned to output signals.

Table 2-143 Pin assignment for digital inputs/digital outputs

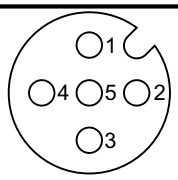
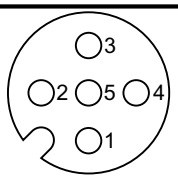
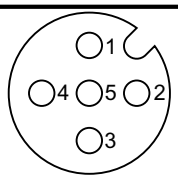
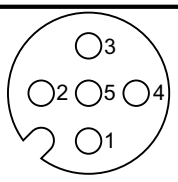
Pin	Assignment	Front view of the sockets	
	X10 to X13 sockets for digital inputs / outputs	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Output signal DQ_1: Connector X10 Output signal DQ_3: Connector X11 Output signal DQ_5: Connector X12 Output signal DQ_7: Connector X13		
3	Ground 1M		
4	Output signal DQ_0: Connector X10 Output signal DQ_2: Connector X11 Output signal DQ_4: Connector X12 Output signal DQ_6: Connector X13		
5	Functional earth FE		

Table 2-144 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Output signal DQ_9: Connector X14 Output signal DQ_{11}: Connector X15 Output signal DQ_{13}: Connector X16 Output signal DQ_{15}: Connector X17		
3	Ground 2M		
4	Output signal DQ_8: Connector X14 Output signal DQ_{10}: Connector X15 Output signal DQ_{12}: Connector X16 Output signal DQ_{14}: Connector X17		
5	Functional earth FE		

Pin assignment of the sockets for digital inputs/digital outputs in the configuration mode DI8/DQ8

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs in the configuration mode DI8/DQ8.
In this configuration mode, pins 2 and 4 for the sockets X10 to X13 are always permanently assigned to the input signals, pins 2 and 4 for the sockets X14 to X17 are always permanently assigned to the output signals.

Table 2-145 Pin assignment for digital inputs/digital outputs

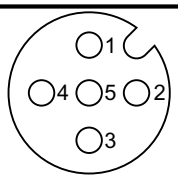
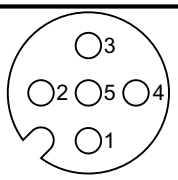
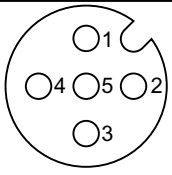
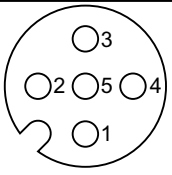
Pin	Assignment	Front view of the sockets	
	X10 to X13 sockets for digital inputs / outputs	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Input signal DI_1: Connector X10 Input signal DI_3: Connector X11 Input signal DI_5: Connector X12 Input signal DI_7: Connector X13		
3	Ground 1M		
4	Input signal DI_0: Connector X10 Input signal DI_2: Connector X11 Input signal DI_4: Connector X12 Input signal DI_6: Connector X13		
5	Functional earth FE		

Table 2-146 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Output signal DQ_9: Connector X14 Output signal DQ_{11}: Connector X15 Output signal DQ_{13}: Connector X16 Output signal DQ_{15}: Connector X17		
3	Ground 2M		
4	Output signal DQ_8: Connector X14 Output signal DQ_{10}: Connector X15 Output signal DQ_{12}: Connector X16 Output signal DQ_{14}: Connector X17		
5	Functional earth FE		

Pin assignment of the sockets for digital inputs/digital outputs in the configuration mode DIQ MIX

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs in the configuration mode DIQ MIX.
In this configuration mode, socket pin 2 is always permanently assigned to input signals, pin 4 is always permanently assigned to output signals.

Table 2-147 Pin assignment for digital inputs/digital outputs

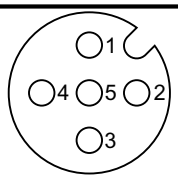
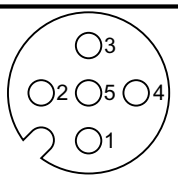
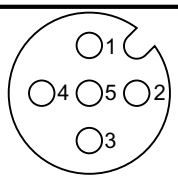
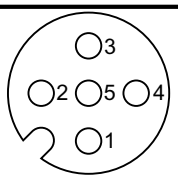
Pin	Assignment	Front view of the sockets	
	X10 to X13 sockets for digital inputs / outputs	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Input signal DI_1: Connector X10 Input signal DI_3: Connector X11 Input signal DI_5: Connector X12 Input signal DI_7: Connector X13		
3	Ground 1M		
4	Output signal DQ_0: Connector X10 Output signal DQ_2: Connector X11 Output signal DQ_4: Connector X12 Output signal DQ_6: Connector X13		
5	Functional earth FE		

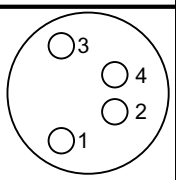
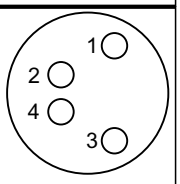
Table 2-148 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Input signal DI_9: Connector X14 Input signal DI_{11}: Connector X15 Input signal DI_{13}: Connector X16 Input signal DI_{15}: Connector X17		
3	Ground 2M		
4	Output signal DQ_8: Connector X14 Output signal DQ_{10}: Connector X15 Output signal DQ_{12}: Connector X16 Output signal DQ_{14}: Connector X17		
5	Functional earth FE		

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

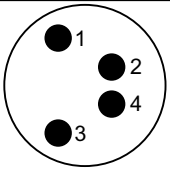
Table 2-149 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

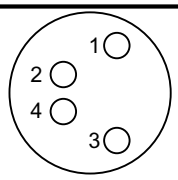
Table 2-150 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the core color of the power cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-151 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

4.3 Parameters/address space

4.3.1 Parameters

The following table shows the parameters for the DIQ 16x24VDC/0.5A 8xM12 digital input / digital output module in the configuration modes for digital inputs and outputs.

Table 2-152 Parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of encoder supply or of the output to ground)
Reaction to CPU/master STOP	• Shut down • Keep last value • Output substitute value	Shut down	Module (digital outputs)
Freely configurable channel*	• DI • DQ	DI	Channel
Substitute value channel	• 0 • 1	0	Channel (digital outputs)

* = Can only be set in DIQ or DIQ with value status configuration mode.
** = Not available in DQ16 mode. Only values starting from 1.6 ms can be configured for the input delay for channels 8..15.

Parameters	Value range	Default	Scope
Input delay**	• 0.05 ms • 0.1 ms • 0.4 ms • 0.8 ms • 1.6 ms • 3.2 ms • 12.8 ms • 20 ms	3.2 ms	Channel (Digital inputs)

* = Can only be set in DIQ or DIQ with value status configuration mode.
** = Not available in DQ16 mode. Only values starting from 1.6 ms can be configured for the input delay for channels 8..15.

4.3.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics, at short-circuit of an encoder supply or of an output to ground.

Freely assignable channel

With this parameter, you set whether the channel is to be operated as an input or output.
You can only set this parameter in the DIQ and DIQ with value status configuration modes.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the channels configured as output of the digital input/output module after a CPU/master STOP:

- Deactivate: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel

With this parameter, you set substitute values for the digital outputs.

Input delay

This parameter can be used to avoid signal faults. Changes to the signal are only detected if they are present and stable for longer than the set input delay time.
You cannot set this parameter in DQ16 mode.

4.3.3 Address space

The DIQ 16x24VDC/0.5A 8xM12 digital input/output module occupies a different number of bytes in the process image input (PII) or process image output (PIQ), depending on which configuration mode you selected.
The following figures show you the various assignments of the address spaces.

NOTE

Parameter assignment of the channels
In the configuration modes for digital inputs and outputs, either all channels are user configurable or all channels have a fixed configuration, depending on the configuration.
For the channels that are configured as an input, the corresponding values in the output data do not trigger any reaction.
For the channels that are configured as an output, the input value in the process image is 0.

Configuration mode DIQ without value status

The tables below show the assignment of the address space for the DIQ 16x24VDC/0.5A 8xM12 digital input/digital output module in the DIQ without value status configuration mode (Quality Information, QI).

Table 2-153 Address space in the configuration mode DIQ without value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Input values on channels 0 ... 7
IB x +1									Input values on channels 8 ... 15
Assignment in the process image output (PIQ)									
QB x									Output values on channels 0 ... 7
QB x +1									Output values on channels 8 ... 15

Configuration mode DIQ with value status

The tables below show the assignment of the address space for the digital input/digital output module DIQ 16x24VDC/0.5A 8xM12 with value status (Quality Information, QI) in the configuration mode DIQ. If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-154 Address space in the configuration mode DIQ with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Input values on channels 0 ... 7
IB x +1									Value status (QI) for inputs on channels 0 ... 7*

* 0 = Value read in at channel is incorrect

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
IB x +2									Value status (QI) for inputs on channels 0 ... 7*
IB x +3									Value status (QI) for inputs on channels 8 ... 15*
IB x +4									Value status (QI) for outputs on channels 0 ... 7*
IB x +5									Value status (QI) for outputs on channels 8 ... 15*
Assignment in the process image output (PIQ)									
QB x									Output values on channels 8 ... 15
QB x +1									Output values on channels 8 ... 15

* 0 = Value read in at channel is incorrect

Configuration mode DQ16

In DQ16 configuration mode, the address space is reduced by the fixed parameter assignment.

Table 2-155 Address space in the configuration mode DQ16

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image output (PIQ)									
QB x									Output values on channels 0 ... 7
QB x +1									Output values on channels 8 ... 15

Configuration mode DI8/DQ8

In DI8/DQ8 configuration mode, the address space is reduced by the fixed parameter assignment of the channels.

Table 2-156 Address space in the configuration mode DI8/DQ8

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Input values on channels 0 ... 7
Assignment in the process image output (PIQ)									
QB x									Output values on channels 8 ... 15

Configuration mode DIQ MIX

In DIQ MIX configuration mode, the address space is reduced by the fixed parameter assignment of the channels.

Table 2-157 Address space in the configuration mode DIQ MIX

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Input values on channels 1, 3, 5, 7, 9, 11, 13 and 15
Assignment in the process image output (PIQ)									
QB x									Output values on channels 0, 2, 4, 6, 8, 10, 12 and 14

Evaluating the value status

An additional 4 bytes are occupied in the input address space if you enable the value status for the digital input/digital output module. The value status of the inputs is assigned to the input bytes x + 2 and x + 3. The value status of the outputs is assigned to the input byte x + 4 and x + 5. This additional information provides information regarding the validity of the digital values or channel status.

Bit = 1: No error on channel.

Bit = 0: Error on channel.
If the channel is configured as input, this means:

- Short-circuit of an encoder supply to ground, or
- Parameter error or
- For channels 8 ... 15: Missing load voltage 2L+

If the channel is configured as output, this means:

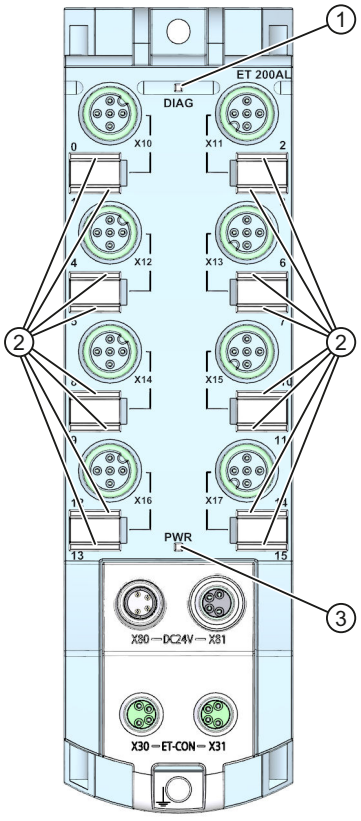
- Short-circuit of output to ground or
- Parameter error or
- For channels 8 ... 15: Missing load voltage 2L+

4.4 Interrupts/diagnostic alarms

4.4.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital input module / digital output module DIQ 16x24VDC/0.5A 8xM12.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 15) (green)
③ Load voltage 2L+ (PWR) (green)

Figure 2-77 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic reports can be found in chapter Diagnostics alarms (Page 29).

DIAG LED

Table 2-158 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-159 LED channel status display

LED channel status	Meaning
☐ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-160 Status display of the PWR LED

PWR LED	Meaning
☐ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

4.4.2 Interrupts

The digital input / digital output module DIQ 16x24VDC/0.5A 8xM12 in the configuration method DIQ supports diagnostic interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of an encoder supply to ground, or
- Short-circuit of an output to ground
- Load voltage 2L+ missing or too low
- Parameter assignment error

4.4.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the LED DIAG flashes red on the digital input/digital output module. You can read out the diagnostics alarms, for example, from the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-161 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short circuit[1]	1_H	Short-circuit encoder supply to ground	Eliminate the short-circuit
		Short-circuit of outputs to ground	
Parameter assignment error	10_H	• The module cannot evaluate parameters for the channel • Incorrect parameter assignment	Correct the parameter assignment.
Load voltage 2L+ missing[2]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Security event: Firmware has been successfully downloaded and activated for installation.[3]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[3]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 If a short-circuit of the encoder supply to ground is detected, the diagnostics alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.

2 If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostics alarm "Load voltage missing" is displayed

3 A diagnostics alarm is output for a signed firmware update.

NOTE

Channel type

The digital input/digital output module is always signaled as a mixed module (channel type "Input/Output") in the case of diagnostic events, even if you have configured the digital input/digital output module exclusively as an output or input module.

Counting

5

Counting function

Counting refers to the detection and summation of events. The respective counters of the module detect encoder signals and pulses and evaluate them accordingly, for example:

- For counting general piece goods up to a maximum limit
- For applications with recurring counting processes

You can control the counting processes with the digital inputs of the digital input / digital output module belonging to the counter. You can control the digital output belonging to the counter exactly to defined counter values via comparative results independently of the user program.

You can parameterize the behavior of the respective counter by means of the functions described below.

Counter limits

The counter values define the range of values of the counter value than can be used. The counter limits are configurable and can be modified during runtime using the user program. The maximum adjustable count limit amounts to 2147483647 (2^{31}-1). The maximum adjustable count limit amounts to -2147483648 (-2^{31}).
You can continue or stop counting (automatic gate stop) on violation of a counting limit At an overflow or underflow of the count value one event bit is respectively set in the feedback interface. The count value jumps to the respective other counting limit.

Start value

You can configure a start value within the counter limits. The start value can be modified during runtime with the user program.

Load value

In addition to the parameterization you can influence the counting behavior additionally via the control interface by means of the load value. Depending on the bit sequence of the load request (LD_SLOT) contained in the control byte you can load the load value (SLOT) as a current count value, start value, comparative value or count limit.

If you re-parameterize the module, loaded values are overwritten automatically. Therefore, if necessary, carry out the adjustment of the values via the control interface again after a re-parameterization.

Comparison value

You specify a comparison value that controls the associated count output independently of the user program.
The comparison value can be parameterized and can be changed with the user program during runtime.

Gate control

Together with the hardware gate the software gate forms the internal gate. The module only counts when the internal gate is open.
You control the HW gate externally via the digital inputs DI_4 and DI_6. You control the SW gate via the user program. You can activate and use the hardware gate in the 2xCount configuration method by using parameterization.

Counting direction

The counting direction is specified either by the direction of the respective counter or via the parameter assignment of the counter.
You control the counting direction via the digital inputs DI_5 and DI_7. You can activate and use the direction inputs in the 2xCount configuration method by using parameterization.

Overview of configuration methods

The following table shows a list of the channel properties for the configuration methods 2xCount and 4xCount.
You can count with DI_0 and DI_2 (configuration method 2xCount) or respectively with DI_0, DI_2, DI_4 and DI_6 (configuration method 4xCount).

Table 2-162 Configuration methods of the DIQ 16x24VDC/0.5A 8xM12

Property		**Configuration method**	
		2xCount (Page 33)	**4xCount** (Page 52)
Number of counters		2	4
Counter width, max. counting frequency		32 bits, 2 kHz	32 bits, 2 kHz
Counter inputs		Channels 0, 2	Channel 0, 2, 4, 6
Count outputs		Channel 1, 3	Channel 1, 3, 5, 7
Input for gate stop / start[1]		Channel 4, 6	-
Input for counting direction[1]		Channel 5, 7	-
Number of freely parameterizable channels		8	8
Parameterizable input delay[2]		0.05 ms .. 20 ms	0.05 ms .. 20 ms
Process data length	Inputs	14 bytes	26 bytes
	Outputs	14 bytes	26 bytes

1 = Can also be used as default digital inputs via the parameter assignment as "Digital input without function".

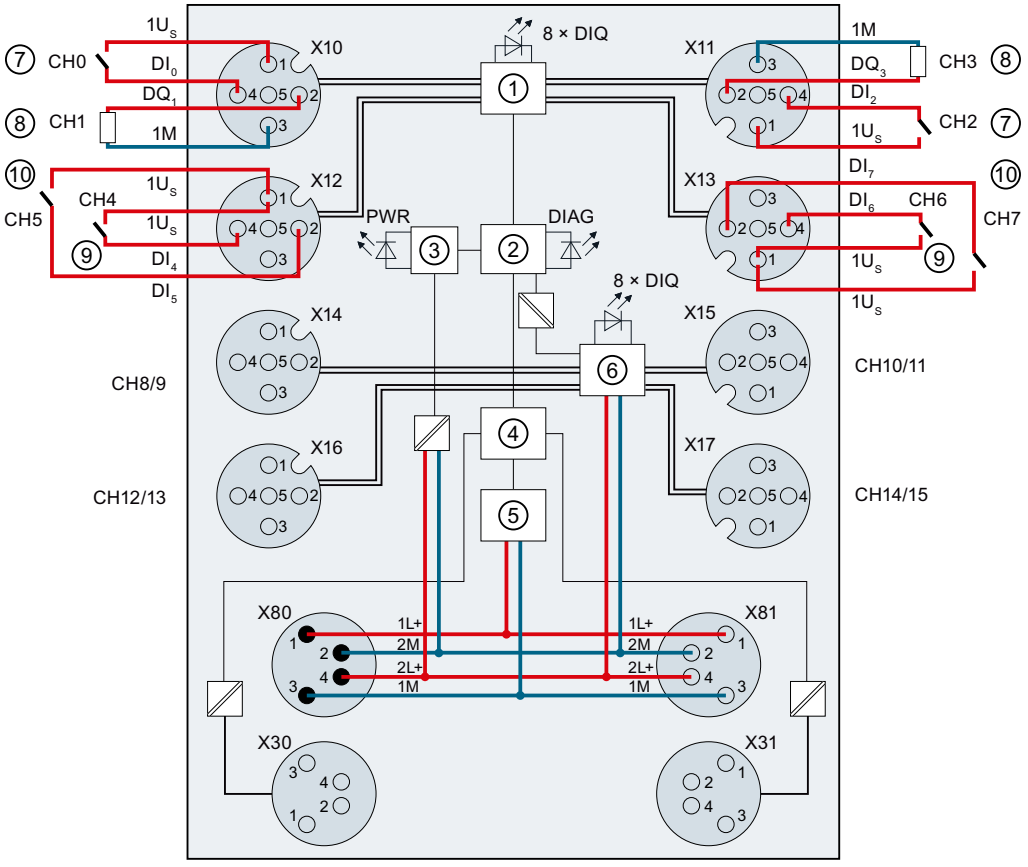
2 = Only values as of 1.6 ms can be parameterized as the input delay for Channels 8..15.

5.1 Configuration method 2xCount

5.1.1 Wiring

5.1.1.1 Terminal and block diagram

The following figure shows as an example the pin assignment of the counters in the configuration method Count (2xCount). Connection examples for allocating the freely parameterizable channels 8..15 are available in the section Configuration method DIQ, subsection Terminal and block diagram (Page 16).



①	DI/DQ circuit (1L+ non-switched)	X81	Loop-through of supply voltages
②	Microcontroller	X30	Infeed of the ET-Connection
③	Monitoring	X31	Loop-through of the ET-Connection
④	ET-Connection interface	1L+	Supply voltage 1L+ (non-switched)
⑤	Internal supply voltage	1M	Ground 1M (non-switched)
⑥	DI/DQ circuit (2L+ switched)	2L+	Load voltage 2L+ (switched)
⑦	Counting input counter	2M	Ground 2M (switched)
⑧	DQ for counters	1U$_S$	24 V encoder supply
⑨	Gate start/stop (level-controlled) or digital input without function	DIQ$_n$	Input/output signal

⑩	Counting direction or digital input without function	DIQ	Channel status LEDs (0 to 15) (green)
X10 to X17	Channels 0 to 15	DIAG	Diagnostic status LED (red/green)
X80	Infeed of supply voltages	PWR	LED supply voltage 2L+ (green)

Figure 2-78 Wiring and block diagram configuration method 2xCount

5.1.1.2 Pin assignment

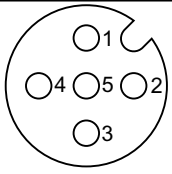
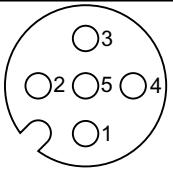
NOTE

Color coding
The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for counting channels and digital inputs / outputs

The table below shows the pin assignments of the 4 sockets for the connection of the counting channels.

Table 2-163 Pin assignment for counting channels

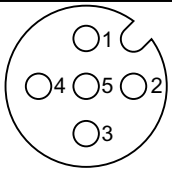
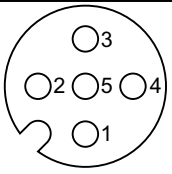
Pin	Assignment	Front view of the sockets	
	X10 to X13 - sockets for counting channels	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Count output for Counter 0: Connector X10 Counting output for Counter 1: Connector X11 Counting direction of Counter 0 or Input signal DI_5: Connector X12 Counting direction of Counter 1 or Input signal DI_7: Connector X13		
3	Ground 1M		
4	Count input for Counter 0: Connector X10 Count input for Counter 1: Connector X11 Counting direction of Counter 0 or Input signal DI_4: Connector X12 Counting direction of Counter 1 or Input signal DI_6: Connector X13		
5	Functional earth FE		

NOTICE

24 V encoder supply $1U_S$
Use only the 24 V encoder supply $1U_S$ provided by the digital input/digital output module to supply power to the encoder.

The table below shows the pin assignments of the 4 sockets for the connection of the digital inputs / digital outputs.

Table 2-164 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 - sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Input/output signal DIQ_9: Connector X14 Input/output signal DIQ_{11}: Connector X15 Input/output signal DIQ_{13}: Connector X16 Input/output signal DIQ_{15}: Connector X17		
3	Ground 2M		
4	Input/output signal DIQ_8: Connector X14 Input/output signal DIQ_{10}: Connector X15 Input/output signal DIQ_{12}: Connector X16 Input/output signal DIQ_{14}: Connector X17		
5	Functional earth FE		

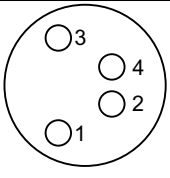
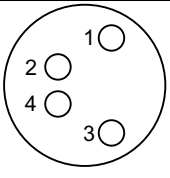
NOTICE

24 V encoder supply $2U_S$
Use only the 24 V encoder supply $2U_S$ provided by the digital input/digital output module to supply power to the encoder.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

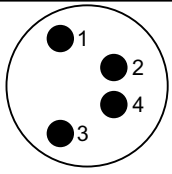
Table 2-165 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	**X31 socket (ET-Connection OUT)**		**X30**	**X31**
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

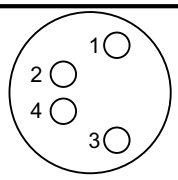
Table 2-166 Pin assignment of the supply voltage connector

Pin	Assignment X80 connector (POWER input)	Assignment of the core color of the power cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-167 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage

Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

5.1.2 Parameters/address space

5.1.2.1 Parameters

In the configuration method 2xCount of the digital input / digital output module DIQ 16x24VDC/0.5A 8xM12 the Channels 0 to 7 are used by the counting function. The Channels 8 to 15 can be parameterized freely.

The following table shows the general parameter of the module.

Table 2-168 General parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of encoder supply or of the output to ground)
Behavior at CPU/master STOP (8...15)	• Shut down • Keep last value • Output substitute value	Shut down	Module (digital outputs)

The following table shows the parameters of Counter 0 and Counter 1.

Table 2-169 Parameters of Counter 0 and Counter 1

Parameter	Value range	Default	Scope
Counting behavior Counter 0 (DI0), Counter 1 (DI2)			
Input delay DI	• 0.05 ms • 0.1 ms • 0.4 ms • 0.8 ms • 1.6 ms • 3.2 ms • 12.8 ms • 20 ms	0.05 ms	Counter
Counting direction[1]	• Forward • Backward	Forward	Counter
Edge selection	• On a rising edge • On a falling edge	On a rising edge	Counter
Behavior when a counting limit is exceeded	• Stop counting • Continue counting	Stop counting	Counter
Comparison value	-2147483648...21474836-47	10	Counter
Start value[2]	-2147483648...21474836-47	0	Counter
High count limit	-2147483648...21474836-47	2147483647	Counter

1 = Is ignored if DI5/DI7 is parameterized as the direction input.

2 = Cannot be parameterized with GSD file

Parameter	Value range	Default	Scope
Counter low limit[2]	-2147483648...21474836-47	0	Counter
Behavior Counter 0 (DQ1), Counter 1 (DQ3)			
Behavior DQ	• Count value between a comparison value and the high counting limit • Count value between a comparison value and the low counting limit	Count value between a comparison value and the high counting limit	Counter
Hardware interrupt DQ	• Inactive • Comparison event for DQ has occurred	Inactive	Counter
Behavior at CPU/master STOP for DQ	• Continue • Output substitute value	Continue	Counter
Substitute value DQ	• 0 • 1	0	Counter
Behavior Counter 0 (DI4), Counter 1 (DI6)			
Behavior DI	• Digital input without function • Gate start/stop (level-controlled)	Digital input without function	Counter
Behavior Counter 0 (DI5), Counter 1 (DI7)			
Behavior DI	• Digital input without function • Counting direction	Digital input without function	Counter
Input delay DI	• 0.05 ms • 0.1 ms • 0.4 ms • 0.8 ms • 1.6 ms • 3.2 ms • 12.8 ms • 20 ms	3.2 ms	Counter

1 = Is ignored if DI5/DI7 is parameterized as the direction input.

2 = Cannot be parameterized with GSD file

The table below shows the parameters of the freely assignable Channels 8...15.

Table 2-170 Parameter freely assignable Channels 8..15

Parameter	Value range	Default	Scope
Freely assignable channel	• DI • DQ	DI	Channel
Substitute value channel	• 0 • 1	0	Channel (digital outputs)
Input delay	• 1.6 ms • 3.2 ms • 12.8 ms • 20 ms	3.2 ms	Channel (digital inputs)

See also

Pin assignment (Page 34)

5.1.2.2 Explanation of the parameters

General parameters

Diagnostics: Missing load voltage 2L+
Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short circuit to ground
Enabling of the diagnostics, at short-circuit of an encoder supply or of an output to ground.

Behavior at CPU/master STOP (8...15)
With this parameter you set the reaction of the digital outputs of after a CPU/master STOP.
Behavior DQ at freely assignable Channels 8...15:

- Deactivate: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The digital output outputs a configured substitute value.

Parameter counting function

Input delay DI
This parameter can be used to suppress signal faults. Changes to the signal are only detected if they are constantly pending longer than the set input delay time.

NOTE

Influences the counting frequency
When setting the input delay take into account that the counting frequency possible is automatically reduced at higher values.
In order to achieve the maximum counting frequency of 2 kHz select an input delay smaller than 0.4 ms.

Counting direction
Use this parameter to select the direction in which counting is carried out:

- Forward
- Backward.

NOTE

If you have parameterized DI_5 or DI_7 as the direction input in the respective counter, this parameter is ineffective.

Edge selection
Use this parameter to select the edge that is counted:

- At rising edge:
  The respective counter counts all the rising edges at the counter input.
- At falling edge:
  The respective counter counts all the falling edges at the counter input.

NOTE
If you have parameterized DI_5 or DI_7 as the direction input in the respective counter and the counting direction changes in the process, the count edge is adapted automatically (contrary edges).

Behavior when a counting limit is exceeded
With this parameter you select the behavior when the high counting limit is violated in the upward direction or the low counting limit is violated in the downward direction:

- Stop counting:
  After a counting limit is violated, the internal gate is closed. This stops the counting process. The counter value is set to the opposite counting limit. To start the counting process again, you must close and reopen the SW gate.
- Continue counting:
  After a counting limit is violated, the counter value is set to the opposite counting limit and counting continues.

Comparison value
With this parameter you specify the comparison value.
The following applies:

- Low counting limit ≤ Comparison value ≤ High counting limit

Start value
With this parameter you specify the start value.
The following applies:

- Low counting limit ≤ Start value ≤ High counting limit

High counting limit
With this parameter you specify the high counting limit.
The following applies:

- Low counting limit < High counting limit ≤ 2147483647 (2^{31} - 1)

Low counting limit
With this parameter you specify the low counting limit.
The following applies:

- High counting limit > Low counting limit ≥ -2147483648 (-2^{31})

Behavior DQ
With the "Behavior DQ" you select the counter values at which the count output is set.
When the current count value fulfils the parameterized condition, the associated count output is set.
This means the signal state "1" is set at the count output when:

- Count value between a comparison value and the high counting limit:
  Comparison value ≤ Count value ≤ High counting limit

or

- Count value between a comparison value and the low counting limit:
  Low counting limit ≤ Count value ≤ Comparison value.

Hardware interrupt DQ
With this parameter you specify whether or not a hardware interrupt is generated by the event "Comparison event occurred for DQ".

Behavior at CPU/master STOP for DQ
With this parameter you set the reaction of the count output of a counter after a CPU/master STOP.
Behavior DQ:

- Continue: Signal state of the count output continues to be controlled by comparison conditions.
- Output substitute value: The count output outputs a configured substitute value.

NOTE

Count value at CPU/Master STOP
Independently of the selected reaction of the count output, the count value continues to change during a CPU/Master STOP depending on the input edge, counting continues.

Substitute value DQ
With this parameter you set the substitute value of the digital output of a counter if the setting "Output substitute value" has been selected at the parameter "Behavior at CPU/master STOP for DQ".

Behavior DI (gate control)
With this parameter you select whether a counting function is assigned to the digital input or whether this functions like a standard digital input:

- Gate start/stop:
  The digital input influences the internal gate of Counter 0 or Counter 1. Signal "1" at the digital input opens the HW gate for the counter. Signal "0" at the digital input closes the HW gate for the counter.
- Digital input without function:
  No counting function is assigned to the digital input. It functions like a standard digital input.

Behavior DI (direction input)
With this parameter you select whether a counting function is assigned to the digital input or whether this functions like a standard digital input:

- Counting direction:
  The digital input reverses the counting direction at Counter 0 or Counter 1, in order to adjust it to the process. With signal "0" at the digital input, the counter forwards. With signal "1" at the digital input, the counter counts backwards.
- Digital input without function:
  No counting function is assigned to the digital input. It functions like a standard digital input.

Parameter freely assignable Channels 8..15

Freely assignable channel
With this parameter, you set whether the channel is to be operated as an input or output.

Input delay channel
This parameter can be used to suppress signal interference. Changes to the signal are only detected if they are constantly pending longer than the set input delay time.

Substitute value channel
With this parameter, you set substitute values for the digital outputs.

See also

Assignment of the feedback interface (Page 45)

5.1.2.3 Assignment of the control interface

The user program uses the control interface to influence the behavior of the counters and the channels 8...15 of the module parameterized as an output.
The figure below shows the address assignment of the module in the process image output in the configuration method 2xCount.
At Counter 0 x stands for the output byte QB 2 in this case, at Counter 1 you add 6 bytes to this output byte.
When you assign a different start address to the digital input/digital output module, the byte sequence changes correspondingly.

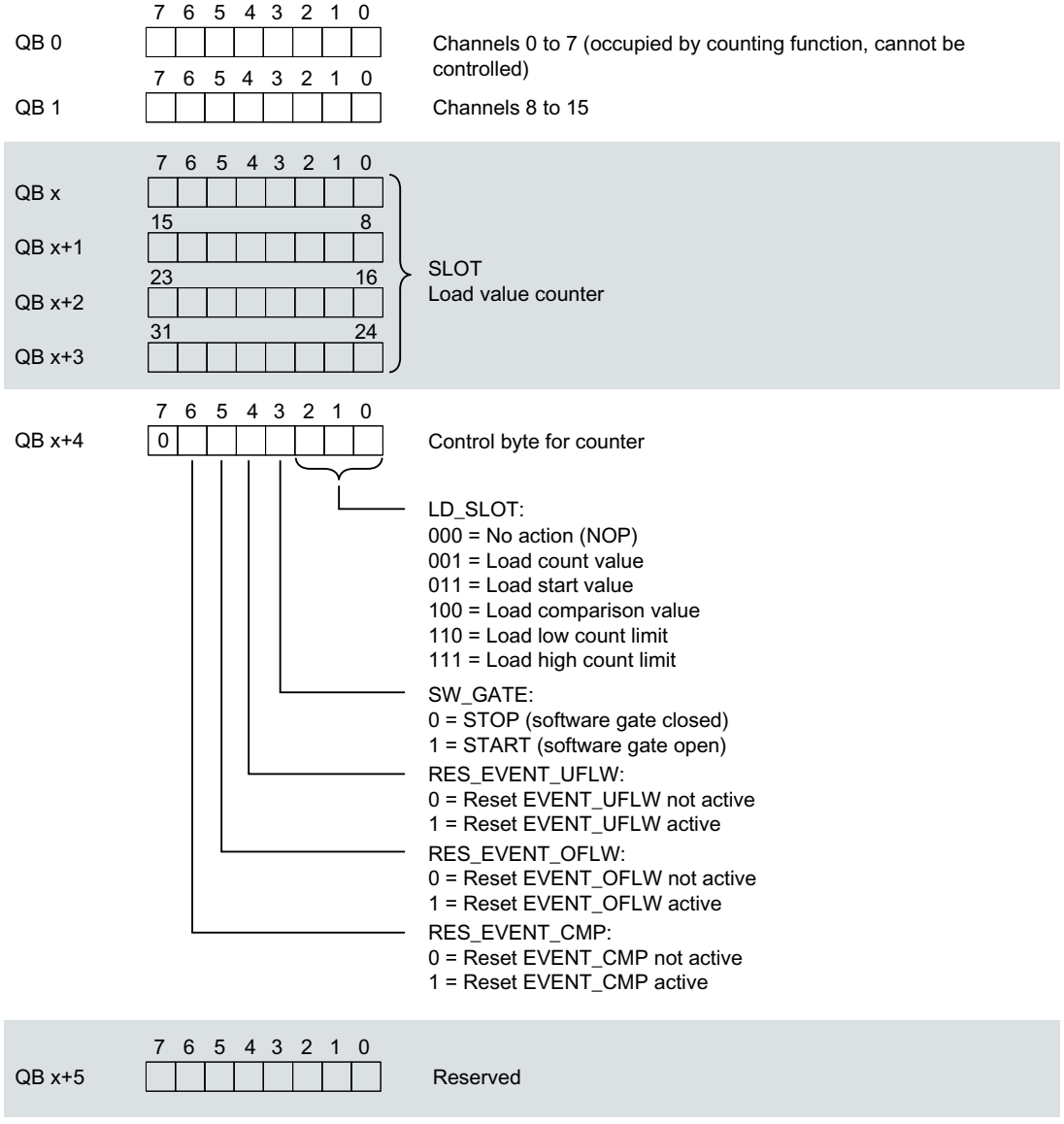


Figure 2-79 Address space control interface configuration method 2xCount

NOTE

Parameter assignment of the channels

The corresponding values in the output data do not trigger any reaction for all the channels that are used as an input.

You cannot control the count outputs via the user program.

5.1.2.4 Explanations on the control interface

Table 2-171 Explanations on the control bits

Control bit	Explanations
SLOT	You specify the load value for the respective counter in these bytes. Through the load request LD_SLOT you load the predefined value into the counter.
LD_SLOT	With this load request you control for which value of the counter the value specified in SLOT is to be loaded. The counter carries out the respective action as soon as LD_SLOT changes. If you have entered the load request LD_SLOT = 011_B open the SW gate, every counting process begins with the value defined in the SLOT as the start value. If you have entered a different load request and open the SW gate, counting is continued with the current count value at every start of the counting process. Both cases also apply at a parameterized HW gate as long as and until the SW gate is closed.
SW_GATE	With this bit you open and close the SW gate of the respective counter. Together with the hardware gate the software gate forms the internal gate. The module only counts when the internal gate is open. 0 means: Software gate closed 1 means: Software gate open
RES_EVENT_UFLW	With this bit you trigger the resetting of the stored event in the feedback bit EVENT_UFLW for the respective counter.
RES_EVENT_OFLW	With this bit you trigger the resetting of the stored event in the feedback bit EVENT_OFLW for the respective counter.
RES_EVENT_CMP	With this bit you trigger the resetting of the stored event in the feedback bit EVENT_CMP for the respective counter.

5.1.2.5 Assignment of the feedback interface

Feedback interface

The user program receives current values and status information from the module via the feedback interface.
The figure below shows the address assignment of the module in the process image input in the configuration method 2xCount.
At Counter 0 x stands for the input byte IB 2 in this case, at Counter 1 you add 6 bytes to this output byte.
When you assign a different start address to the digital input/digital output module, the byte sequence changes correspondingly.

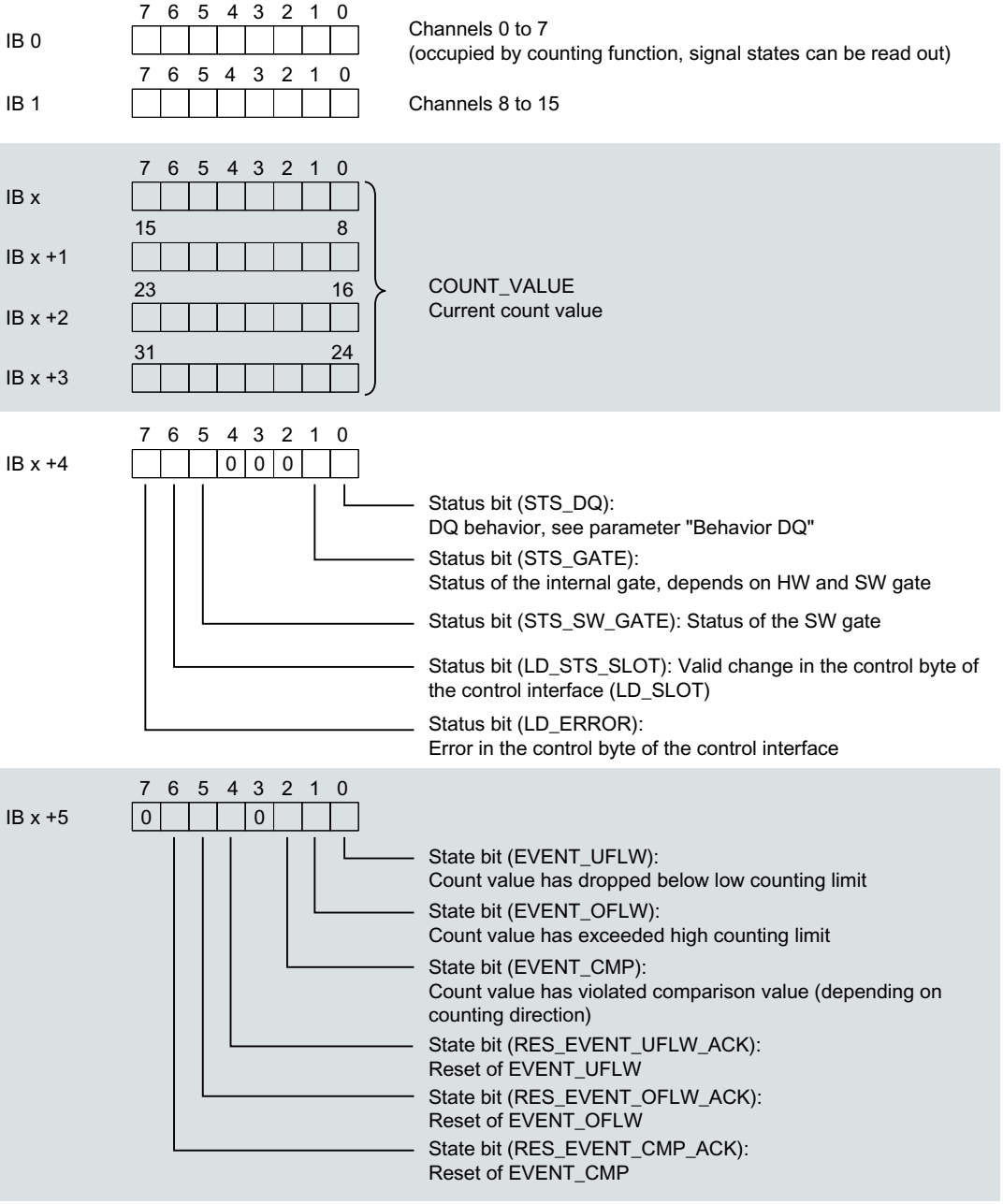


Figure 2-80 Address space feedback interface configuration method 2xCount

5.1.2.6 Explanations for the feedback interface

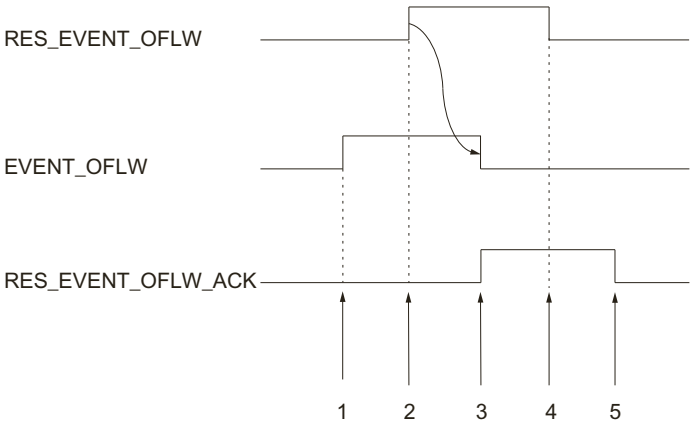
Table 2-172 Explanations for the feedback bits

Feedback bit	Explanations
COUNT_VALUE	This value supplies the current count value for the respective counter.
STS_DQ	This bit returns the current signal state of the count output.
STS_GATE	Together with the hardware gate the software gate forms the internal gate. This bit shows the state of the internal gate for the respective counter. The module only counts when the internal gate is open. 0 means: Internal gate closed / counter does not count 1 means: internal Tor open / counter counts **Note:** After a POWER OFF / ON or a change in the parameterization, all the values of the changed counter are transferred again to the module. In the process the internal gate of the respective counter is closed and the count value is set to the start value. Close and open the respective SW gate to restart the counting process. **Note:** When the PROFIBUS interface model is used, the CPU/Master automatically generates the "rising edge" signal after disconnection/reconnection of the communications. This continues the counting process.
STS_SW_GATE	This bit shows the status of the software gate. 0 means: Software gate closed 1 means: Software gate open
LD_STS_SLOT	This bit indicates through a status change (toggling) for the respective counter that loading of the control interface has been carried out successfully.
LD_ERROR	This bit indicates for the respective counter that an error has occurred during loading of the control interface. The load value was not accepted. One of the following conditions is fulfilled: • Low counting limit > Count value • Low counting limit > Start value • Low counting limit > Comparison value • Count value > High counting limit • Start value > High counting limit • Comparison value > High counting limit • Low counting limit ≥ High counting limit • No valid load request in LD_SLOT
EVENT_UFLW	This bit shows for the respective counter whether an underflow (value dropped below the low count limit) has occurred. You reset the state by acknowledging with RES_EVENT_UFLW.
EVENT_OFLW	This bit shows for the respective counter whether an overflow (value exceeded the high count limit) has occurred. You reset the state by acknowledging with RES_EVENT_OFLW.
EVENT_CMP	This bit shows for the respective counter whether a comparison event with the comparison value has occurred. You reset the state by acknowledging with RES_EVENT_CMP. The EVENT_CMP bit is not set if the count value is set to the start value.
RES_EVENT_UFLW_ACK	This bit shows for the respective counter whether the resetting of the event bit EVENT_UFLW is active.
RES_EVENT_OFLW_ACK	This bit shows for the respective counter whether the resetting of the event bit EVENT_OFLW is active.
RES_EVENT_CMP_ACK	This bit shows for the respective counter whether the resetting of the event bit EVENT_CMP is active.

Complete acknowledgment principle

Storing bits are acknowledged in accordance with the complete acknowledgment principle.

The figure below shows an example for the course of the complete acknowledgment principle at an overflow:



① The feedback bit EVENT_OFLW is set as a storing event at an overflow bit.
② The set the control bit RES_EVENT_OFLW in order to initiate resetting of EVENT_OFLW.
③ The feedback bit RES_EVENT_OFLW_ACK is set when the resetting of EVENT_OFLW has been recognized.
④ You reset the control bit RES_EVENT_OFLW .
⑤ The feedback bit RES_EVENT_OFLW_ACK is reset.

Figure 2-81 Acknowledgment principle

NOTE
When you have initiated the resetting of an event bit, you have to wait for the respective feedback bit. You can initiate a further reset subsequently.

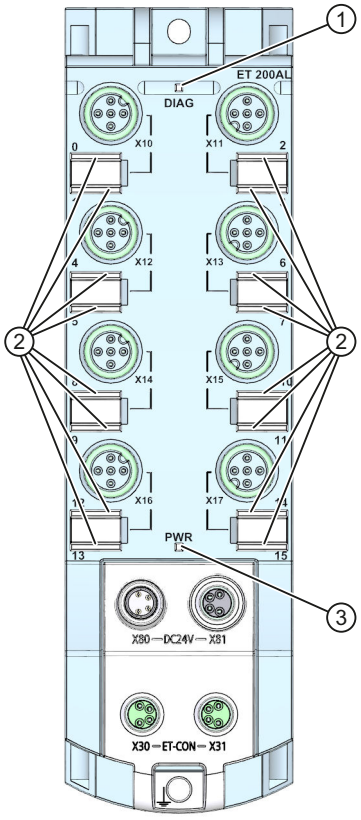
NOTE
An opening of the SW gate or HW gate (0-1 transition) resets all event bits.

5.1.3 Interrupts/diagnostic alarms

5.1.3.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital input module / digital output module DIQ 16x24VDC/0.5A 8xM12.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 15) (green)
③ Load voltage 2L+ (PWR) (green)

Figure 2-82 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic reports can be found in chapter Diagnostics alarms (Page 51).

DIAG LED

Table 2-173 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
On	Module parameters assigned and no module diagnostics
Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-174 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

PWR LED

Table 2-175 Status display of the PWR LED

PWR LED	Meaning
Off	Load voltage 2L+ is missing or too low
On	Load voltage 2L+ present

5.1.3.2 Interrupts

The digital input / digital output module DIQ 16x24VDC/0.5A 8xM12 in the configuration method 2xCount supports diagnostic and hardware interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of an encoder supply to ground, or
- Short-circuit of an output to ground
- Load voltage 2L+ missing or too low
- Parameter assignment error

Hardware interrupt

The module generates a hardware interrupt at the following event:

- Comparison event occurred for DQ

For detailed information on the error event, refer to the hardware interrupt organization block with the "RALRM" instruction (read additional interrupt info) and to the STEP 7 online help.

The module channel that triggered the hardware interrupt is entered in the start information of the organization block. The figure below shows the assignment to the bits of the local data double word 8.

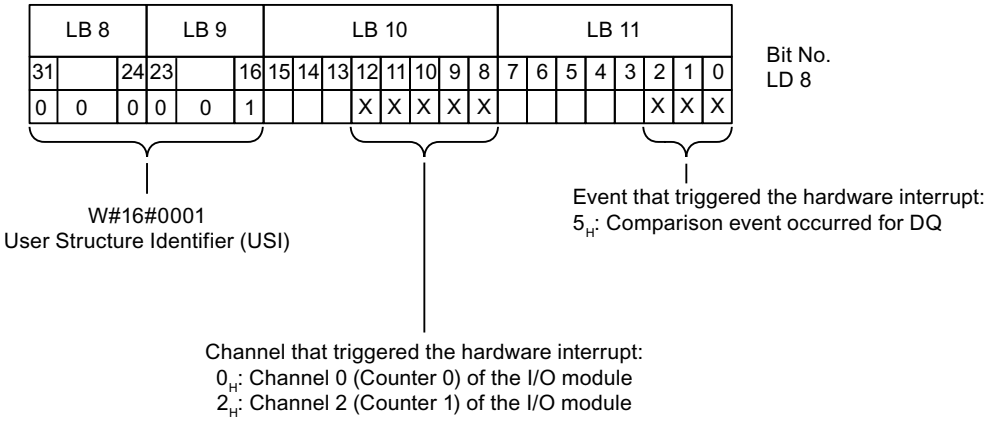


Figure 2-83 Start information of the organization block in the configuration method 2xCount

5.1.3.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the LED DIAG flashes red on the digital input/digital output module.
You can read out the diagnostics alarms, for example, from the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-176 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short circuit[1]	1_H	Short-circuit of an encoder supply to ground	• Eliminate the short-circuit
		Short-circuit of an output to ground	
Parameter assignment error	10_H	Module parameter assignment is faulty	Correction of the parameter assignment
Load voltage 2L+ missing[2]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Hardware interrupt lost	16_H	At least one hardware interrupt could not be signaled because too many hardware interrupts are pending.	Correct the program or the process

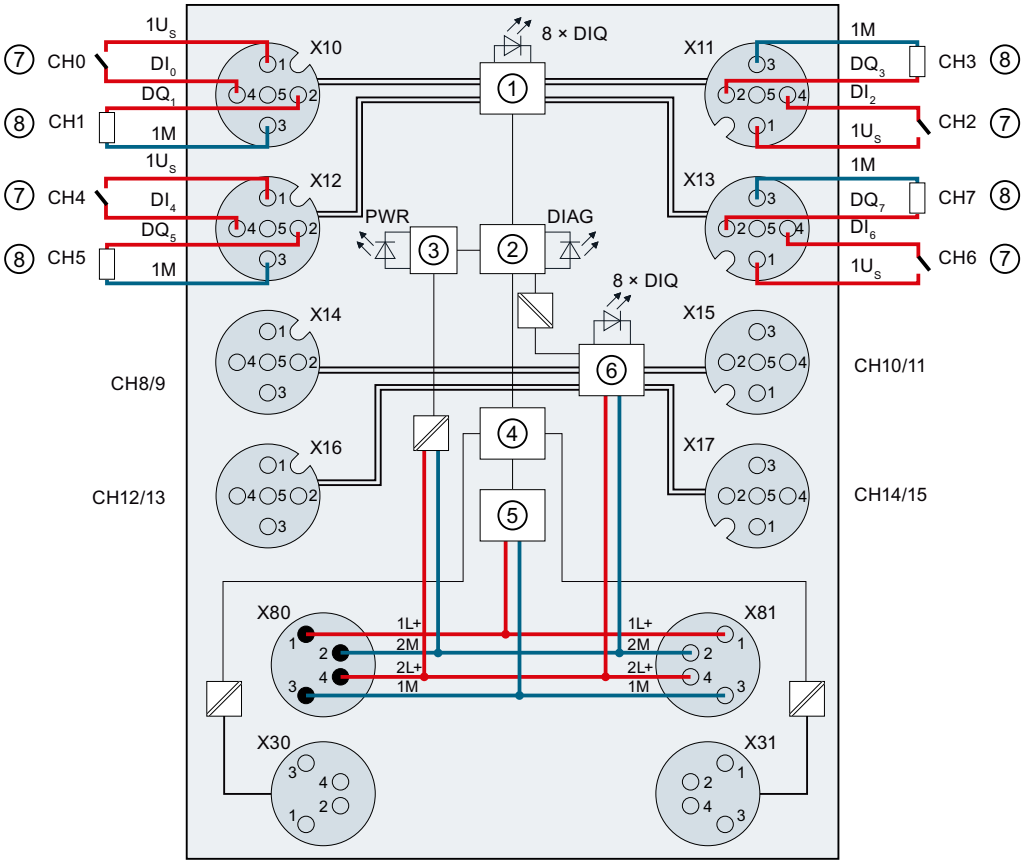
[1] If a short-circuit of the encoder supply to ground is detected, the diagnostic alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.
[2] If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostic alarm "Load voltage missing" is displayed.

5.2 Configuration method 4xCount

5.2.1 Wiring

5.2.1.1 Terminal and block diagram

The following figure shows as an example the pin assignment of the counters in the configuration method Count (4xCount). Connection examples for allocating the freely parameterizable channels 8..15 are available in the section Configuration method DIQ, subsection Terminal and block diagram (Page 16).



①	DI/DQ circuit (1L+ non-switched)	X30	Infeed of the ET-Connection
②	Microcontroller	X31	Loop-through of the ET-Connection
③	Monitoring	1L+	Supply voltage 1L+ (non-switched)
④	ET-Connection interface	1M	Ground 1M (non-switched)
⑤	Internal supply voltage	2L+	Load voltage 2L+ (switched)
⑥	DI/DQ circuit (2L+ switched)	2M	Ground 2M (switched)
⑦	Counting input counter	1U$_S$	24 V encoder supply
⑧	DQ for counters	DIQ$_n$	Input/output signal
X10 to X17	Channels 0 to 15	DIQ	Channel status LEDs (0 to 15) (green)
X80	Infeed of supply voltages	DIAG	Diagnostic status LED (red/green)
X81	Loop-through of supply voltages	PWR	LED supply voltage 2L+ (green)

Figure 2-84 Wiring and block diagram configuration method 4xCount

5.2.1.2 Pin assignment

NOTE

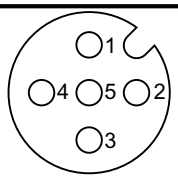
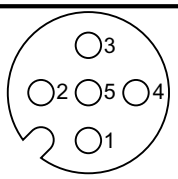
Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for counting channels and digital inputs / outputs

The table below shows the pin assignments of the 4 sockets for the connection of the counting channels.

Table 2-177 Pin assignment for counting channels

Pin	Assignment	Front view of the sockets	
	X10 to X13 - sockets for counting channels	**X10, X12**	**X11, X13**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Count output for Counter 0: Connector X10 Counting output for Counter 1: Connector X11 Counting output for Counter 2: Connector X12 Counting output for Counter 3: Connector X13		
3	Ground 1M		
4	Count input for Counter 0: Connector X10 Count input for Counter 1: Connector X11 Count input for Counter 2: Connector X12 Count input for Counter 3: Connector X13		
5	Functional earth FE		

NOTICE

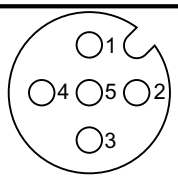
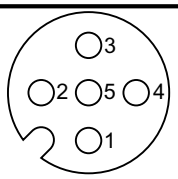
24 V encoder supply $1U_S$

Use only the 24 V encoder supply $1U_S$ provided by the digital input/digital output module to supply power to the encoder.

The table below shows the pin assignments of the 4 sockets for the connection of the digital inputs / digital outputs.

Table 2-178 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X14 to X17 - sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Input/output signal DIQ_9: Connector X14 Input/output signal DIQ_{11}: Connector X15 Input/output signal DIQ_{13}: Connector X16 Input/output signal DIQ_{15}: Connector X17		

Pin	Assignment	Front view of the sockets	
	X14 to X17 - sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
3	Ground 2M		
4	Input/output signal DIQ_8: Connector X14 Input/output signal DIQ_{10}: Connector X15 Input/output signal DIQ_{12}: Connector X16 Input/output signal DIQ_{14}: Connector X17		
5	Functional earth FE		

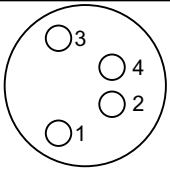
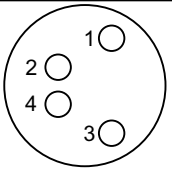
NOTICE

24 V encoder supply $2U_S$
Use only the 24 V encoder supplies $2U_S$ provided by the digital input/digital output module to supply power to the encoder.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

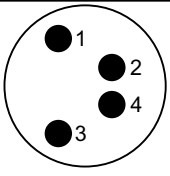
Table 2-179 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	**X31 socket (ET-Connection OUT)**		**X30**	**X31**
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield-ing	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

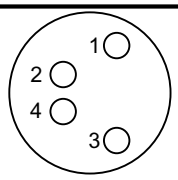
Table 2-180 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the core color of the power cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-181 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the ET-Connection connectors and the connectors for the supply voltage can destroy the module.

5.2.2 Parameters/address space

5.2.2.1 Parameters

In the configuration method 4xCount of the digital input / digital output module DIQ 16x24VDC/0.5A 8xM12 the Channels 0 to 7 are used by the counting function. The Channels 8 to 15 can be parameterized freely.

The following table shows the general parameter of the module.

Table 2-182 General parameters

Parameters	Value range	Default	Scope
Diagnostics: Missing load voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit to ground	• Disable • Enable	Disable	Module (Short-circuit of the encoder supply or of the output to ground)
Behavior at CPU/master STOP (8...15)	• Shut down • Keep last value • Output substitute value	Shut down	Module (digital outputs)

The table below shows the parameters of Counter 0 to Counter 3.

Table 2-183 Parameters of Counter 0 to Counter 3

Parameter	Value range	Default	Scope
Counting behavior Counter 0 (DI0), Counter 1 (DI2), Counter 2 (DI4) and Counter 3 (DI6)			
Input delay DI	• 0.05 ms • 0.1 ms • 0.4 ms • 0.8 ms • 1.6 ms • 3.2 ms • 12.8 ms • 20 ms	0.05 ms	Counter
Counting direction	• Forward • Backward	Forward	Counter
Edge selection	• On a rising edge • On a falling edge	On a rising edge	Counter
Behavior when a counting limit is exceeded	• Stop counting • Continue counting	Stop counting	Counter
Comparison value	-2147483648...2147483-647	10	Counter
Start value[1]	-2147483648...2147483-647	0	Counter
High count limit	-2147483648...2147483-647	2147483647	Counter
Low counting limit[1]	-2147483648...2147483-647	0	Counter
Behavior Counter 0 (DQ1), Counter 1 (DQ3), Counter 2 (DQ5), Counter 3 (DQ7)			
Behavior DQ	• Count value between a comparison value and the high counting limit • Count value between a comparison value and the low counting limit	Count value between a comparison value and the high counting limit	Counter
Hardware interrupt DQ	• Inactive • Comparison event for DQ has occurred	Inactive	Counter
Behavior at CPU/master STOP for DQ	• Continue • Output substitute value	Continue	Counter
Substitute value DQ	• 0 • 1	0	Counter

1 = Cannot be parameterized with GSD file

The table below shows the parameters of the freely assignable Channels 8...15.

Table 2-184 Parameter freely assignable Channels 8..15

Parameter	Value range	Default	Scope
Freely assignable channel	• DI • DQ	DI	Channel
Substitute value channel	• 0 • 1	0	Channel (digital outputs)
Input delay	• 1.6 ms • 3.2 ms • 12.8 ms • 20 ms	3.2 ms	Channel (digital inputs)

See also

Pin assignment (Page 53)

5.2.2.2 Explanation of the parameters

General parameters

Diagnostics: Missing load voltage 2L+
Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short circuit to ground
Enabling of the diagnostics, at short-circuit of an encoder supply or of an output to ground.

Behavior at CPU/master STOP (8...15)
With this parameter you set the reaction of the digital outputs of after a CPU/master STOP.
Behavior DQ at freely assignable Channels 8...15:

- Deactivate: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The digital output outputs a configured substitute value.

Parameter counting function

Input delay DI
This parameter can be used to suppress signal faults. Changes to the signal are only detected if they are constantly pending longer than the set input delay time.

NOTE

Influences the counting frequency
When setting the input delay take into account that the counting frequency possible is automatically reduced at higher values.
In order to achieve the maximum counting frequency of 2 kHz select an input delay smaller than 0.4 ms.

Counting direction
Use this parameter to select the direction in which counting is carried out:

- Forward
- Backward.

Edge selection
Use this parameter to select the edge that is counted:

- At rising edge:
  The respective counter counts all the rising edges at the counter input.
- At falling edge:
  The respective counter counts all the falling edges at the counter input.

Behavior when a counting limit is exceeded
With this parameter you select the behavior when the high counting limit is violated in the upward direction or the low counting limit is violated in the downward direction:

- Stop counting:
  After a counting limit is violated, the internal gate is closed. This stops the counting process. The counter value is set to the opposite counting limit. To start the counting process again, you must close and reopen the SW gate.
- Continue counting:
  After a counting limit is violated, the counter value is set to the opposite counting limit and counting continues.

Comparison value
With this parameter you specify the comparison value.
The following applies:

- Low counting limit ≤ Comparison value ≤ High counting limit

Start value
With this parameter you specify the start value.
The following applies:

- Low counting limit ≤ Start value ≤ High counting limit

High counting limit
With this parameter you specify the high counting limit.
The following applies:

- Low counting limit < High counting limit ≤ 2147483647 (2^{31} - 1)

Low counting limit
With this parameter you specify the low counting limit.
The following applies:

- High counting limit > Low counting limit ≥ -2147483648 (-2^{31})

Behavior DQ
With the "Behavior DQ" you select the counter values at which the count output is set. When the current count value fulfils the parameterized condition, the associated count output is set.
This means the signal state "1" is set at the count output when:

- Count value between a comparison value and the high counting limit:
  Comparison value ≤ Count value ≤ High counting limit

or

- Count value between a comparison value and the low counting limit:
  Low counting limit ≤ Count value ≤ Comparison value.

Hardware interrupt DQ
With this parameter you specify whether or not a hardware interrupt is generated by the event "Comparison event occurred for DQ".

Behavior at CPU/master STOP for DQ
With this parameter you set the reaction of the count output of a counter after a CPU/master

STOP.
Behavior DQ:

- Continue: Signal state of the count output continues to be controlled by comparison conditions.
- Output substitute value: The count output outputs a configured substitute value.

NOTE

Count value at CPU/Master STOP
Independently of the selected reaction of the count output, the count value continues to change during a CPU/Master STOP depending on the input edge, counting continues.

Substitute value DQ
With this parameter you set the substitute value of the digital output of a counter if the setting "Output substitute value" has been selected at the parameter "Behavior at CPU/master STOP for DQ".

Parameter freely assignable Channels 8..15

Freely assignable channel
With this parameter, you set whether the channel is to be operated as an input or output.

Input delay channel
This parameter can be used to suppress signal interference. Changes to the signal are only detected if they are constantly pending longer than the set input delay time.

Substitute value channel
With this parameter, you set substitute values for the digital outputs.

5.2.2.3 Assignment of the control interface

The user program uses the control interface to influence the behavior of the counters and the channels 8...15 of the module parameterized as an output.
The figure below shows the address assignment of the module in the process image output in the configuration method 4xCount.
At Counter 0 x stands for the output byte QB 2 in this case, at Counters 1 to 3 you add 6 bytes, 12 bytes and 18 bytes respectively to this output byte.
When you assign a different start address to the digital input/digital output module, the byte sequence changes correspondingly.

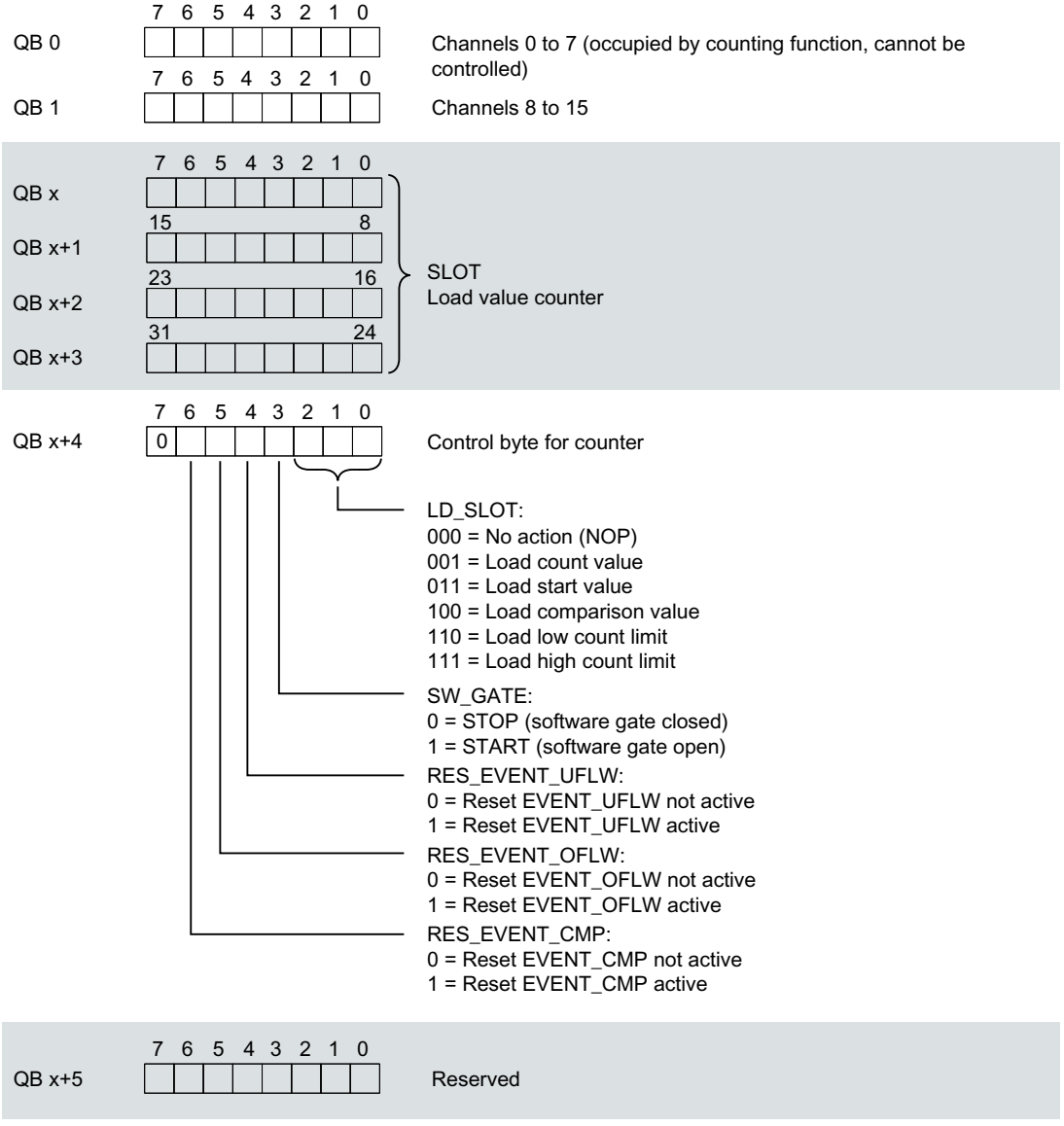


Figure 2-85 Address space control interface configuration method 4xCount

NOTE

Parameter assignment of the channels

The corresponding values in the output data do not trigger any reaction for all the channels that are used as an input.

You cannot control the count outputs via the user program.

5.2.2.4 Explanations on the control interface

Table 2-185 Explanations on the control bits

Control bit	Explanations
SLOT	You specify the load value for the respective counter in these bytes. Through the load request LD_SLOT you load the predefined value into the counter.
LD_SLOT	With this load request you control for which value of the counter the value specified in SLOT is to be loaded. The counter carries out the respective action as soon as LD_SLOT changes. If you have entered the load request LD_SLOT = 011_B open the SW gate, every counting process begins with the value defined in the SLOT as the start value. If you have entered a different load request and open the SW gate, counting is continued with the current count value at every start of the counting process. Both cases apply as long as and until the SW gate is closed.
SW_GATE	With this bit you open and close the SW gate of the respective counter. The module only counts when the software gate is open. 0 means: Software gate closed 1 means: Software gate open
RES_EVENT_UFLW	With this bit you trigger the resetting of the stored event in the feedback bit EVENT_UFLW for the respective counter.
RES_EVENT_OFLW	With this bit you trigger the resetting of the stored event in the feedback bit EVENT_OFLW for the respective counter.
RES_EVENT_CMP	With this bit you trigger the resetting of the stored event in the feedback bit EVENT_CMP for the respective counter.

5.2.2.5 Assignment of the feedback interface

Feedback interface

The user program receives current values and status information from the module via the feedback interface.
The figure below shows the address assignment of the module in the process image input in the configuration method 4xCount.
At Counter 0 x stands for the input byte IB 2 in this case, at Counters 1 to 3 you add 6 bytes, 12 bytes and 18 bytes respectively to this input byte.
When you assign a different start address to the digital input/digital output module, the byte sequence changes correspondingly.

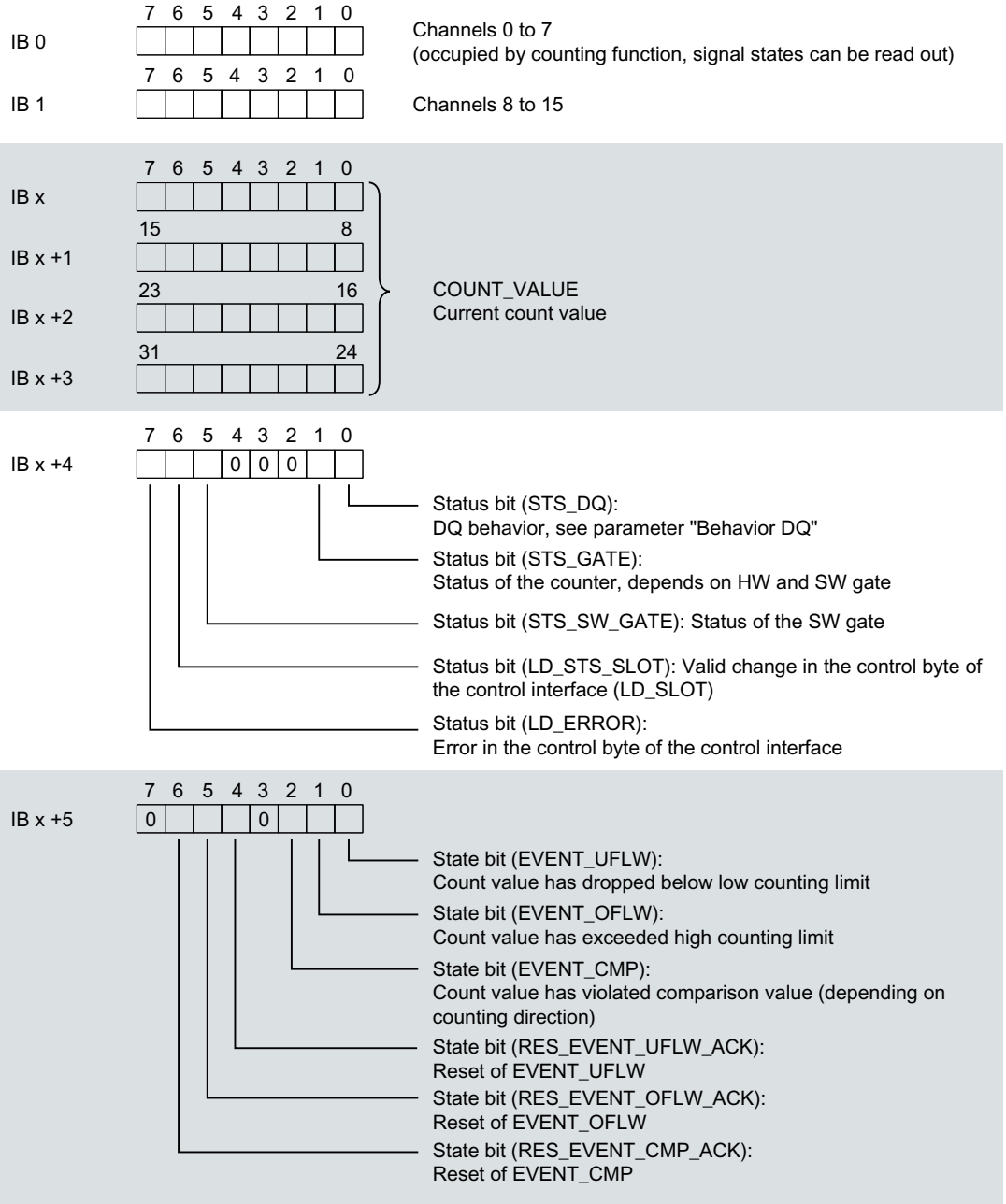


Figure 2-86 Address space feedback interface configuration method 4xCount

5.2.2.6 Explanations for the feedback interface

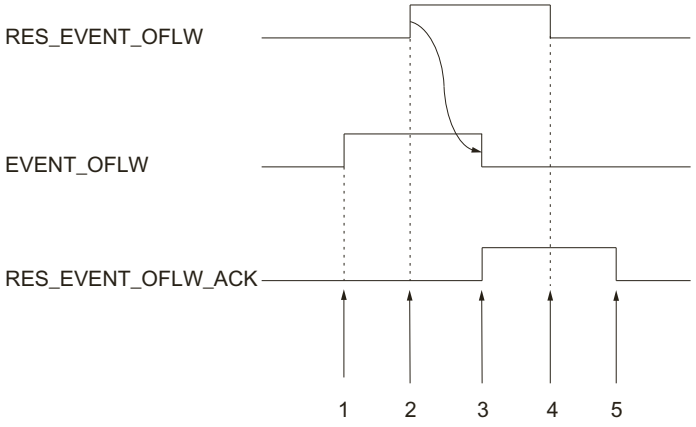
Table 2-186 Explanations for the feedback bits

Feedback bit	Explanations
COUNT_VALUE	This value supplies the current count value for the respective counter.
STS_DQ	This bit returns the current signal state of the count output.
STS_GATE	This bit shows the state of the internal gate for the respective counter. The module only counts when the internal gate is open. 0 means: Internal gate closed / counter does not count 1 means: internal Tor open / counter counts **Note:** After a POWER OFF / ON or a change in the parameterization, all the values of the changed counter are transferred again to the module. In the process the internal gate of the respective counter is closed and the count value is set to the start value. Close and open the respective SW gate to restart the counting process. **Note:** When the PROFIBUS interface model is used, the CPU/Master automatically generates the "rising edge" signal after disconnection/reconnection of the communications. This continues the counting process.
STS_SW_GATE	This bit shows the status of the software gate. 0 means: Software gate closed 1 means: Software gate open
LD_STS_SLOT	This bit indicates through a status change (toggling) for the respective counter that loading of the control interface has been carried out successfully.
LD_ERROR	This bit indicates for the respective counter that an error has occurred during loading of the control interface. The load value was not accepted. One of the following conditions is fulfilled: • Low counting limit > Count value • Low counting limit > Start value • Low counting limit > Comparison value • Count value > High counting limit • Start value > High counting limit • Comparison value > High counting limit • Low counting limit ≥ High counting limit • No valid load request in LD_SLOT
EVENT_UFLW	This bit shows for the respective counter whether an underflow (value dropped below the low count limit) has occurred. You reset the state by acknowledging with RES_EVENT_UFLW.
EVENT_OFLW	This bit shows for the respective counter whether an overflow (value exceeded the high count limit) has occurred. You reset the state by acknowledging with RES_EVENT_OFLW.
EVENT_CMP	This bit shows for the respective counter whether a comparison event with the comparison value has occurred. You reset the state by acknowledging with RES_EVENT_CMP. The EVENT_CMP bit is not set if the count value is set to the start value.
RES_EVENT_UFLW_ACK	This bit shows for the respective counter whether the resetting of the event bit EVENT_UFLW is active.
RES_EVENT_OFLW_ACK	This bit shows for the respective counter whether the resetting of the event bit EVENT_OFLW is active.
RES_EVENT_CMP_ACK	This bit shows for the respective counter whether the resetting of the event bit EVENT_CMP is active.

Complete acknowledgment principle

Storing bits are acknowledged in accordance with the complete acknowledgment principle.

The figure below shows an example for the course of the complete acknowledgment principle at an overflow:



① The feedback bit EVENT_OFLW is set as a storing event at an overflow bit.
② The set the control bit RES_EVENT_OFLW in order to initiate resetting of EVENT_OFLW.
③ The feedback bit RES_EVENT_OFLW_ACK is set when the resetting of EVENT_OFLW has been recognized.
④ You reset the control bit RES_EVENT_OFLW .
⑤ The feedback bit RES_EVENT_OFLW_ACK is reset.

Figure 2-87 Acknowledgment principle

NOTE
When you have initiated the resetting of an event bit, you have to wait for the respective feedback bit. You can initiate a further reset subsequently.

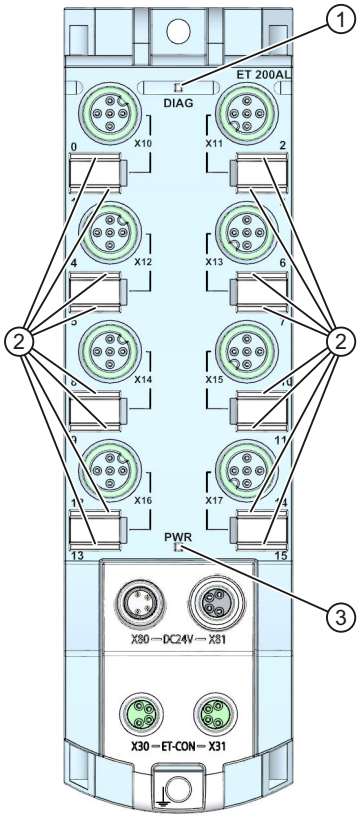
NOTE
An opening of the SW gate or HW gate (0-1 transition) resets all event bits.

5.2.3 Interrupts/diagnostic alarms

5.2.3.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the digital input module / digital output module DIQ 16x24VDC/0.5A 8xM12.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 15) (green)
③ Load voltage 2L+ (PWR) (green)

Figure 2-88 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic reports can be found in chapter Diagnostics alarms (Page 68).

DIAG LED

Table 2-187 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED channel status

Table 2-188 LED channel status display

LED channel status	Meaning
☐ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-189 Status display of the PWR LED

PWR LED	Meaning
☐ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.2.3.2 Interrupts

The digital input / digital output module DIQ 16x24VDC/0.5A 8xM12 in the configuration method 4xCount supports diagnostic and hardware interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of an encoder supply to ground, or
- Short-circuit of an output to ground
- Load voltage 2L+ missing or too low
- Parameter assignment error

Hardware interrupt

The module generates a hardware interrupt at the following event:

- Comparison event occurred for DQ

For detailed information on the error event, refer to the hardware interrupt organization block with the "RALRM" instruction (read additional interrupt info) and to the STEP 7 online help.

The module channel that triggered the hardware interrupt is entered in the start information of the organization block. The figure below shows the assignment to the bits of the local data double word 8.

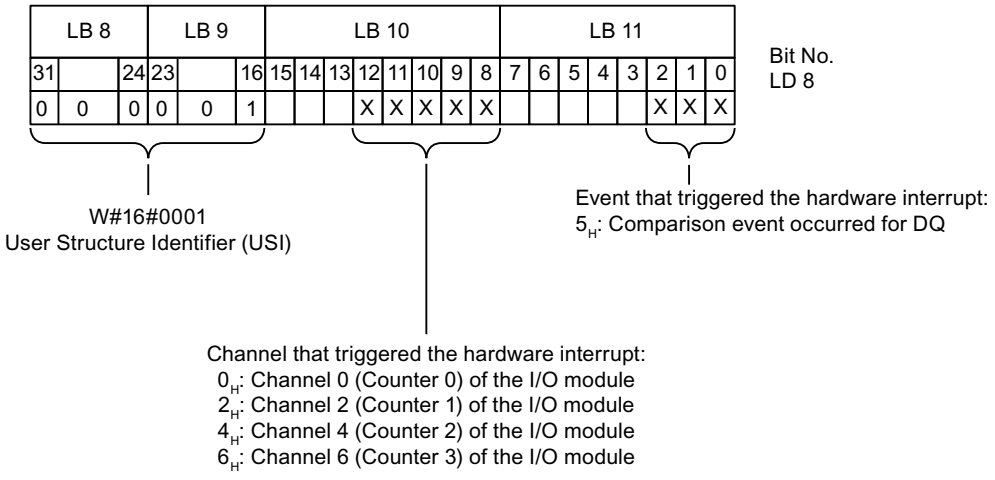


Figure 2-89 Start information of the organization block in the configuration method 4xCount

5.2.3.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the LED DIAG flashes red on the digital input/digital output module.
You can read out the diagnostics alarms, for example, from the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-190 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short circuit[1]	1_H	Short-circuit of an encoder supply to ground	• Eliminate the short-circuit
		Short-circuit of an output to ground	
Parameter assignment error	10_H	Module parameter assignment is faulty	Correction of the parameter assignment
Load voltage 2L+ missing[2]	11_H	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
Hardware interrupt lost	16_H	At least one hardware interrupt could not be signaled because too many hardware interrupts are pending.	Correct the program or the process

[1] If a short-circuit of the encoder supply to ground is detected, the diagnostic alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.
[2] If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostic alarm "Load voltage missing" is displayed.

5.3 Examples of counting

In this section, you will find examples of the behavior of the counter and how you can specify this behavior. You specify the properties of the counter in the parameter assignment.

The boundary conditions apply for the following examples:

- You set the bit SW_GATE to "1", the counting process starts.
- If you reset the bit SW_GATE before a count limit is reached, the counting process stops. Set the bit SW_GATE to restart the counting process.
  The value with which the counting process starts again depends on the content of the control interface.

These conditions only apply if you do not use a HW gate (configuration method 2xCount).

Behavior DQ - Count value between a comparison value and the high counting limit (counting direction forward)

The following section shows the behavior of the count output with the parameter assignment "Set output DQ: Count value between a comparison value and the high counting limit".

The count output is set to "1" if the current values lies between the comparison value and the high count limit.
You can optionally enable a hardware interrupt through the parameterization. This is generated with the rising edge of the count output.

The following figure shows an example of the signal state of the count output depending on the parameterization mentioned above.

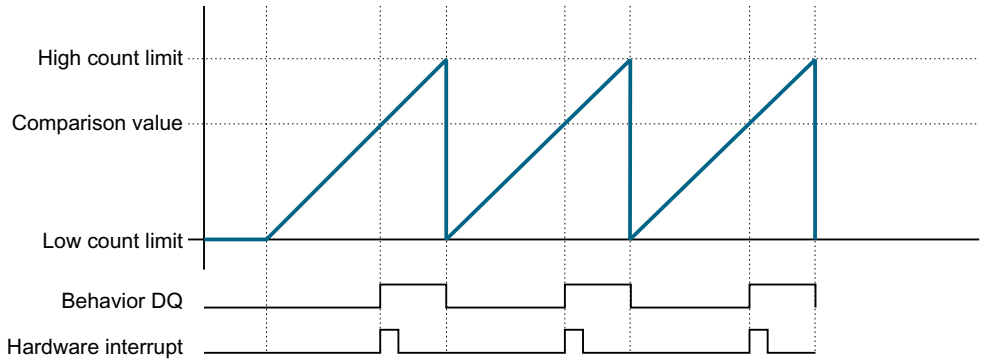


Figure 2-90 Behavior DQ and hardware interrupt

Behavior DQ - count value between a comparison value and the low counting limit (counting direction backward)

The following section shows the behavior of the count output with the parameter assignment "Set output DQ: Between a comparison value and the low counting limit".

The count output is set to "1" if the current values lies between the comparison value and the low count limit.
You can optionally enable a hardware interrupt through the parameterization. This is generated with the rising edge of the count output.

The following figure shows an example of the signal state of the count output depending on the parameterization mentioned above.

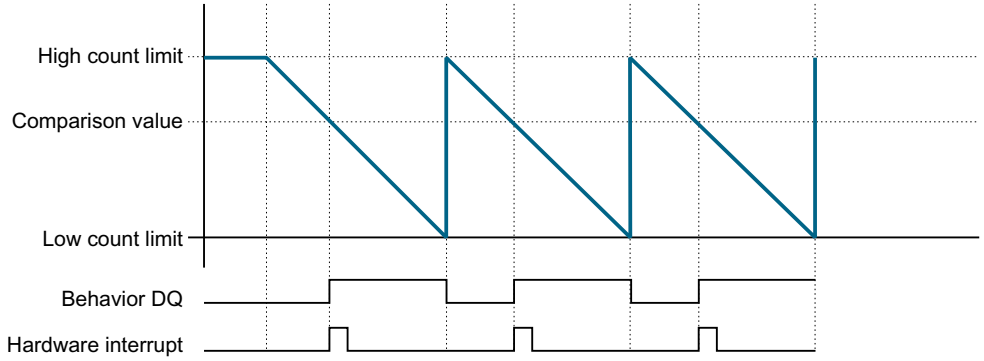


Figure 2-91 Behavior DQ and hardware interrupt

Start and stop the counting process via the gate control (counting direction forward, configuration method 2xCount)

The following section shows the behavior of the counter depending on the control input at the parameterization "Behavior DI: Gate control in combination with "Behavior when a counting limit is exceeded: Stop counting".

If you set the HW gate to "1" via the control input, the counting process is started. If you set the HW gate to "0", the counting process stops.
Note that the counting process also stops if you close the SW gate while the HW gate is

opened.
HW gate ans SW gate together form the internal gate. The module only counts when the internal gate is open.

The following figure shows an example of the behavior of the counter at gate control with the principle of stopping counting when a counting limit is exceeded.

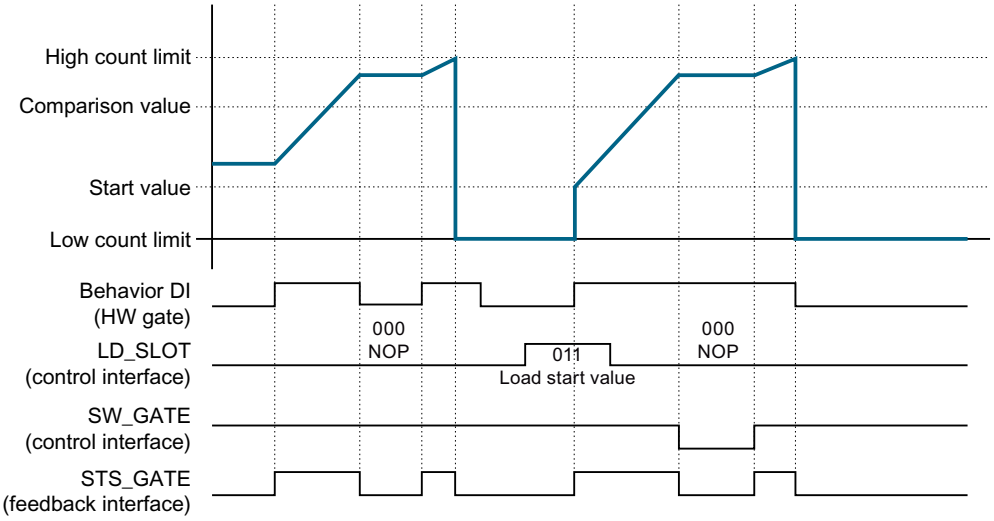


Figure 2-92 Gate control and principle: Stop counting

Change counting direction via count input and stop counting (configuration method 2xCount)

The following section shows the behavior of the counter depending on the direction input at the parameterization "Behavior DI: Counting direction" in combination with "Behavior when a counting limit is exceeded: Stop counting".
If you have parameterized the digital input of a counter as a direction input, you can change the counting direction via corresponding signals at this input.

Irrespective of the parameterization the counter always forward id the signal state "0" is set at direction input or, respectively backward if the signal state is "1".
If you change the counting direction via a signal change at the direction input, the edge detection (rising / falling edge) is also switched over.

The following figure shows an example of the behavior of the counter at a change in the counting direction with the principle of stopping counting when a counting limit is exceeded.

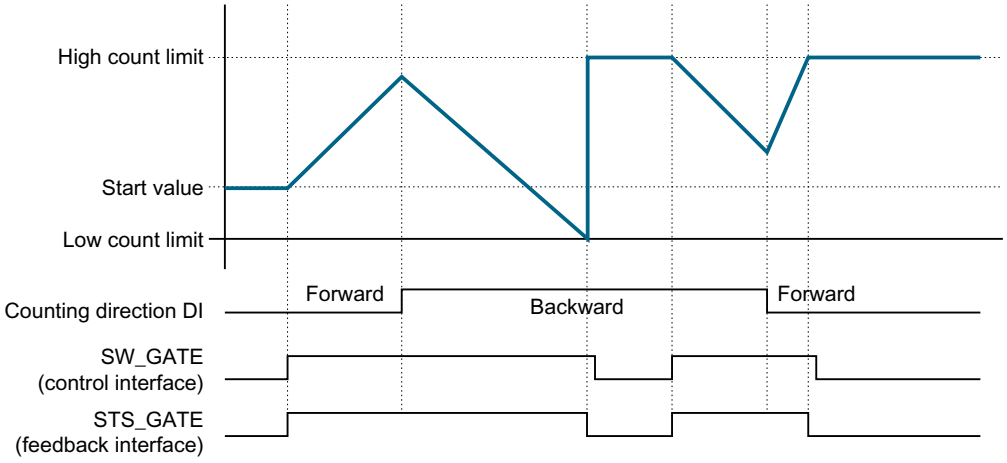


Figure 2-93 Changing the counting direction and principle: Stop counting

Behavior when a counting limit is exceeded - Stop counting (counting direction forward)

The following section describes the effects of the parameter "Behavior when a counting limit is exceeded: Stop counting" in the counting direction forward. To control the counter, the bits of the control byte of the control interface are used, see the configuration method 2xCount, section Assignment of the control interface (Page 43) and configuration method 4xCount, section Assignment of the control interface (Page 60).

You have entered the bit string 011 in the control byte of the control interface. This bit string loads the value defined in the load value (SLOT) as the start value of the counter via the load request (LD_SLOT).

After the high counting limit is violated, counting is aborted (counting stops) and the counted value jumps to the low counting limit.
The bit STS_GATE is reset in the feedback interface, the bit EVENT_OFLW is set.

The following figure shows an example of the principle of stopping counting when the high count limit is exceeded, counting direction forward.
The behavior "Behavior DQ" is set to "Count value between a comparison value and the high counting limit".

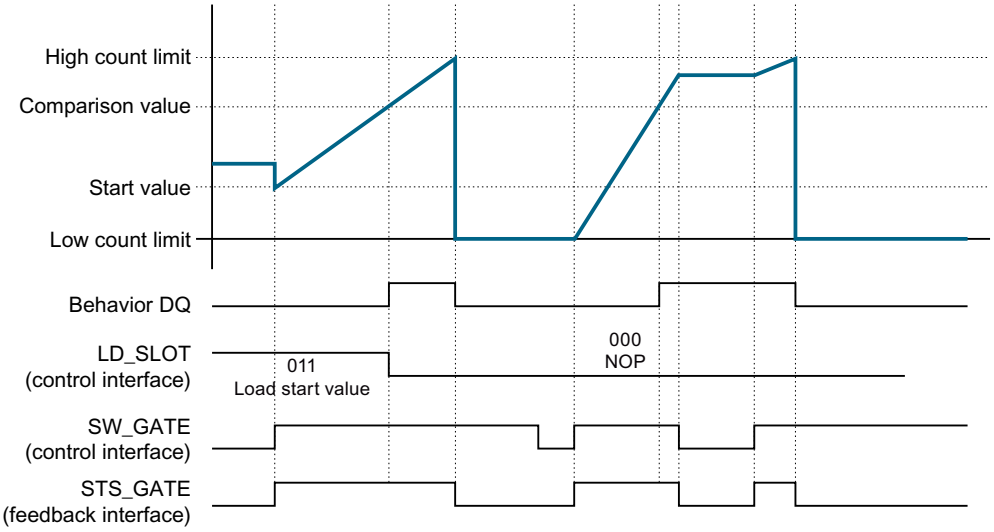


Figure 2-94 Principle: Stop counting (counting direction forward)

You can find additional information on the behavior of the counter at an overflow in the section Explanations for the feedback interface (Page 46).

Behavior when a counting limit is exceeded - Continue counting (counting direction backward)

The following section describes the effects of the parameter "Behavior when a counting limit is exceeded: Continue counting". To control the counter, the bits of the control byte of the control interface are used, see the configuration method 2xCount, section Assignment of the control interface (Page 43) and configuration method 4xCount, section Assignment of the control interface (Page 60).

After the low counting limit is underpassed, the counted value jumps to the high counting limit and counting is continued.
The bit STS_GATE is **not** reset when a count limit is exceeded.

The following figure shows an example of the principle of stopping counting when the low count limit is exceeded, counting direction backward.
The behavior "Behavior DQ" is set to "Count value between a comparison value and the high counting limit".

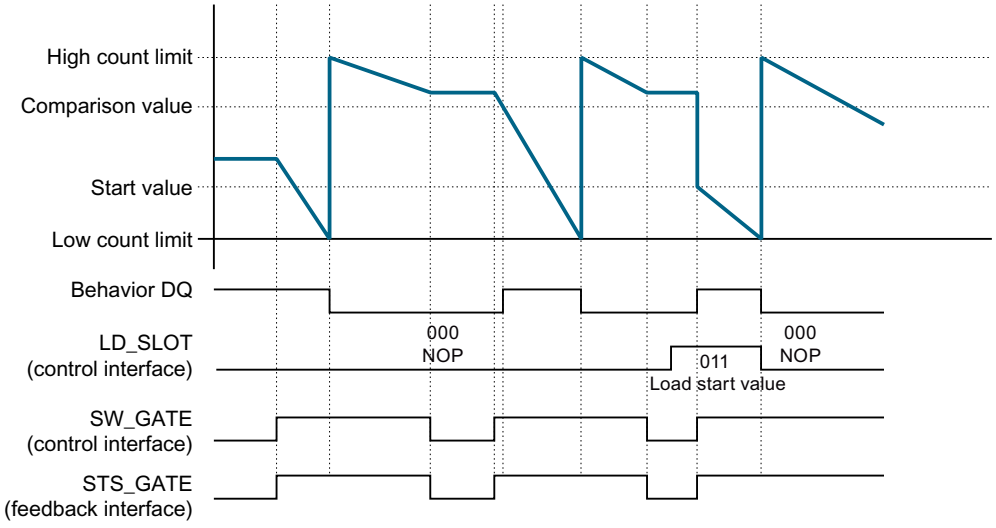


Figure 2-95 Principle: Continue counting (counting direction backward)

Reference

You will find general information on the counting function in the section Counting (Page 31).
Further information about the pin assignment, parameters, control and feedback interface, etc. is available in the sections Configuration method 2xCount (Page 33) and Configuration method 4xCount (Page 52).

Technical specifications

6

Technical specifications of the DIQ 16x24VDC/0.5A 8xM12 digital input/digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7143-5AH00-0BA0/td?dl=en).

Article number	6ES7143-5AH00-0BA0
General information	
Product type designation	DIQ 16x24VDC/0.5A
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V14 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 Hotfix 7 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Operating mode	
• DI	Yes
• Counter	Yes
• DQ	Yes
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up

Article number	6ES7143-5AH00-0BA0
Input current	
Current consumption (rated value)	60 mA
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	8
24 V encoder supply	
• Short-circuit protection	Yes; Per load voltage, electronic
• Output current, max.	1.4 A; Total current of all encoders, max. 0.7 A per load voltage
Power loss	
Power loss, typ.	4 W
Digital inputs	
Number of digital inputs	16; Parameterizable as DIQ
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	16
Digital input functions, parameterizable	
• Freely usable digital input	Yes
• Counter	Yes
– Number, max.	4
– Counting frequency, max.	2 kHz
– Counting width	32 bit; Incl. sign
– Counting direction up/down	Yes
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– parameterizable	Yes
– at "0" to "1", min.	0.05 ms; 1.6 ms for channels 8 through 15
– at "0" to "1", max.	20 ms
– at "1" to "0", min.	0.05 ms; 1.6 ms for channels 8 through 15
– at "1" to "0", max.	20 ms
for technological functions	
– parameterizable	Yes
Cable length	
• unshielded, max.	30 m

Article number	6ES7143-5AH00-0BA0
Digital outputs	
Number of digital outputs	16; Parameterizable as DIQ
• in groups of	8; 2 load groups for 8 outputs each
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	0.7 A
Limitation of inductive shutdown voltage to	L+ (-53 V)
Digital output functions, parameterizable	
• Switching tripped by comparison values	Yes
• Freely usable digital output	Yes
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per group, max.	4 A
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Outputs to M; encoder supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes

Article number	6ES7143-5AH00-0BA0
Potential separation channels	
• between the channels, in groups of	8
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No; 8 channels are non-isolated and 8 channels are isolated from supply voltage 1L+
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	No
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	195 g

PROFIenergy

7

7.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the digital input/digital output module with counting function is explained in the following sections.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

7.2 Behavior of the digital inputs

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-191 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] There are two encoder supplies, $1U_S$ for Channels 0 to 7 and $2U_S$ for Channels 8 to 15. At a "Pause" the supplies can only be switched off if no channel is configured in PE_MODE_PROCEED.

7.3 Behavior of the digital outputs

Display

The channel status LEDs are directly affected by the signal level at the socket.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-192 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

7.4 Behavior of the digital inputs of the counters

Display

The channel status LEDs are directly influenced by the signal level at the socket.
If the encoder supply is switched off, this causes the channel status LEDs to also switch off.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the "Short-circuit" alarms.
- During the "pause", error detection of "Short circuit" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

NOTE

Channels of a counter

All the channels that belong to a counter must have the same PROFIenergy behavior.
If substitute value behavior is parameterized, this also has to be the same for all channels of a counter.
If the PROFIenergy behavior is not the same for all the channels of a counter, the module rejects the PROFIenergy parameterization.
Further information on the assignment of the counting channels for the configuration method 2xCount is available in the section Pin assignment (Page 34), for the configuration method 4xCount in the section Pin assignment (Page 53).

Mode parameter

The following table shows the "Mode" parameter.

Table 2-193 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	The counter functions as in the normal count mode. The count output depends on the count value.
	1_D: PE_MODE_SHUTDOWN	The count value is no loner updated. The count output is set to 0.
	3_D: PE_MODE_LAST_VALUE	The count value is no longer updated (the input does not supply any edges). The count output contains the last value, since the count is no longer updated.
	4_D: PE_MODE_SUBST_VALUE	The count value is no longer updated (the input does not supply any edges). The count output is set to the parameterized substitute value, irrespective of the count value.

Dimension drawing

A

The figure below shows the dimension drawing of the DIQ 16x24VDC/0.5A 8xM12 digital input/digital output module in front and side views.

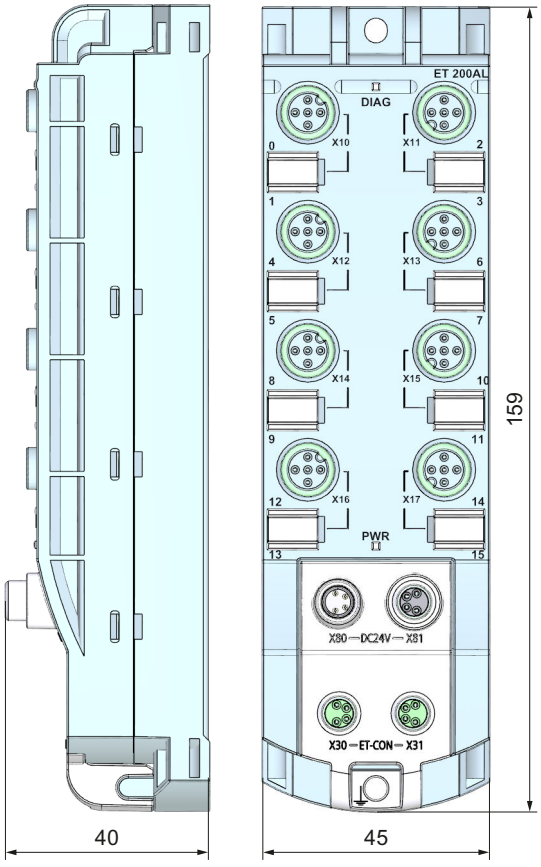


Figure 2-96 Dimension drawing

Parameter data record

B

B.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Module parameter length = 14_D ($0000\ 1110_B$)							

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

3 The following applies only to the configuration of the channel as a DI. For the channels 0 ... 7, you can parameterize one of the 8 different input delay values.

4 The following applies only to the configuration of the channel as a DI. For channels 8 ... 15, you can parameterize a value starting at 1.6 ms from the 4 different input delay values.

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2...5	**Parameter**							
2	Reserved[1]				Response at CPU/master STOP[2]	Diagnostics: Short-circuit to ground	Diagnostics: Missing load voltage 2L+	Reserved[1]
					00_B: Shut down 10_B: Keep last value 11_B: Output substitute value	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	
3	Configuration method channel 7	Configuration method channel 6	Configuration method channel 5	Configuration method channel 4	Configuration mode channel 3	Configuration mode channel 2	Configuration mode channel 1	Configuration mode channel 0
	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ
4	Configuration mode channel 15	Configuration mode channel 14	Configuration mode channel 13	Configuration mode channel 12	Configuration mode channel 11	Configuration mode channel 10	Configuration mode channel 9	Configuration mode channel 8
	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ	0_B: DI 1_B: DQ
5	Substitute value channel 7[2]	Substitute value channel 6[2]	Substitute value channel 5[2]	Substitute value channel 4[2]	Substitute value channel 3[2]	Substitute value channel 2[2]	Substitute value channel 1[2]	Substitute value channel 0[2]
	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1
6	Substitute value channel 15[2]	Substitute value channel 14[2]	Substitute value channel 13[2]	Substitute value channel 12[2]	Substitute value channel 11[2]	Substitute value channel 10[2]	Substitute value channel 9[2]	Substitute value channel 8[2]
	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1	0_B: 0 1_B: 1
7	Input delay channel 1[3]				Input delay channel 0[3]			
	0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
8	Input delay channel 3[3]				Input delay channel 2[3]			

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

3 The following applies only to the configuration of the channel as a DI. For the channels 0 ... 7, you can parameterize one of the 8 different input delay values.

4 The following applies only to the configuration of the channel as a DI. For channels 8 ... 15, you can parameterize a value starting at 1.6 ms from the 4 different input delay values.

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
8	0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
9	Input delay channel 5[3]				Input delay channel 4[3]			
	0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
10	Input delay channel 7[3]				Input delay channel 6[3]			
	0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0000_B: 0.05 ms 0001_B: 0.1 ms 0011_B: 0.4 ms 0100_B: 0.8 ms 0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
11	Input delay channel 9[4]				Input delay channel 8[4]			
	0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
12	Input delay channel 11[4]				Input delay channel 10[4]			
	0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
13	Input delay channel 13[4]				Input delay channel 12[4]			
	0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
14	Input delay channel 15[4]				Input delay channel 14[4]			
	0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms				0101_B: 1.6 ms 0110_B: 3.2 ms 1001_B: 12.8 ms 1010_B: 20 ms			
15	Reserved[1]							

1 Reserved bits must be set to 0

2 The following applies only to the configuration of the channel as a DQ

3 The following applies only to the configuration of the channel as a DI. For the channels 0 ... 7, you can parameterize one of the 8 different input delay values.

4 The following applies only to the configuration of the channel as a DI. For channels 8 ... 15, you can parameterize a value starting at 1.6 ms from the 4 different input delay values.

B.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 29) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-194 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	Byte 1	Byte 2	Byte 3			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
Analog input module AI 4xU/I/RTD 4xM12 (6ES7144-5KD00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostics alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Representation of analog values B

Parameter data record C

10/2024
A5E32350124-AH

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 14
4.2 Pin assignment 16

5 Parameters/address space 20

5.1 Measurement types and measuring ranges 20
5.2 Parameters 20
5.3 Explanation of the parameters 24
5.4 Address space 27

6 Interrupts/diagnostics alarms 29

6.1 Status and error displays 29
6.2 Interrupts 30
6.3 Diagnostics alarms 33

7 Technical specifications 36

8 PROFIenergy 41

8.1 Pause function 41
8.2 Response of the analog input module 42

A Dimension drawing 43

B Representation of analog values 44
B.1 Representation of analog values in voltage measuring ranges 44
B.2 Representation of analog values in current measuring ranges 44
B.3 Representation of analog values for resistance-based sensors 45
B.4 Representation of analog values for resistance thermometer 45

C Parameter data record 47
C.1 Structure of data record 128 for the module parameter assignment 47
C.2 Error transferring the data record 50

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7144-5KD00-0BA0

View of the module

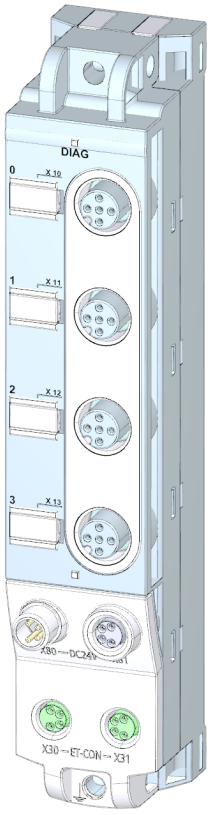


Figure 2-97 View of the analog input module AI 4xU/I/RTD 4xM12

Properties

The module has the following technical properties:

- 4 analog inputs
- M12 sockets for connection of sensors
- Measurement type can be set for each channel:
  - Voltage
  - Current (2-/4-wire transducers)
  - Resistance (2-/3-wire connection)
  - Resistance thermometer (RTD) (2-/3-wire connection)
- Resolution 16-bit
- Dimensions 30 x 159 mm
- Configurable diagnostics can be set for each channel
- Hardware interrupt on limit violation can be set per channel (two high and two low limits per channel)

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

NOTE

Process values during startup
As long as no parameters have been received by the I/O module, the I/O module returns the process value $7FFF_H$.

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

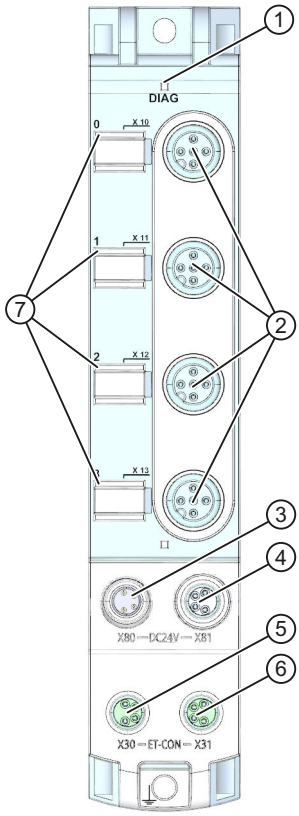
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the analog input module AI 4xU/I/RTD 4xM12.



① DIAG: LED display for the diagnostic status
② X10 to X13: Sockets for the input signal
③ X80: Connector for infeed of the supply voltage (POWER input)
④ X81: Socket for loop-through of the supply voltage (POWER output)
⑤ X30: Socket for ET-Connection IN
⑥ X31: Socket for ET-Connection OUT
⑦ LED displays 0 to 3 for the channel status

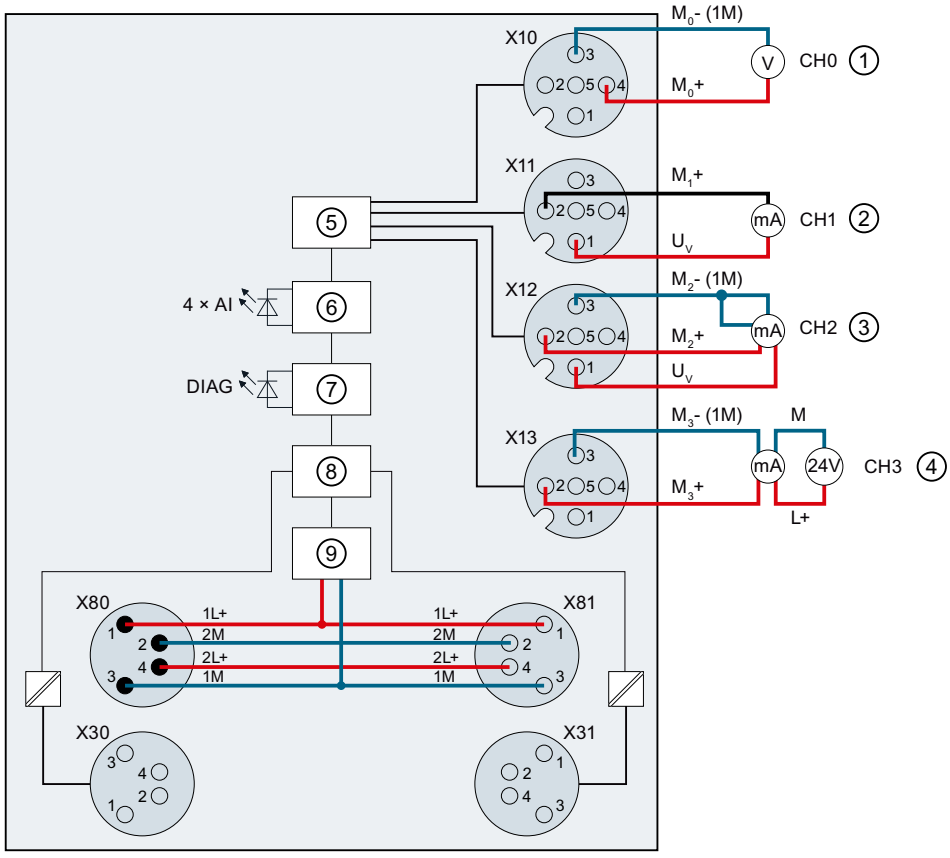
Figure 2-98 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The figure below shows an example of the pin assignment for voltage measurement and current measurement.

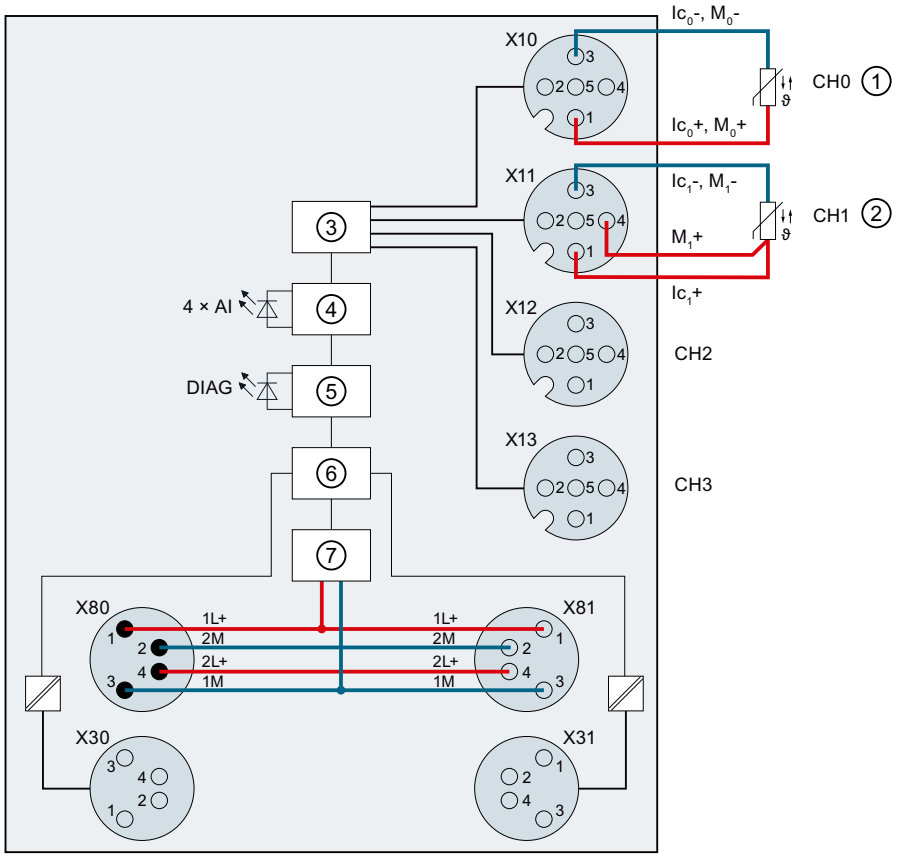


①	Voltage measurement	X30	Infeed of the ET-Connection
②	Current measurement (2 DMU)	X31	Loop-through of the ET-Connection
③	Current measurement (4 DMU, with internal power supply)	1L+	Supply voltage 1L+ (non-switched)
④	Current measurement (4 DMU, with external power supply)	1M	Ground 1M (non-switched)
⑤	Multiplexer	2L+	Load voltage 2L+ (switched)
⑥	Analog-to-digital converter (ADC)	2M	Ground 2M (switched)
⑦	Microcontroller	M_n+	Measuring input positive, channel n
⑧	ET-Connection interface	M_n-	Measuring input negative, channel n
⑨	Internal supply voltage	U_V	24 V encoder supply

X10 to X13	Channels 0 to 3	AI	LEDs channel status (0, 1, 2 and 3) (green)
X80	Infeed of supply voltages	DIAG	LED diagnostic status (red/green)
X81	Loop-through of supply voltages		

Figure 2-99 Terminal and block diagram for voltage and current measurement

The example in the following figure shows the pin assignment for the resistance thermometer.



①	RTD/R 2-wire connection	X30	Infeed of the ET-Connection
②	RTD/R 3-wire connection	X31	Loop-through of the ET-Connection
③	Multiplexer	1L+	Supply voltage 1L+ (non-switched)
④	Analog-to-digital converter (ADC)	1M	Ground 1M (non-switched)
⑤	Microcontroller	2L+	Load voltage 2L+ (switched)
⑥	ET-Connection interface	2M	Ground 2M (switched)
⑦	Internal supply voltage	M_n+	Measuring input positive, channel n
X10 to X13	Channels 0 to 3	M_n-	Measuring input negative, channel n
X80	Infeed of supply voltages	Ic_n+, Ic_n-	Current output, current feed, RTD/R channel n
X81	Loop-through of supply voltages	AI	LEDs channel status (0, 1, 2 and 3) (green)
		DIAG	LED diagnostic status (red/green)

Figure 2-100 Terminal and block diagram for resistance thermometer

4.2 Pin assignment

NOTE

Color coding
The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for analog inputs

The tables below show the pin assignments of the four sockets for connection of the analog inputs.

Table 2-195 Pin assignment of the sockets for analog inputs (voltage measurement)

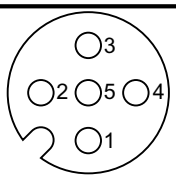
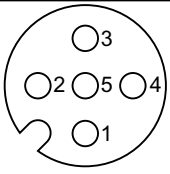
Pin	Assignment **X10 to X13 - sockets for analog inputs (voltage measurement)**	Front view of the sockets
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)	
2	Reserved	
3	Encoder supply ground 1M	
4	Measuring input M_0+: Connector X10 Measuring input M_1+: Connector X11 Measuring input M_2+: Connector X12 Measuring input M_3+: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

Table 2-196 Pin assignment of the sockets for analog inputs (current measurement)

Pin	Assignment **X10 to X13 sockets for analog inputs (current measurement)**	Front view of the sockets
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)	
2	Measuring input M_0+: Connector X10 Measuring input M_1+: Connector X11 Measuring input M_2+: Connector X12 Measuring input M_3+: Connector X13	
3	Encoder supply ground 1M	
4	Reserved	
5	Functional earth FE	
Shield	Functional earth FE	

NOTICE

Short-circuit from encoder supply to measuring input
In the operating mode current measurement a short-circuit from the encoder supply to the measuring input can destroy the input channel.

Table 2-197 Pin assignment of the sockets for analog inputs (RTD/R 2-wire connection)

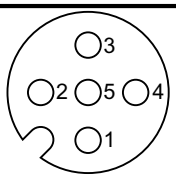
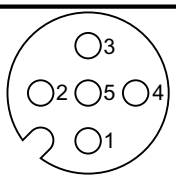
Pin	Assignment **X10 to X13 sockets for analog inputs (RTD/R 2-wire connection)**	Front view of the sockets
1	Measurement cable Ic_0+, M_0+: Connector X10 Measurement cable Ic_1+, M_1+: Connector X11 Measurement cable Ic_2+, M_2+: Connector X12 Measurement cable Ic_3+, M_3+: Connector X13	
2	Reserved	
3	Measurement cable Ic_0-, M_0-: Connector X10 Measurement cable Ic_1-, M_1-: Connector X11 Measurement cable Ic_2-, M_2-: Connector X12 Measurement cable Ic_3-, M_3-: Connector X13	
4	Reserved	
5	Functional earth FE	
Shield	Functional earth FE	

Table 2-198 Pin assignment of the sockets for analog inputs (RTD/R 3-wire connection)

Pin	Assignment **X10 to X13 sockets for analog inputs (RTD/R 3-wire connection)**	Front view of the sockets
1	Constant current cable Ic_0+: Connector X10 Constant current cable Ic_1+: Connector X11 Constant current cable Ic_2+: Connector X12 Constant current cable Ic_3+: Connector X13	
2	Reserved	
3	Measurement cable Ic_0-, M_0-: Connector X10 Measurement cable Ic_1-, M_1-: Connector X11 Measurement cable Ic_2-, M_2-: Connector X12 Measurement cable Ic_3-, M_3-: Connector X13	
4	Measuring input M_0+: Connector X10 Measuring input M_1+: Connector X11 Measuring input M_2+: Connector X12 Measuring input M_3+: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

NOTICE

Incorrect connection of sensors at channel
If the measurement type current or voltage measurement is configured at the I/O module, a connected resistance thermometer could be destroyed.

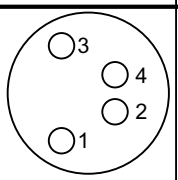
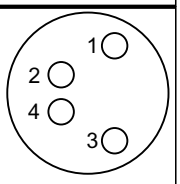
NOTE

Coupler plug for RTD measurement
For RTD measurements, use a coupler plug with gold-plated contacts. Other materials can create contact resistance that can result in incorrect measured values.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

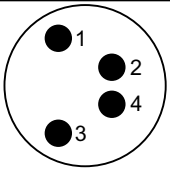
Table 2-199 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the core color of the bus cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	yellow		
2	RXP	TXP	white		
3	RXN	TXN	blue		
4	TXN	RXN	orange		
Shield	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

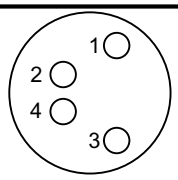
Table 2-200 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the core color of the power cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	brown	
2	Ground 2M (switched)	white	
3	Ground 1M (non-switched)	blue	
4	Load voltage 2L+ (switched)	black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-201 Pin assignment of the supply voltage socket

Pin	Assignment **X81 socket (POWER output)**	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	brown	
2	Ground 2M (switched)	white	
3	Ground 1M (non-switched)	blue	
4	Load voltage 2L+ (switched)	black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the connector for ET-Connection and the connector for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Measurement types and measuring ranges

The table below indicates which measuring range is configurable.

Table 2-202 Measurement type and measuring ranges

Measurement type	Measuring range	Temperature coefficient	Resolution
Deactivated	–	–	–
Voltage	1 V to 5 V 0 V to 10 V	–	max. 16-bit
Current (4-wire transducer)	0 mA to 20 mA 4 mA to 20 mA	–	max. 16-bit
Current (2-wire transducer)	4 mA to 20 mA	–	max. 16-bit
Resistance (3-wire connection) Resistance (2-wire connection)	150 Ω, 300 Ω	–	max. 15-bit
Resistance thermometer (3-wire connection) Resistance thermometer (2-wire connection)	Pt 100 climatic range/ Pt 100 standard range	Pt 0.003850, Pt 0.003916, Pt 0.003902, Pt 0.003920, Pt 0.003851 EN 60751	max. 16-bit incl. sign
	Ni 100 climatic range/ Ni 100 standard range	Ni 0.006180, Ni 0.006720	max. 16-bit incl. sign

5.2 Parameters

Parameters of the analog input module AI 4xU/I/RTD 4xM12

The table below lists the parameters that can be set. The effective range of the parameters that can be set depends on the type of configuration. The following configurations are possible:

- Distributed operation on PROFINET IO
- Distributed operation with PROFIBUS DP

NOTICE
Match of encoder and parameters The default setting of the analog inputs is voltage measurement (1 V to 5 V). Make sure that the connected encoders and the selected parameters match. The connected encoder can be destroyed in the case of incorrect parameters.

The table below shows the PROFINET and PROFIBUS parameters for the analog input module AI 4xU/I/RTD 4xM12 for configuration with GSD file.

Explanation of abbreviations in table below:

4-DMU 4-wire transducer
2-DMU 2-wire transducer
R-3L Resistance 3-wire transducer
R-2L Resistance 2-wire transducer
RTD-3L Resistance thermometer 3-wire transducer
RTD-2L Resistance thermometer 2-wire transducer

Table 2-203 Configurable parameters and their defaults

Parameters	Value range	Default	GSD file PROFINET IO	GSD file PROFIBUS DP
Temperature unit	• Degrees Celsius • Degrees Fahrenheit • Kelvin	Degrees Celsius	Module	Module
Measurement type/measuring range channel n	• Deactivated • 1 V to 5 V • 0 V to 10 V • 0 mA to 20 mA (4-DMU) • 4 mA to 20 mA (4-DMU) • 4 mA to 20 mA (2-DMU) • R-3L 150 ohm • R-3L 300 ohm • R-2L 150 ohm • R-2L 300 ohm	1 V to 5 V	Channel	Channel
Measurement type/measuring range channel n	• RTD-3L Pt100 3851 cl. EN 60751 • RTD-3L Pt100 3851 std. EN 60751 • RTD-3L Pt100 3916 cl. • RTD-3L Pt100 3916 std. • RTD-3L Pt100 3902 cl. • RTD-3L Pt100 3902 std. • RTD-3L Pt100 392 cl. • RTD-3L Pt100 392 std. • RTD-3L Pt100 3850 cl. • RTD-3L Pt100 3850 std. • RTD-2L Pt100 3851 cl. • RTD-2L Pt100 3851 std. • RTD-2L Pt100 3916 cl. • RTD-2L Pt100 3916 std. • RTD-2L Pt100 3902 cl. • RTD-2L Pt100 3902 std. • RTD-2L Pt100 392 cl. • RTD-2L Pt100 392 std. • RTD-2L Pt100 3850 cl. • RTD-2L Pt100 3850 std. • RTD-3L Ni100 618 cl. • RTD-3L Ni100 618 std. • RTD-3L Ni100 672 cl. • RTD-3L Ni100 672 std. • RTD-2L Ni100 618 cl. • RTD-2L Ni100 618 std. • RTD-2L Ni100 672 cl. • RTD-2L Ni100 672 std.	1 V to 5 V	Channel	Channel

Parameters	Value range	Default	GSD file PROFINET IO	GSD file PROFIBUS DP
Smoothing channel n	• None • Weak • Medium • Strong	None	Channel	Channel
Interference frequency suppression	• 3600 Hz • 60 Hz • 50 Hz • 16.67 Hz	50 Hz	Channel	Module
Short-circuit to ground channel n	• Disable • Enable	Disable	Channel	Channel
Wire break channel n	• Disable • Enable	Disable	Channel	Channel
Diagnostics: Overflow/underflow	• Disable • Enable	Disable	---	Module
Diagnostics: Underflow channel n	• Disable • Enable	Disable	Channel	---
Diagnostics: Overflow channel n	• Disable • Enable	Disable	Channel	---
Hardware interrupt high limit 1 channel n	• Disable • Enable	Disable	Channel	---
Hardware interrupt low limit 1 channel n	• Disable • Enable	Disable	Channel	---
Hardware interrupt high limit 2 channel n	• Disable • Enable	Disable	Channel	---
Hardware interrupt low limit 2 channel n	• Disable • Enable	Disable	Channel	---
High limit 1 channel n	The value range depends on the measurement type. The value range (min./max.) permitted for the measurement type is listed in the table below.		Channel	---
Low limit 1 channel n			Channel	---
High limit 2 channel n			Channel	---
Low limit 2 channel n			Channel	---

NOTE

Unused channels

"Deactivate" unused inputs in the parameter assignment to shorten the cycle time of the module.

A deactivated input always returns the value $7FFF_H$.

The table below shows the permitted value ranges for the measurement type.

Table 2-204 Measuring ranges of the hardware interrupts

Measurement type	Measuring range	Low limit	High limit	Default		Unit
				Low limit	High limit	
Voltage	1 V to 5 V	0.297	5.703	1	5	V
		-4863	32510	0	27648	Decimal
	0 V to 10 V	-1.758	11.758	0	10	V
		-4863	32510	0	27648	Decimal
Current	0 mA to 20 mA	-3.51	23.51	0	20	mA
		-4863	32510	0	27648	Decimal
	4 mA to 20 mA	1.19	22.81	4	20	mA
		-4863	32510	0	27648	Decimal
Resistance	150 ohm	0.01	176.37	0.01	150	Ω
		1	32510	1	27648	Decimal
	300 ohm	0.01	352.75	0.01	300	Ω
		1	32510	1	27648	Decimal
Resistance thermometer	Pt100 cl.	-144.99	154.99	-120	130	°C
		-14499	15499	-12000	13000	Decimal
		-228.99	310.99	-184	266	F
		-22899	31099	-18400	26600	Decimal
	Ni100 cl.	-104.99	154.99	-60	130	°C
		-10499	15499	-6000	13000	Decimal
		-156.99	310.99	-76	266	F
		-15699	31099	-7600	26600	Decimal
	Pt100 std.	-242.9	999.9	-200	850	°C
		-2429	9999	-2000	8500	Decimal
		-405.3	1831.9	-328	1562	F
		-4053	18319	-3280	15620	Decimal
		30.3	1273.1	73.2	1123.2	K
		303	12731	732	11232	Decimal
	Ni100 std.	-104.9	294.9	-60	250	°C
		-1049	2949	-600	2500	Decimal
		-156.9	562.9	-76	482	F
		-1569	5629	-760	4820	Decimal
		168.3	568.1	213.2	523.2	K
		1683	5681	2132	5232	Decimal

5.3 Explanation of the parameters

Temperature unit

You use this parameter to set the temperature unit with which you want to measure the temperature.

Measurement type/measuring range channel n

You use this parameter to set the measurement type or the measuring range for acquiring the measured values.

NOTE

Unused channels

"Deactivate" unused channels in the parameter assignment to improve the cycle time of the module.

A deactivated channel always returns the value $7FFF_H$.

Temperature coefficient (for RTD, resistance thermometer)

The temperature coefficient depends on the chemical composition of the material. In Europe, only one value is used per sensor type (default value).

The correction factor for the temperature coefficient (α value) specifies how much the resistance of a certain material changes when the temperature is raised by 1 °C.

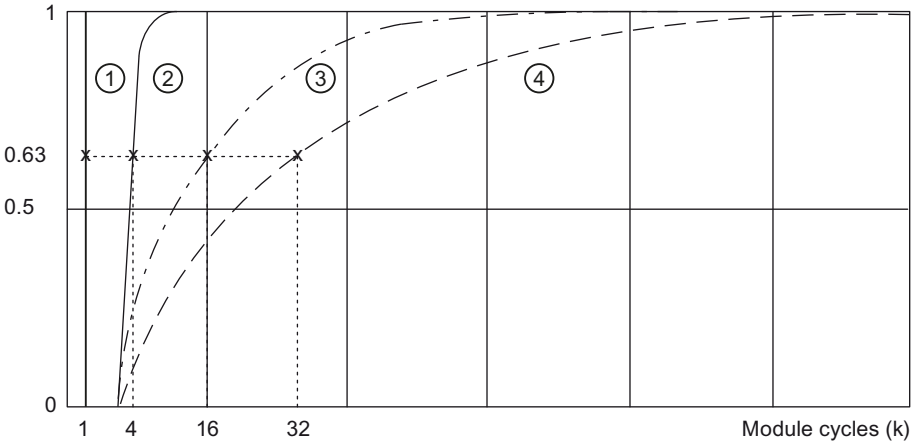
The further values facilitate sensor-specific setting of the temperature coefficient and enhance accuracy.

Smoothing channel n

The purpose of smoothing is to filter out interferences. The greater the smoothing factor, the better the filter effect. This is technically implemented in the form of a digital filter. The smoothing can be set in 4 levels. The smoothing factor k is equal to the number of module cycles. The time constant of the smoothing filter is the product of the smoothing factor k and the cycle time of the I/O module. The greater the smoothing, the greater the time constant of the filter.

Smoothing time = number of module cycles (k) × cycle time of the module.

The following figure shows how many module cycles it takes for the smoothed analog value to approach 100%, depending on the configured smoothing. This is valid for all signal changes at the analog input.



① No smoothing (k = 1)
② Weak (k = 4)
③ Medium (k = 16)
④ Strong (k = 32)

Figure 2-101 Smoothing

Interference frequency suppression channel n

This parameter suppresses interference for analog input modules which is caused by the frequency of the alternating voltage network in use.

The frequency of the alternating voltage network may negatively affect the measured value, in particular when measuring in the low voltage range and with thermocouples. With this parameter, the user specifies the line frequency that is predominant in the plant.

Diagnostics: Short-circuit to ground channel n

Enabling of the diagnostics if a short-circuit of the encoder supply to ground occurs.

Diagnostics: Wire break channel n

Enabling of the diagnostics if the analog input module has no current flow or the current is too weak for measurement at the correspondingly configured input.

NOTE

Wire break diagnostics

A wire break diagnostics is not possible for all measuring ranges and measurement types for analog input channels.

The table below shows the rules you must observe in the case of a wire break in the measuring ranges 1 to 5, 4 to 20 mA:

Table 2-205 Parameters for wire break

Parameter	Event	Measured value	Explanation
Wire break enabled[1]	Wire break	$7FFF_H$	**Wire break** diagnostics
Wire break disabled[1] Underflow enabled	Wire break	8000_H	Measured value after leaving the underrange Diagnostics alarm **Low limit violated**
Wire break disabled[1] Underflow disabled	Wire break	8000_H	Measured value after leaving the underrange

[1] Measuring range limits for detection of wire break and measuring range undershoot:
- 1 V to 5 V: at 0.296 V
- 4 mA to 20 mA: at 1.185 mA

The table below shows the diagnostics that can occur for wire break with the measurement type RTD/R.

Table 2-206 Diagnostics with RTD/R

Diagnostics: Wire break	Diagnostics: Overflow	Diagnostics: Underflow*	Event	Process data	Diagnostics alarm per channel
activated	Deactivated	Deactivated	Wire break	0x7FFF	Wire break
Deactivated	Deactivated	Activated	Wire break	0x7FFF	-
Deactivated	Activated	Deactivated	Wire break	0x7FFF	High limit exceeded
Deactivated	Activated	Activated	Wire break	0x7FFF	High limit violated
Deactivated	Deactivated	Deactivated	Wire break	0x7FFF	-

* This column does not apply to the measurement type resistance.

Diagnostics: Underflow channel n

Enabling of the diagnostics when the measured value falls below the underrange.

Diagnostics: Overflow channel n

Enabling of the diagnostics when the measured value exceeds the overrange.

Diagnostics: Overflow/Underflow (for PROFIBUS only)

Enabling of the diagnostics when the measured value exceeds the overrange or falls below the underrange.

The diagnostic enable has an effect on all channels.

Hardware interrupt high/low limit 1 or 2 channel n

Enabling of a hardware interrupt when the high limit 1 or 2 or the low limit 1 or 2 is violated.

Requirement: An OB 4x must be assigned to the CPU/device.

Additional information on the structure of hardware interrupts is available in the section Interrupts (Page 30).

High/low limit 1 or 2 channel n

Specify a threshold at which a hardware interrupt is triggered when it is exceeded or undershot.

5.4 Address space

The tables below shows the assignment of the address space for the analog input module AI 4xU/I/RTD 4xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-207 Address space in the configuration mode AI with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Input value channel 0
IB x +1									
IB x +2									Input value channel 0
IB x +3									
IB x +4									Input value channel 1
IB x +5									
IB x +6									Input value channel 3
IB x +7									
IB x +8	0	0	0	0					Value status (QI) for inputs on channels 0 ... 3*

* 0 = Value read in at channel is incorrect

Configuration options of the AI 4xU/I/RTD 4xM12 analog input module

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

If you enable the value status for the analog input module, a bit is also assigned in the input address space. Bits 0 to 3 in this byte are assigned to a channel and provide information on the validity of the analog value. The value status is independent of whether or not diagnostics was configured.

Bit = 1: No error on channel.

Bit = 0: Error on channel.

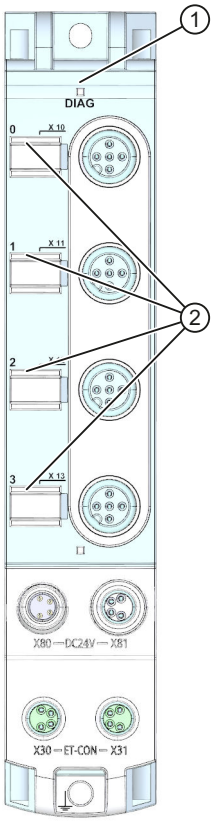
Interrupts/diagnostics alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED display (status and error displays) of the analog input module AI 4xU/I/RTD 4xM12.



① Diagnostic status (DIAG) (red/green)
② Channel status (0, 1, 2 and 3) (green)

Figure 2-102 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 33).

DIAG LED

Table 2-208 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED for the channel status

Table 2-209 Status display of the LEDs 0, 1, 2 and 3

LED 0, 1, 2 and 3	Meaning
☐ Off	• Channel deactivated • Channel activated and incorrect parameter assignment • Parameter error possible with GSD
■ On	• Channel activated and correct parameter assignment

6.2 Interrupts

Analog input module AI 4xU/I/RTD 4xM12 supports the following diagnostic and hardware interrupts.

Diagnostic interrupt

The table below shows the events for which the analog input module returns a diagnostic interrupt, depending on the parameter assignment.

Table 2-210 Diagnostic interrupts

Measurement type	Measuring range	Diagnostics				
		Short-circuit to ground	Wire break	Underflow[1]	Overflow[1]	Underflow/ Overflow[2]
Voltage	**1 V to 5 V**	x	x	x	x	x
	0 V to 10 V	x	-	x	x	x
Current	**2-DMU 4 mA to 20 mA**	x	x	x	x	x

1 Column valid for configuration with PROFINET GSD file

2 Column valid for configuration with PROFIBUS GSD file

Measurement type	Measuring range	Diagnostics				
		Short-circuit to ground	Wire break	Underflow[1]	Overflow[1]	Underflow/ Overflow[2]
Current	**4-DMU 0 mA to 20 mA**	x	-	x	x	x
	4-DMU 4 mA to 20 mA	x	x	x	x	x
Resistance	**150 Ω**	-	x	-	x	x
	300 Ω	-	x	-	x	x
Resistance thermometer	**PT100**	-	x	x	x	x
	Ni100	-	x	x	x	x

1 Column valid for configuration with PROFINET GSD file

2 Column valid for configuration with PROFIBUS GSD file

Hardware interrupt

The analog input module generates a hardware interrupt with the following events:

- Low limit 1 violated
- High limit 1 violated
- Low limit 2 violated
- High limit 2 violated

Detailed information on the event is available in the hardware interrupt organization block with the instruction "RALRM" (Read additional interrupt information) and in the STEP 7 online help.

The start information of the organization block includes information on which channel of the analog input module triggered the hardware interrupt.

NOTE

Violation of two limits

If two limits are violated at the same time, limit 1 is always signaled first, followed by limit 2.

The figure below shows the assignment to the bits of the local data double word 8.

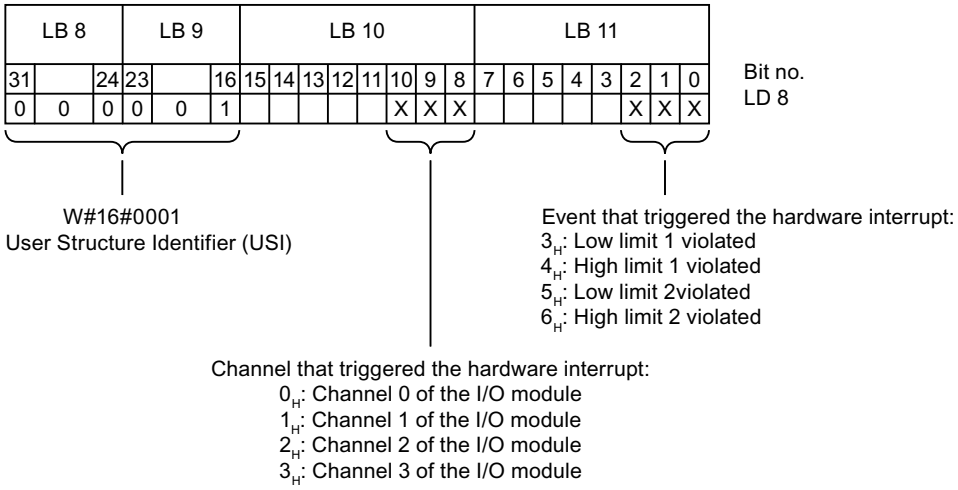


Figure 2-103 Start information of the organization block

Structure of the additional interrupt information

Table 2-211 Structure of USI = W#16#0001

Data block name	Contents	Comment	Bytes
USI (User Structure Identifier)	W#16#0001	Additional interrupt info for hardware interrupts of the I/O module	2
The channel that triggered the hardware interrupt follows.			
Channel	B#16#00 to B#16#03	Number of channel which triggered the event	1
The error event that triggered the hardware interrupt follows.			
Event	B#16#03	Low limit 1 violated	1
	B#16#04	High limit 1 violated	
	B#16#05	Low limit 2 violated	
	B#16#06	High limit 2 violated	

6.3 Diagnostics alarms

A diagnostics alarm is output for each diagnostic event and the DIAG LED flashes red on the analog input module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

The following tables set out the diagnostics alarms for the set measuring range.

Table 2-212 Diagnostics alarms, security event

Diagnostics alarm	Error code	Meaning	Solution
Security event: Firmware has been successfully downloaded and activated for installation.[1]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[1]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 A diagnostics alarm is output for a signed firmware update.

Table 2-213 Diagnostics alarms - for the measuring range: 1 V to 5 V, 2-DMU 4 mA to 20 mA and 4-DMU 4 mA to 20 mA

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit	1_H	Short-circuit encoder supply to ground	Correct interplay between module and encoder
Wire break	6_H	Wire break between the module and sensor	Connect the cable
		Channel not connected (open)	• Deactivate diagnostics • Connect the channel • Deactivate channel
High limit violated	7_H	Value is above overrange.	Correct interplay between module and sensor
Low limit violated	8_H	Value is below underrange.	Correct interplay between module and sensor
Error	9_H	Value is significantly above or below underrange/overrange.	Correct interplay between module and sensor
Parameter error	10_H	Module parameter assignment is faulty	Correct the parameter assignment
Hardware interrupt lost	16_H	At least one hardware interrupt could not be signaled because too many hardware interrupts are pending.	Correct the program or the process

Table 2-214 Diagnostics alarms - for the measuring range: 0 V to 10 V and 4-DMU 0 mA to 20 mA

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit	1_H	Short-circuit encoder supply to ground	Correct interplay between module and encoder
High limit violated	7_H	Value is above overrange.	Correct interplay between module and sensor
Low limit violated	8_H	Value is below underrange.	Correct interplay between module and sensor
Error	9_H	Value is significantly above or below underrange/overrange.	Correct interplay between module and sensor
Parameter error	10_H	Module parameter assignment is faulty	Correct the parameter assignment
Hardware interrupt lost	16_H	At least one hardware interrupt could not be signaled because too many hardware interrupts are pending.	Correct the program or the process

Table 2-215 Diagnostics alarms - for the measuring range: 150 Ω and 300 Ω

Diagnostics alarm	Error code	Meaning	Solution
Wire break	6_H	Impedance of encoder circuit too high	Use a different encoder type or modify the wiring, for example, using cables with larger cross-section
		Wire break between the module and sensor	Connect the cable
		Channel not connected (open)	• Deactivate diagnostics • Connect the channel • Deactivate channel
High limit violated	7_H	Value is above overrange.	Correct interplay between module and sensor
Parameter error	10_H	Module parameter assignment is faulty	Correct the parameter assignment
Hardware interrupt lost	16_H	At least one hardware interrupt could not be signaled because too many hardware interrupts are pending.	Correct the program or the process

NOTE

Measurement type resistor (3-wire terminal)

A wire break of the M+ cable is not detected with measurement type resistor (3-wire terminal). An incorrect measuring value is output in this case.

Table 2-216 Diagnostics alarms - for the measuring range: Pt100 and Ni100

Diagnostics alarm	Error code	Meaning	Solution
Wire break	6_H	Impedance of encoder circuit too high	Use a different encoder type or modify the wiring, for example, using cables with larger cross-section
		Wire break between the module and sensor	Connect the cable
		Channel not connected (open)	• Deactivate diagnostics • Connect the channel • Deactivate channel
High limit violated	7_H	Value is above overrange.	Correct interplay between module and sensor
Low limit violated	8_H	Value is below underrange.	Correct interplay between module and sensor
Parameter error	10_H	Module parameter assignment is faulty	Correct the parameter assignment
Hardware interrupt lost	16_H	At least one hardware interrupt could not be signaled because too many hardware interrupts are pending.	Correct the program or the process

Technical specifications

7

Technical specifications of the AI 4xU/I/RTD 4xM12 analog input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7144-5KD00-0BA0/td?dl=en).

Article number	6ES7144-5KD00-0BA0
General information	
Product type designation	AI 4xU/I/RTD
HW functional status	FS07
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	From V5.5 SP4 Hotfix 3
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Input current	
Current consumption (rated value)	35 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	4
24 V encoder supply	
• Short-circuit protection	Yes; per channel, electronic
• Output current, max.	0.5 A; Per channel, total current of all channels max. 1 A
Power loss	
Power loss, typ.	1.5 W
Analog inputs	
Number of analog inputs	4
• For current measurement	4

Article number	6ES7144-5KD00-0BA0
• For voltage measurement	4
• For resistance/resistance thermometer measurement	4
permissible input voltage for voltage input (destruction limit), max.	30 V
permissible input current for current input (destruction limit), max.	50 mA
Cycle time (all channels), min.	8 ms
Technical unit for temperature measurement adjustable	Yes; Degrees Celsius / degrees Fahrenheit / Kelvin
Input ranges (rated values), voltages	
• 0 to +10 V	Yes
– Input resistance (0 to 10 V)	10 MΩ
• 1 V to 5 V	Yes
– Input resistance (1 V to 5 V)	10 MΩ
Input ranges (rated values), currents	
• 0 to 20 mA	Yes
– Input resistance (0 to 20 mA)	50 Ω
• 4 mA to 20 mA	Yes
– Input resistance (4 mA to 20 mA)	50 Ω
Input ranges (rated values), resistance thermometer	
• Ni 100	Yes; Standard/climate
– Input resistance (Ni 100)	10 MΩ
• Pt 100	Yes; Standard/climate
– Input resistance (Pt 100)	10 MΩ
Input ranges (rated values), resistors	
• 0 to 150 ohms	Yes
– Input resistance (0 to 150 ohms)	10 MΩ
• 0 to 300 ohms	Yes
– Input resistance (0 to 300 ohms)	10 MΩ
Cable length	
• shielded, max.	30 m
Analog value generation for the inputs	
Measurement principle	integrating
Integration and conversion time/resolution per channel	
• Resolution with overrange (bit including sign), max.	16 bit
• Integration time, parameterizable	Yes; channel by channel
• Integration time (ms)	0,3 / 16,7 / 20 / 60
• Interference voltage suppression for interference frequency f1 in Hz	3 600 / 60 / 50 / 16.7
• Conversion time (per channel)	2 / 18 / 21 / 61 ms
Smoothing of measured values	
• parameterizable	Yes

Article number	6ES7144-5KD00-0BA0
• Step: None	Yes; 1x cycle time
• Step: low	Yes; 4x cycle time
• Step: Medium	Yes; 16x cycle time
• Step: High	Yes; 32x cycle time
Encoder	
Connection of signal encoders	
• for voltage measurement	Yes
• for current measurement as 2-wire transducer	Yes
• for current measurement as 4-wire transducer	Yes
• for resistance measurement with two-wire connection	Yes
• for resistance measurement with three-wire connection	Yes
Errors/accuracies	
Linearity error (relative to input range), (+/-)	0.025 %
Temperature error (relative to input range), (+/-)	0.01 %/K
Crosstalk between the inputs, max.	-70 dB
Repeat accuracy in steady state at 25 °C (relative to input range), (+/-)	0.01 %
Operational error limit in overall temperature range	
• Voltage, relative to input range, (+/-)	0.35 %
• Current, relative to input range, (+/-)	0.45 %
• Resistance, relative to input range, (+/-)	0.25 %
• Resistance thermometer, relative to input range, (+/-)	0.25 %
Basic error limit (operational limit at 25 °C)	
• Voltage, relative to input range, (+/-)	0.25 %
• Current, relative to input range, (+/-)	0.25 %
• Resistance, relative to input range, (+/-)	0.15 %
• Resistance thermometer, relative to input range, (+/-)	0.15 %
Interference voltage suppression for f = n x (f1 +/- 0.5 %), f1 = interference frequency	
• Series mode interference (peak value of interference < rated value of input range), min.	40 dB
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
• Limit value alarm	Yes; Parameterizable
Diagnoses	
• Wire-break	Yes; at 4 mA to 20 mA and 1 V to 5 V
• Short-circuit	Yes; Encoder supply to M, channel by channel
• Overflow/underflow	Yes

Article number	6ES7144-5KD00-0BA0
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS02
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded

Article number	6ES7144-5KD00-0BA0
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	168 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific response of the analog input module is explained in the section below.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (http://support.automation.siemens.com/WW/view/en/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 Response of the analog input module

Requirement

You can use the PROFIenergy function when you use the internal encoder supply.

Display

The channel status LEDs are not affected by PROFIenergy.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- Encoder supply switch-off upon the start of "pause" does not result in the alarm "Wire break".
- "Wire break", "Short circuit", "High limit violated" and "Low limit violated" error detection is not possible during the "pause":
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.
- Hardware interrupts are not signaled.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-217 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: $7FFF_H$ • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Encoder supply U_S switched off [1] • Pause substitute value: Configured pause substitute value • Value status "BAD"

[1] Encoder supply U_S is only provided for measurement type current and voltage and can only be deactivated in these measurement types.

Dimension drawing

A

The figure below shows the dimension drawing of the AI 4xU/I/RTD 4xM12 analog input module in front and side view.

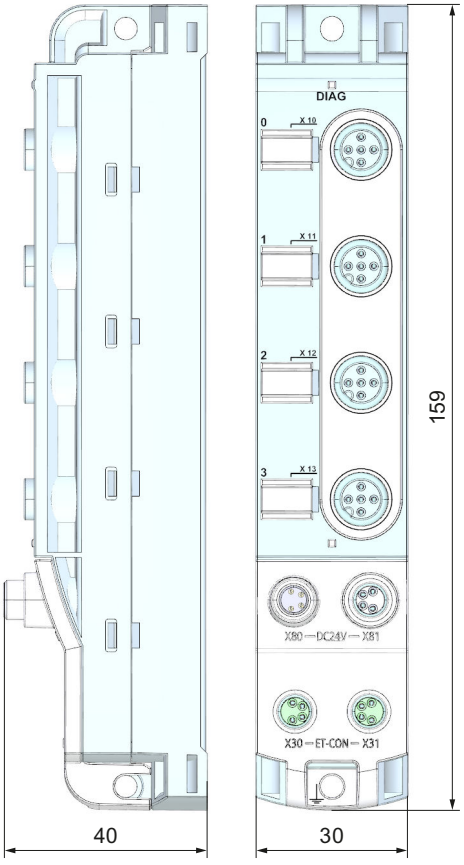


Figure 2-104 Dimension drawing

Representation of analog values

B

B.1 Representation of analog values in voltage measuring ranges

Table 2-218 Voltage measuring range 1 V to 5 V and 0 V to 10 V

Values		Voltage measuring range		Range
Dec.	**Hex.**	**1 V to 5 V**	**0 V to 10 V**	
32767	7FFF	>5.704 V	>11.759 V	Overflow
32511	7EFF	5.704 V	11.759 V	Overrange
27649	6C01			
27648	6C00	5 V	10 V	Nominal range
20736	5100	4 V	7.5 V	
1	1	1 V + 144.7 µV	0 V + 361.7 µV	
0	0	1 V	0 V	
-1	FFFF			Underrange
-4864	ED00	0.296 V	-1.759	
-32768	8000	<0.296 V	< -1.759	Underflow

B.2 Representation of analog values in current measuring ranges

Table 2-219 Current measuring ranges 0 mA to 20 mA and 4 mA to 20 mA

Values		Current measuring range		Range
Dec.	**Hex.**	**0 mA to 20 mA**	**4 mA to 20 mA**	
32767	7FFF	>23.52 mA	>22.81 mA	Overflow
32511	7EFF	23.52 mA	22.81 mA	Overrange
27649	6C01			
27648	6C00	20 mA	20 mA	Nominal range
20736	5100	15 mA	16 mA	
1	1	723.4 nA	4 mA + 578.7 nA	
0	0	0 mA	4 mA	
-1	FFFF			Underrange
-4864	ED00	-3.52 mA	1.185 mA	
-32768	8000	<-3.52 mA	<1.185 mA	Underflow

B.3 Representation of analog values for resistance-based sensors

Resistance-based sensor

Table 2-220 Resistance-based sensor of 150 Ω and 300 Ω

Values		Resistance-based sensor range		Range
Dec.	**Hex.**	**150 Ω**	**300 Ω**	
32767	7FFF	>176.38 Ω	>352.77 Ω	Overflow
32511	7EFF	176.38 Ω	352.77 Ω	Overrange
27649	6C01			
27648	6C00	150 Ω	300 Ω	Nominal range
20736	5100	112.5 Ω	225 Ω	
1	1	5.43 mΩ	10.85 mΩ	
0	0	0 Ω	0 Ω	
-1 : -4864	FFFF : ED00	(negative values are physically impossible)		Underrange[1]
-32768	8000			Underflow[1]

[1] If the sensors are not connected correctly

B.4 Representation of analog values for resistance thermometer

Table 2-221 Resistance thermometer Pt 100 standard

Pt x00 standard in °C (1 digit = 0.1°C)	Values		Pt x00 standard in °F (1 digit = 0.1 °F)	Values		Pt x00 standard in K (1 digit = 0.1 K)	Values		Range
	Dec.	**Hex.**		**Dec.**	**Hex.**		**Dec.**	**Hex.**	
>1000.0	32767	7FFF	>1832.0	32767	7FFF	>1273.2	32767	7FFF	Overflow
1000.0 : 850.1	10000 : 8501	2710 : 2135	1832.0 : 1562.1	18320 : 15621	4790 : 3D05	1273.2 : 1123.3	12732 : 11233	31BC : 2BE1	Overrange
850.0 : -200.0	8500 : -2000	2134 : F830	1562.0 : -328.0	15620 : -3280	3D04 : F330	1123.2 : 73.2	11232 : 732	2BE0 : 2DC	Nominal range
-200.1 : -243.0	-2001 : -2430	F82F : F682	-328.1 : -405.4	-3281 : -4054	F32F : F02A	73.1 : 30.2	731 : 302	2DB : 12E	Underrange
<-243.0	-32768	8000	<-405.4	-32768	8000	<30.2	32768	8000	Underflow

Table 2-222 Resistance thermometer Pt 100 climatic

Pt x00 climatic in °C (1 digit = 0.01 °C)	Values		Pt x00 climatic in °F (1 digit = 0.01 °F)	Values		Range
	Dec.	**Hex.**		**Dec.**	**Hex.**	
>155.00	32767	7FFF	>311.00	32767	7FFF	Overflow
155.00 : 130.01	15500 : 13001	3C8C : 32C9	311.00 : 266.01	31100 : 26601	797C : 67E9	Overrange

Pt x00 climatic in °C (1 digit = 0.01 °C)	Values		Pt x00 climatic in °F (1 digit = 0.01 °F)	Values		Range
	Dec.	Hex.		Dec.	Hex.	
130.00 : -120.00	13000 : -12000	32C8 : D120	266.00 : -184.00	26600 : -18400	67E8 : B820	Nominal range
-120.01 : -145.00	-12001 : -14500	D11F : C75C	-184.01 : -229.00	-18401 : -22900	B81F : A68C	Underrange
<-145.00	-32768	8000	<-229.00	-32768	8000	Underflow

Table 2-223 Resistance thermometer Ni 100 standard

Ni x00 standard in °C (1 digit = 0.1 °C)	Values		Ni x00 standard in °F (1 digit = 0.1 °F)	Values		Ni x00 standard in K (1 digit = 0.1 K)	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
>295.0	32767	7FFF	>563.0	32767	7FFF	>568.2	32767	7FFF	Overflow
295.0 : 250.1	2950 : 2501	B86 : 9C5	563.0 : 482.1	5630 : 4821	15FE : 12D5	568.2 : 523.3	5682 : 5233	1632 : 1471	Overrange
250.0 : -60.0	2500 : -600	9C4 : FDA8	482.0 : -76.0	4820 : -760	12D4 : FD08	523.2 : 213.2	5232 : 2132	1470 : 854	Nominal range
-60.1 : -105.0	-601 : -1050	FDA7 : FBE6	-76.1 : -157.0	-761 : -1570	FD07 : F9DE	213.1 : 168.2	2131 : 1682	853 : 692	Underrange
<-105.0	-32768	8000	<-157.0	-32768	8000	<168.2	32768	8000	Underflow

Table 2-224 Resistance thermometer Ni 100 climatic

Ni x00 climatic in °C (1 digit = 0.01 °C)	Values		Ni x00 climatic in °F (1 digit = 0.01 °F)	Values		Range
	Dec.	Hex.		Dec.	Hex.	
>155.00	32767	7FFF	>311.00	32767	7FFF	Overflow
155.00 : 130.01	15500 : 13001	3C8C : 32C9	311.00 : 266.01	31100 : 26601	797C : 67E9	Overrange
130.00 : -60.00	13000 : -6000	32C8 : E890	266.00 : -76.00	26600 : -7600	67E8 : E250	Nominal range
-60.01 : -105.00	-6001 : -10500	E88F : D6FC	-76.01 : -157.00	-7601 : -15700	E24F : C2AC	Underrange
<-105.00	-32768	8000	<-157.00	-32768	8000	Underflow

Parameter data record

C

C.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters. The channel parameter blocks are identical and are shown based on the example of channel 0.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Number of parameter structures = 2_D ($0000\ 0010_B$)							
2...3	**Module header information**							
2	Number of module parameter blocks = 1_D ($0000\ 0001_B$)							
3	Module parameter length = 1_D ($0000\ 0001_B$)							
4...5	**Module parameter block**							
4	Reserved[1]		Temperature unit[2] 00_B: Degrees Celsius 01_B: Degrees Fahrenheit 10_B: Kelvin[3]		Reserved[1]			
5	Channel parameter length = 12_D ($0000\ 1100_B$)							
6...21	**Channel 0 channel parameter block**							
6	Temperature coefficient[3, 4] 0000_B: Pt 0.00385055[3] 0001_B: Pt 0.003916[3] 0010_B: Pt 0.003902[3] 0011_B: Pt 0.00392[3] 0100_B: Pt 0.00385[3] 1000_B: Ni 0.00618[4] 1001_B: Ni 0.00672[4]				Measurement type 0000_B: Deactivated 0001_B: Voltage 0010_B: Current 4-wire transducer 0011_B: Current 2-wire transducer 0101_B: Resistor 3-wire terminal 0110_B: Resistor 2-wire terminal 1000_B: Thermal resistor 3-wire terminal 1001_B: Thermal resistor 2-wire terminal			
7	Measuring range $0000\ 0000_B$: Deactivated $0000\ 0001_B$: 150 Ω[5] $0000\ 0010_B$: 300 Ω[5] $0000\ 0010_B$: 0 ... 20 mA[6] $0000\ 0011_B$: 4 ... 20 mA[6, 7] $0000\ 1010_B$: 1 ... 5 V[8] $0000\ 1011_B$: 0 ... 10 V[8] $0000\ 0000_B$: Pt 100 climatic range[9] $0000\ 0001_B$: Ni 100 climatic range[9] $0000\ 0010_B$: Pt 100 standard range[9]							

1 Reserved bits must be set to 0

2 Only for thermal resistor measuring type. Otherwise, set the bit to 0

3 Only for "Pt climatic range and Pt standard range" measuring range . Otherwise, set the bit to 0

4 Only for "Ni climatic range and Ni standard range" measuring range. Otherwise, set the bit to 0

5 Only for "Thermal resistor" measurement type

6 Only for "Current 4-wire transducer" measurement type

7 Only for "2-wire transducer" measurement type

8 Only for "Voltage" measurement type

9 Only for "Thermal resistor" measurement type

10 Not for the "Resistor" measurement types. Set the bit to 0 for these measurement types

11 Not for the "Voltage - 0 ... 10 V" and "Current 4-wire transducer - 0 ... 20 mA" measurement types. Set the bit to 0 for these measurement types

12 Not for the "Resistor" and thermal resistor measurement types. Set the bit to 0 for these measurement types

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
	0000 0011$_B$: Ni 100 standard range[9]							
8	Interference frequency suppression				Smoothing			
	0001$_B$: 60 Hz (16.6 ms) 0010$_B$: 50 Hz (20 ms) 0100$_B$: 16.67 Hz (60 ms) 0110$_B$: 3600 Hz (0.3 ms)				0000$_B$: None 0001$_B$: Weak 0010$_B$: Medium 0011$_B$: Strong			
9	Hardware interrupt, low limit 1	Hardware interrupt, high limit 1	Hardware interrupt, low limit 2	Hardware interrupt, high limit 2	Diagnostics overflow	Diagnostics underflow[10]	Diagnostics wire break[11]	Diagnostics short-circuit to ground[12]
	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable	0$_B$: Disable 1$_B$: Enable
10 **11**	High limit 1: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Measuring ranges of the hardware interrupts.							
12 **13**	Low limit 1: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Measuring ranges of the hardware interrupts.							
14 **15**	High limit 2: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Measuring ranges of the hardware interrupts.							
16 **17**	Low limit 2: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Measuring ranges of the hardware interrupts.							
18...29	**Channel 1 channel parameter block**							
30...41	**Channel 2 channel parameter block**							
42...53	**Channel 3 channel parameter block**							

1 Reserved bits must be set to 0

2 Only for thermal resistor measuring type. Otherwise, set the bit to 0

3 Only for "Pt climatic range and Pt standard range" measuring range . Otherwise, set the bit to 0

4 Only for "Ni climatic range and Ni standard range" measuring range. Otherwise, set the bit to 0

5 Only for "Thermal resistor" measurement type

6 Only for "Current 4-wire transducer" measurement type

7 Only for "2-wire transducer" measurement type

8 Only for "Voltage" measurement type

9 Only for "Thermal resistor" measurement type

10 Not for the "Resistor" measurement types. Set the bit to 0 for these measurement types

11 Not for the "Voltage - 0 ... 10 V" and "Current 4-wire transducer - 0 ... 20 mA" measurement types. Set the bit to 0 for these measurement types

12 Not for the "Resistor" and thermal resistor measurement types. Set the bit to 0 for these measurement types

See also

Parameters (Page 20)

C.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 33) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-225 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	Byte 1	Byte 2	Byte 3			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	Byte 1	Byte 2	Byte 3			
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓
DF	80	E1	02	Invalid diagnostics enable bit set for operating mode.	Check the parameters of the I/O device.	✓
DF	80	E1	04	Invalid value set for hardware interrupt limit.	Check the parameters of the I/O device.	✓
DF	80	E1	05	Invalid coding set for measuring range / measurement type.	Check the parameters of the I/O device.	✓
DF	80	E1	08	Invalid coding set for interference frequency suppression / integration time.	Check the parameters of the I/O device.	✓
DF	80	E1	09	Invalid coding set for smoothing.	Check the parameters of the I/O device.	✓
DF	80	E1	10	Invalid measurement type set.	Check the parameters of the I/O device.	✓
DF	80	E1	20	Invalid temperature coefficient set.	Check the parameters of the I/O device.	✓
DF	80	E1	21	Invalid temperature unit set.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
Analog input module AI 4xRTD/TC 4xM12 (6ES7144-5KD50-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostics alarms 6

Technical specifications 7

Dimension drawing A

Representation of analog values B

Parameter data record C

10/2024
A5E48753535-AC

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 14

4 Wiring 15

4.1 Terminal and block diagram 15
4.2 Pin assignment 17

5 Parameters/address space 21

5.1 Measurement types and measuring ranges 21
5.2 Parameters 22
5.3 Explanation of the parameters 27
5.4 Structure of a data record for dynamic reference temperature 31
5.5 Address space 32

6 Interrupts/diagnostics alarms 34

6.1 Status and error displays 34
6.2 Interrupts 35
6.3 Diagnostics alarms 37

7 Technical specifications 39

7.1 Technical specifications 39

A Dimension drawing 44

A.1 Dimension drawing 44

B Representation of analog values 45
B.1 Representation of analog values in voltage measuring range 45
B.2 Representation of analog values for resistance-based sensors 46
B.3 Representation of analog values for thermal resistors 46
B.4 Representation of analog values for thermocouples 48

C Parameter data record 51
C.1 Structure of data record 128 for the module parameter assignment 51
C.2 Structure of data record 192 for the dynamic reference temperature 54
C.3 Error transferring the data record 56

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7144-5KD50-0BA0

View of the module

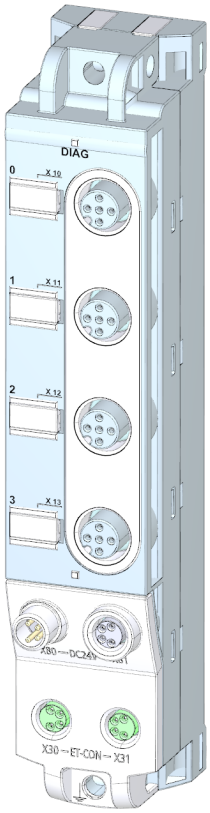


Figure 2-105 View of the analog input module AI 4xRTD/TC 4xM12

Properties

The module has the following technical properties:

- 4 analog inputs
- M12 sockets for connection of sensors
- Measurement type can be set for each channel:
  - Voltage measurement: ±80 mV
  - Resistance measurement: 0-150 Ohm, 0-300 Ohm (2-/3-/4-wire connection)
  - Thermal resistance measurement: Pt/Ni100, Pt/Ni1000 (2-/3-/4-wire connection)
  - Thermocouple measurement: Type B, C, E, J, K, L, N, R, S, T, U
- Connection for isolated/non-isolated thermocouples
- Resolution 16-bit
- Dimensions 30 x 159 x 40 mm
- Accuracy according to AMS2750E
- Configurable diagnostics can be set for each channel
- Hardware interrupt on limit violation can be set per channel (two high and two low limits per channel)
- Various options to compensate for the reference junction temperature

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)

NOTE

Process values during startup
As long as no parameters have been received by the I/O module, the I/O module returns the process value $7FFF_H$.

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

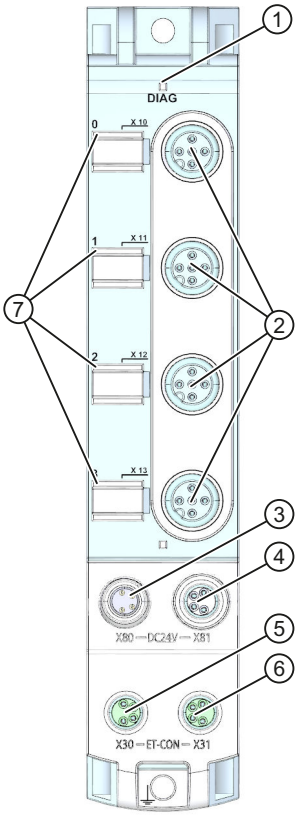
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator control and display elements of the analog input module AI 4xRTD/TC 4xM12.



① DIAG: LED display for the diagnostic status
② X10 to X13: Sockets for the input signal
③ X80: Connector for infeed of the supply voltage (POWER input)
④ X81: Socket for loop-through of the supply voltage (POWER output)
⑤ X30: Socket for ET-Connection IN
⑥ X31: Socket for ET-Connection OUT
⑦ LED displays 0 to 3 for the channel status

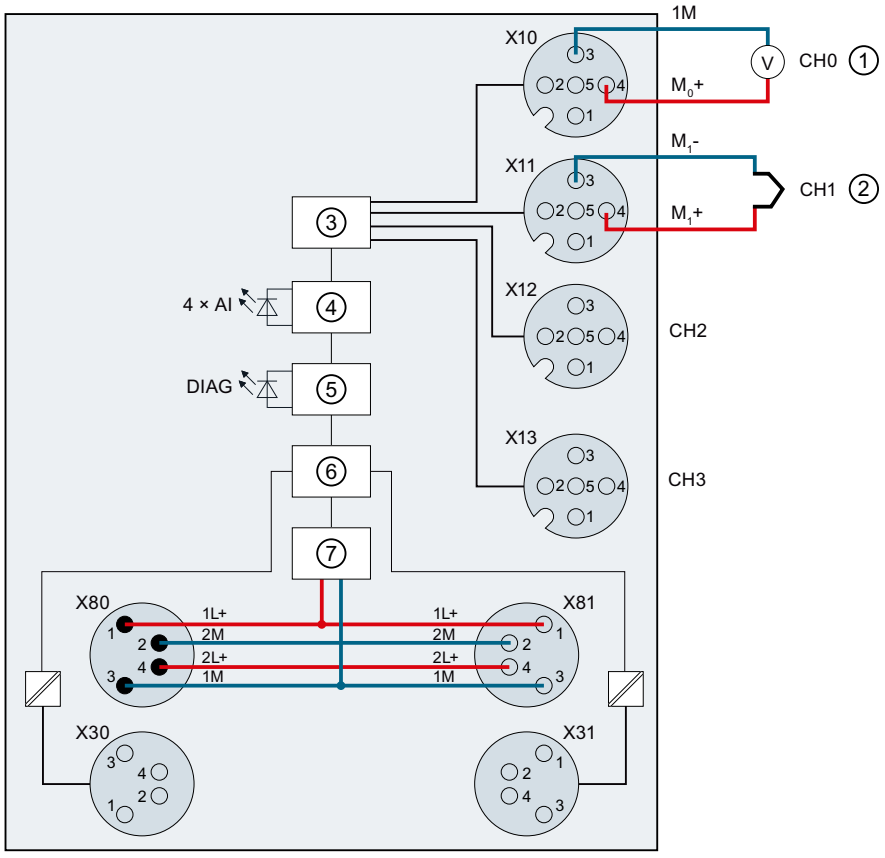
Figure 2-106 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

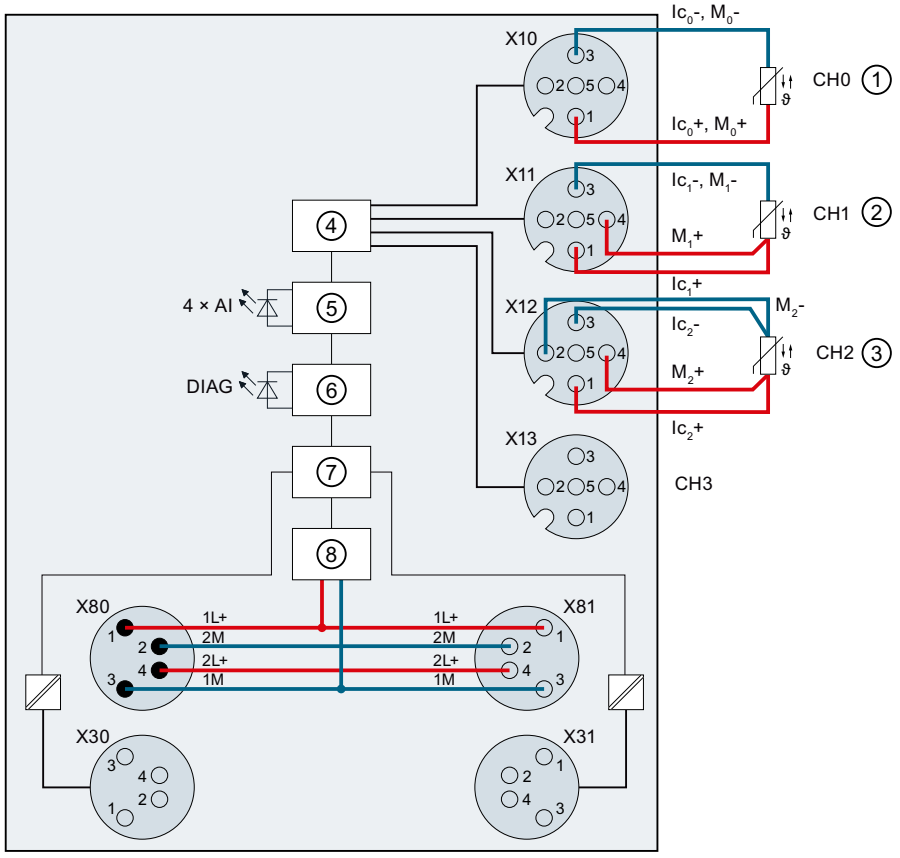
The figure below shows an example of the pin assignment for voltage measurement and thermocouple measurement.



①	Voltage measurement	X30	Infeed of the ET-Connection
②	Thermocouple measurement	X31	Loop-through of the ET-Connection
③	Multiplexer	1L+	Supply voltage 1L+ (non-switched)
④	Analog-to-digital converter (ADC)	1M	Ground 1M (non-switched)
⑤	Microcontroller	2L+	Load voltage 2L+ (switched)
⑥	ET-Connection interface	2M	Ground 2M (switched)
⑦	Internal supply voltage	M_n+	Measuring input positive, channel n
X10 bis X13	Channels 0 to 3	M_n-	Measuring input negative, channel n
X80	Infeed of supply voltages	AI	Channel status LEDs (0, 1, 2 and 3) (green)
X81	Loop-through of supply voltages	DIAG	LED diagnostic status (red/green)

Figure 2-107 Example of voltage and thermocouple measurement

The figure below shows an example of the pin assignment for thermal resistance and resistance measurement.



①	RTD/R 2-wire connection	X30	Infeed of the ET-Connection
②	RTD/R 3-wire connection	X31	Loop-through of the ET-Connection
③	RTD/R 4-wire connection	1L+	Supply voltage 1L+ (non-switched)
④	Multiplexer	1M	Ground 1M (non-switched)
⑤	Analog-to-digital converter (ADC)	2L+	Load voltage 2L+ (switched)
⑥	Microcontroller	2M	Ground 2M (switched)
⑦	ET-Connection interface	M_n+	Measuring input positive, channel n
⑧	Internal supply voltage	M_n-	Measuring input negative, channel n
X10 to X13	Channels 0 to 3	Ic_n+, Ic_n-	Current output, current feed, RTD/R channel n
X80	Infeed of supply voltages	AI	Channel status LEDs (0, 1, 2 and 3) (green)
X81	Loop-through of supply voltages	DIAG	LED diagnostic status (red/green)

Figure 2-108 Example of resistance and thermal resistance measurement

4.2 Pin assignment

NOTE

Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for analog inputs

The tables below show the pin assignments of the four sockets for connection of the analog inputs.

Table 2-226 Pin assignment for thermocouple + voltage measurement

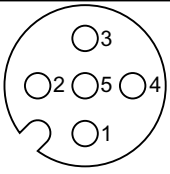
Pin	Assignment **X10 ... X13- sockets for analog inputs (thermocouple)**	Front view of the sockets
1	Reserved	
2	Reserved	
3	Measuring input M_0-: Connector X10 Measuring input M_1-: Connector X11 Measuring input M_2-: Connector X12 Measuring input M_3-: Connector X13	
4	Measuring input M_0+: Connector X10 Measuring input M_1+: Connector X11 Measuring input M_2+: Connector X12 Measuring input M_3+: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

Table 2-227 Pin assignment for analog inputs (RTD/R 2-wire connection)

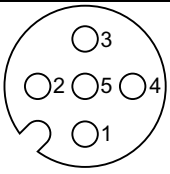
Pin	Assignment **X10 ... X13 - sockets for analog inputs (RTD/R 2-wire connection)**	Front view of the sockets
1	Measurement cable Ic_0+, M_0+: Connector X10 Measurement cable Ic_1+, M_1+: Connector X11 Measurement cable Ic_2+, M_2+: Connector X12 Measurement cable Ic_3+, M_3+: Connector X13	
2	Reserved	
3	Measurement cable Ic_0-, M_0-: Connector X10 Measurement cable Ic_1-, M_1-: Connector X11 Measurement cable Ic_2-, M_2-: Connector X12 Measurement cable Ic_3-, M_3-: Connector X13	
4	Reserved	
5	Functional earth FE	
Shield	Functional earth FE	

Table 2-228 Pin assignment for analog inputs (RTD/R 3-wire connection)

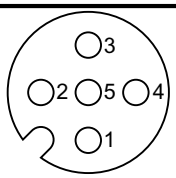
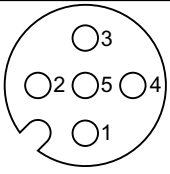
Pin	Assignment **X10 ... X13 - sockets for analog inputs (RTD/R 3-wire connection)**	Front view of the sockets
1	Constant current cable Ic_0+: Connector X10 Constant current cable Ic_1+: Connector X11 Constant current cable Ic_2+: Connector X12 Constant current cable Ic_3+: Connector X13	
2	Reserved	
3	Measurement cable Ic_0-, M_0-: Connector X10 Measurement cable Ic_1-, M_1-: Connector X11 Measurement cable Ic_2-, M_2-: Connector X12 Measurement cable Ic_3-, M_3-: Connector X13	
4	Measuring input M_0+: Connector X10 Measuring input M_1+: Connector X11 Measuring input M_2+: Connector X12 Measuring input M_3+: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

Table 2-229 Pin assignment for analog inputs (RTD/R 4-wire connection)

Pin	Assignment **X10 ... X13 - sockets for analog inputs (RTD/R 4-wire connection)**	Front view of the sockets
1	Constant current cable Ic_0+: Connector X10 Constant current cable Ic_1+: Connector X11 Constant current cable Ic_2+: Connector X12 Constant current cable Ic_3+: Connector X13	
2	Measuring line M_0-: Connector X10 Measuring line M_1-: Connector X11 Measuring line M_2-: Connector X12 Measuring line M_3-: Connector X13	
3	Constant current cable Ic_0-: Connector X10 Constant current cable Ic_1-: Connector X11 Constant current cable Ic_2-: Connector X12 Constant current cable Ic_3-: Connector X13	
4	Measuring input M_0+: Connector X10 Measuring input M_1+: Connector X11 Measuring input M_2+: Connector X12 Measuring input M_3+: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

NOTE

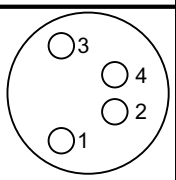
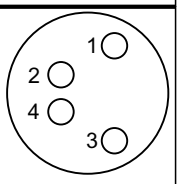
Coupler plug for RTD measurement

For RTD measurements, use a coupler plug with gold-plated contacts. Other materials can create contact resistance that can result in incorrect measured values.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

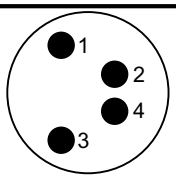
Table 2-230 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the core color of the bus cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

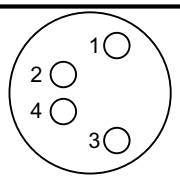
Table 2-231 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the core color of the power cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-232 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the connector for ET-Connection and the connector for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Measurement types and measuring ranges

The table below indicates which measuring range is configurable.

Table 2-233 Measurement type and measuring ranges

Measurement type	Measuring range	Temperature coefficient	Resolution
Deactivated	–	–	–
Voltage	+/- 80 mV	–	Max. 16-bit
• Resistance (2-wire connection) • Resistance (3-wire connection) • Resistance (4-wire connection)	• 150 Ω • 300 Ω	–	Max. 15-bit
• Thermal resistor (2-wire connection) • Thermal resistor (3-wire connection) • Thermal resistor (4-wire connection)	• Pt 100 climatic range • Pt 100 standard range • Pt 1000 climatic range • Pt 1000 standard range	• Pt 0.003851 (EN 60751-) • Pt 0.003916 • Pt 0.003902 • Pt 0.00392 • Pt 0.00385	Max. 16-bit incl. sign
	• Ni 100 climatic range • Ni 100 standard range • Ni 1000 climatic range • Ni 1000 standard range	• Ni 0.00618 • Ni 0.00672	Max. 16-bit incl. sign
Thermocouple	Type: B, C, E, J, K, L, N, R, S, T, U	–	Max. 16-bit incl. sign

5.2 Parameters

Parameters of the analog input module AI 4xRTD/TC 4xM12

Specify the module properties with the various parameters in the course of the parameter assignment of the module with STEP 7. The following table lists the configurable parameters. The effective range of the configurable parameters depends on the type of configuration. The following configurations are possible:

- Distributed mode on PROFINET IO
- Distributed mode with PROFIBUS DP
- Central operation with an ET 200SP CPU

NOTICE
Match of encoder and parameters The default setting of the analog inputs is voltage measurement (± 80 mV). Make sure that the connected encoders and the selected parameters match.

Parameters and presettings of the analog input module.

The table below shows the PROFINET IO and PROFIBUS DPparameters for the analog input module AI 4xRTD/TC 4xM12 for configuration with GSD file.

Table 2-234 Configurable parameters and their default (GSD)

Parameter	Value range	Default	Effective range with configuration software e.g. STEP 7 (TIA Portal)	
			GSD file PROFINET IO	GSD file PROFIBUS DP
Temperature unit	• Degrees Celsius • Degrees Fahrenheit • Kelvin	Degrees Celsius	Module	Module
Type/range of measurement	• Disabled	Voltage ±80 mV	Channel	Channel
	• Voltage ±80 mV			
	Resistance (2-, 3-, 4-wire connection) • 150 Ω • 300 Ω			
	Thermal resistor (2-, 3-, 4-wire connection) • Pt 100 climatic range • Pt 1000 climatic range • Pt 100 standard range • Pt 1000 standard range • Ni 100 climatic range • Ni 1000 climatic range • Ni 100 standard range • Ni 1000 standard range			

1 Interference frequency suppression: Noise at 400 Hz is automatically included in the filtering at 50 Hz.

2 For 2-wire connection only

Parameter	Value range	Default	Effective range with configuration software e.g. STEP 7 (TIA Portal)	
			GSD file PROFINET IO	GSD file PROFIBUS DP
Type/range of measurement	Thermocouple • Type B • Type N • Type E • Type R • Type S • Type J • Type L • Type T • Type K • Type U • Type C	Voltage ±80 mV	Channel	Channel
Temperature coefficient	• Pt 0.003851 (EN 60751) • Pt 0.003916 • Pt 0.003902 • Pt 0.00392 • Pt 0.00385 • Ni 0.00618 • Ni 0.00672	Pt 0.003851 (EN 6075-1)	Channel	Channel
Reference junction	• Fixed reference temperature • Dynamic reference temperature • Internal reference junction • No compensation	Internal reference junction	Channel	Channel
Fixed reference temperature	-2290 ... 3276	0	Channel	Module
Smoothing	• None • Weak • Medium • Strong	None	Channel	Channel
Interference frequency suppression	• 60 Hz (16.6 ms) • 50 Hz (20 ms)[1] • 16.6 Hz (60 ms)	50 Hz (20 ms)[1]	Channel	Channel
Diagnostics: Reference junction	• Disable • Enable	Disable	Channel	Channel
Diagnostics: Wire break	• Disable • Enable	Disable	Channel	Channel
Diagnostics Overflow/underflow diagnostics	• Disable • Enable	Disable	---	Channel
Diagnostics: Underflow	• Disable • Enable	Disable	Channel	---
Diagnostics: Overflow	• Disable • Enable	Disable	Channel	---
Conductor resistance [mΩ][2]	0 ... 50000 mΩ	0	Channel	---
Hardware interrupt high limit 1	• Disable • Enable	Disable	Channel	---

1 Interference frequency suppression: Noise at 400 Hz is automatically included in the filtering at 50 Hz.

2 For 2-wire connection only

Parameter	Value range	Default	Effective range with configuration software e.g. STEP 7 (TIA Portal)	
			GSD file PROFINET IO	GSD file PROFIBUS DP
Hardware interrupt low limit 1	• Disable • Enable	Disable	Channel	---
Hardware interrupt high limit 2	• Disable • Enable	Disable	Channel	---
Hardware interrupt low limit 2	• Disable • Enable	Disable	Channel	---
High limit 1	The value range depends on the measurement type. The value range (min./max.) permitted for the measurement type is listed in the table 4-3 **Value ranges of the hardware interrupts**.	27648	Channel	---
Low limit 1		0	Channel	---
High limit 2		27648	Channel	---
Low limit 2		0	Channel	---

1 Interference frequency suppression: Noise at 400 Hz is automatically included in the filtering at 50 Hz.

2 For 2-wire connection only

NOTE

Unused channels

"Deactivate" unused inputs in the parameter assignment to shorten the cycle time of the module.

A deactivated input always returns the value $7FFF_H$.

Value ranges of the hardware interrupts

The table below shows the permitted value ranges of the hardware interrupts for the measurement type.

Table 2-235 Value ranges of the hardware interrupts

Measurement type	Measuring range	Low limit	High limit	Unit
Voltage	± 80 mV	-94.071	94.068	mV
		-32511	32510	Decimal
Resistance	150 ohm	0.01	176.38	Ω
		2	32510	Decimal
	300 ohm	0.01	352.76	Ω
		1	32510	Decimal
Thermal resistance	Pt 100 Std. Pt 1000 Std.	-242.9	999.9	°C
		-2429	9999	Decimal
		-405.3	1831.9	F
		-4053	18319	Decimal
		30.3	1273.1	K
		303	12731	Decimal
	Pt 100 Cl.	-144.99	154.99	°C

Measurement type	Measuring range	Low limit	High limit	Unit
Thermal resistance	Pt 1000 Cl.	-14499	15499	Decimal
		-228.99	310.99	F
		-22899	31099	Decimal
	Ni 100 Std. Ni 1000 Std.	-104.9	294.9	°C
		-1049	2949	Decimal
		-156.9	562.9	F
		-1569	5629	Decimal
		168.3	568.1	K
		1683	5681	Decimal
	Ni 100 Cl. Ni 1000 Cl.	-104.99	154.99	°C
		-10499	15499	Decimal
		-156.99	310.99	F
		-15699	31099	Decimal
Thermocouple	Type B	-119.9	2069.9	°C
		-1199	20699	Decimal
		-183.9	3276.5	F
		-1839	32765	Decimal
		153.3	2343.1	K
		1533	23431	Decimal
	Type N	-269.9	1549.9	°C
		-2699	15499	Decimal
		-453.9	2821.9	F
		-4539	28219	Decimal
		3.3	1823.1	K
		33	18231	Decimal
	Type E	-269.9	1199.9	°C
		-2699	11999	Decimal
		-453.9	2191.9	F
		-4539	21919	Decimal
		3.3	1473.1	K
		33	14731	Decimal
	Types R, S	-169.9	2018.9	°C
		-1699	20189	Decimal
		-273.9	3276.5	F
		-2739	32765	Decimal
		103.3	2292.1	K
		1033	22921	Decimal
	Type J	-209.9	1449.9	°C
		-2099	14499	Decimal
		-345.9	2641.9	F
		-3459	26419	Decimal
		63.3	1723.1	K
		633	17231	Decimal

Measurement type	Measuring range	Low limit	High limit	Unit
Thermocouple	Type L	-199.9	1149.9	°C
		-1999	11499	Decimal
		-327.9	2101.9	F
		-3279	21019	Decimal
		73.3	1423.1	K
		733	14231	Decimal
	Type T	-269.9	539.9	°C
		-2699	5399	Decimal
		-453.9	1003.9	F
		-4539	10039	Decimal
		3.3	813.1	K
		33	8131	Decimal
	Type K	-269.9	1621.9	°C
		-2699	16219	Decimal
		-453.9	2951.5	F
		-4539	29515	Decimal
		3.3	1895.1	K
		33	18951	Decimal
	Type U	-199.9	849.9	°C
		-1999	8499	Decimal
		-327.9	1561.9	F
		-3279	15619	Decimal
		73.3	1123.1	K
		733	11231	Decimal
	Type C	-119.9	2499.9	°C
		-1199	24999	Decimal
		-183.9	3276.5	F
		-1839	32765	Decimal
		153.3	2773.1	K
		1533	27731	Decimal

"Fixed reference temperature" parameter for thermocouples

The parameter "Fixed reference temperature" can only be set if you selected = "Fixed Reference Temperature" for the "Reference junction" parameter.

The following table shows the value ranges for the "reference temperature" for thermocouples.

Table 2-236 Value ranges for the "reference temperature" for thermocouples.

Temperature unit	Temperature		Decimal	
	Min.	Max	Min.	Max
Celsius	-145.0	155	-1450	1550
Fahrenheit	-229.0	311.0	-2290	3110
Kelvin	128.2	327.6	1282	3276

5.3 Explanation of the parameters

Temperature unit

You use this parameter to set the temperature unit with which you want to measure the temperature.

Type/range of measurement

You use this parameter to set the measurement type or the measuring range for acquiring the measured values.

NOTE

Unused channels

"Deactivate" unused channels in the parameter assignment to improve the cycle time of the module.

A deactivated channel always returns the value $7FFF_H$.

Temperature coefficient (for RTD)

The temperature coefficient depends on the chemical composition of the material. In Europe, only one value is used per sensor type (default value).

The correction factor for the temperature coefficient (α value) specifies how much the resistance of a certain material changes when the temperature is raised by 1 °C.

The further values facilitate sensor-specific setting of the temperature coefficient and enhance accuracy.

Reference junction

If the measuring point is subjected to a different temperature than the reference junction (free ends of the thermocouple at the connection point), a thermal voltage arises between the free ends. The level of the thermal voltage depends:

- On the temperature difference between the measuring point and the free ends
- On the type of material combination of the thermocouple

Since a temperature difference is always detected with a thermocouple, the temperature of the reference junction has to be determined in order to determine the temperature of the measuring point.

The possible compensation types that can be parameterized via the parameter "reference junction" are set out in the table below.

Table 2-237 Parameterizable compensation types for the "reference junction" parameter

Compensation type	Explanation
Fixed reference temperature	**Properties** With this type of compensation, the reference junction temperature is stored as a fixed value. **Principle of operation** The reference junction temperature is specified in the "fixed reference temperature" parameter.

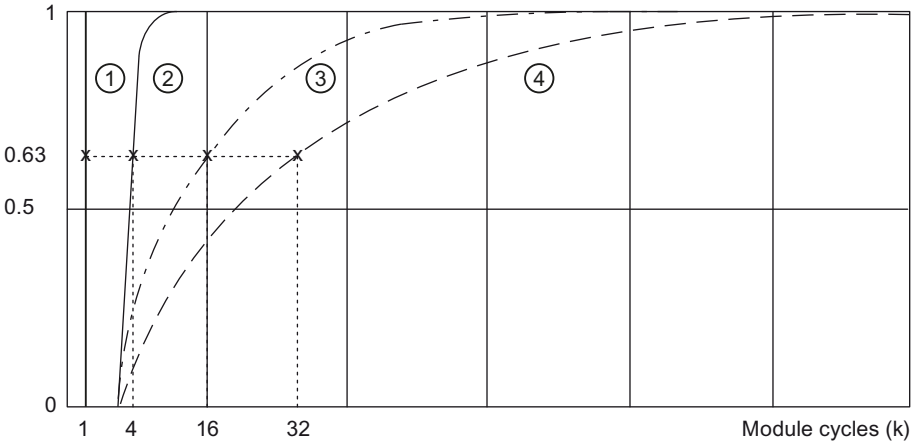
Compensation type	Explanation
	The possible value range is displayed in the Value ranges for the "reference temperature" for thermocouples.. The configured reference junction temperature applies to all channels of the module that you have selected for this type of compensation. **Wiring** Connect the thermocouples to terminals 3 and 4 from the reference junction with copper cables. If you detect the reference junction temperature directly at the M12 connector of the AI 4xRTD/TC 4xM12, you can also connect the thermocouples directly or with compensating lines.
Dynamic reference temperature	**Properties** With this compensation, the reference junction temperature can be measured via an external module of another station. **Principle of operation** The reference junction temperature is transferred by means of SFB 53 by the data records 192 - 195 from the CPU to the AI 4xRTD/TC 4xM12 electronic module. Each channel that you select for this type of compensation can have its own reference junction temperature assigned to it via the user program. For more information, see section Structure of a data record for dynamic reference temperature (Page 31). **Wiring** Connect the thermocouples to Terminals 3 and 4 from the reference junction with copper cables. If you detect the reference junction temperature directly at the M12 connector of the AI 4xRTD/TC 4xM12, you can also connect the thermocouples directly or with compensating lines.
Internal reference junction	**Properties** With this compensation type, the reference junction temperature is determined with an internal temperature sensor that is integrated in the AI 4xRTD/TC 4xM12 electronic module. Note: Take the reaction time to changes of the ambient temperature into account. **Principle of operation** The reference junction temperature is detected through an internal temperature sensor. All channels of the AI 4xRTD/TC 4xM12 that you select for this type of compensation receive the same reference junction temperature. **Wiring** Connect the thermocouples directly or with compensating lines to the AI 4xRTD/TC 4xM12.
No compensation	**Properties** With this compensation type, the reference junction temperature of the thermocouples is measured outside the AI 4xRTD/TC 4xM12 electronic module. You can, for example, connect a compensating box to the thermocouple for this purpose. **Principle of operation** The temperature of the reference junction for this type of compensation is specified as 0 °C. This can be achieved by using a compensating box. A separate compensating box is required for each thermocouple. **Wiring** Connect the compensating box with theAI 4xRTD/TC 4xM12 with copper cables. Note: Thermocouples of Type B do not require a compensating box up to a reference junction temperature of 50 °C.

Smoothing

The purpose of smoothing is to filter out interferences. The greater the smoothing factor, the better the filter effect. This is technically implemented in the form of a digital filter. The smoothing can be set in 4 levels. The smoothing factor k is equal to the number of module cycles. The time constant of the smoothing filter is the product of the smoothing factor k and the cycle time of the I/O module. The greater the smoothing, the greater the time constant of the filter.

Smoothing time = number of module cycles (k) × cycle time of the module.

The following figure shows how many module cycles it takes for the smoothed analog value to approach 100%, depending on the configured smoothing. This is valid for all signal changes at the analog input.



① No smoothing (k = 1)
② Weak (k = 4)
③ Medium (k = 16)
④ Strong (k = 32)

Figure 2-109 Smoothing

Interference frequency suppression

This parameter suppresses interference for analog input modules which is caused by the frequency of the alternating voltage network in use.

The frequency of the alternating voltage network may negatively affect the measured value, in particular when measuring in the low voltage range and with thermocouples. With this parameter, the user specifies the line frequency that is predominant in the plant.

Diagnostics: Reference junction

Enabling of the reference junction diagnostics if the reference temperature of the reference junction needs to be determined for the TC channel being operated.

Diagnostics: Wire break

Enabling of the diagnostics if the analog input module has no current flow or the current is too weak for measurement at the correspondingly configured input.

NOTE

Wire break diagnostics

With analog input channels, wire break diagnostics is not possible for the measurement type voltage ± 80 mV.

The following table shows the diagnostics that may occur on wire break.

Table 2-238 Diagnostics with RTD/R

Diagnostics: Wire break	Diagnostics: Overflow	Diagnostics underflow	Event	Process data	Diagnostics alarm per channel
Enabled	Disabled	Disabled	Wire break	0x7FFF	Wire break
Disabled	Disabled	Enabled	Wire break	0x7FFF	-
Disabled	Enabled	Disabled	Wire break	0x7FFF	High limit violated
Disabled	Enabled	Enabled	Wire break	0x7FFF	High limit violated
Disabled	Disabled	Disabled	Wire break	0x7FFF	-

Diagnostics: Overflow/Underflow (for PROFIBUS only)

Enabling of the diagnostics when the measured value exceeds the overrange or falls below the underrange.

Diagnostics: Underflow

Enabling of the diagnostics when the measured value falls below the underrange.

Diagnostics: Overflow

Enabling of the diagnostics when the measured value exceeds the overrange.

Conductor resistance

Parameters for the measurement types resistor and thermal resistor (2-wire connection).

The parameter is used to compensate the conductor resistance without interfering with the sensor wiring.

Hardware interrupt high/low limit 1 or 2

Enabling of a hardware interrupt when the high limit 1 or 2 or the low limit 1 or 2 is violated.

Requirement: An OB 4x must be assigned to the CPU/device.

Additional information on the structure of hardware interrupts is available in the section Interrupts (Page 35).

High/low limit 1 or 2

Specify a threshold at which a hardware interrupt is triggered when it is exceeded or undershot.

See also

Parameters (Page 22)

5.4 Structure of a data record for dynamic reference temperature

The **WRREC** instruction is used to transfer the reference junction temperature via data record 192 to data record 195 to the module.

The description of the WRREC instruction can be found in the online help from STEP 7.

If you have set the "Dynamic reference temperature" value for the "Reference junction" parameter, the module expects a new data record at least every 5 minutes. If the module does not receive a new data record within this time, it generates the "Reference channel error" diagnostics message.

Assignment of data record and channel

The assignment of the channels is:

- Data record 192 for channel 0
- Data record 193 for channel 1
- Data record 194 for channel 2
- Data record 195 for channel 3

Structure of data record 192 for dynamic reference temperature

The following figure shows you an example of the structure of data record 192 for channel 0. The structure for data records 193 to 195 is identical.

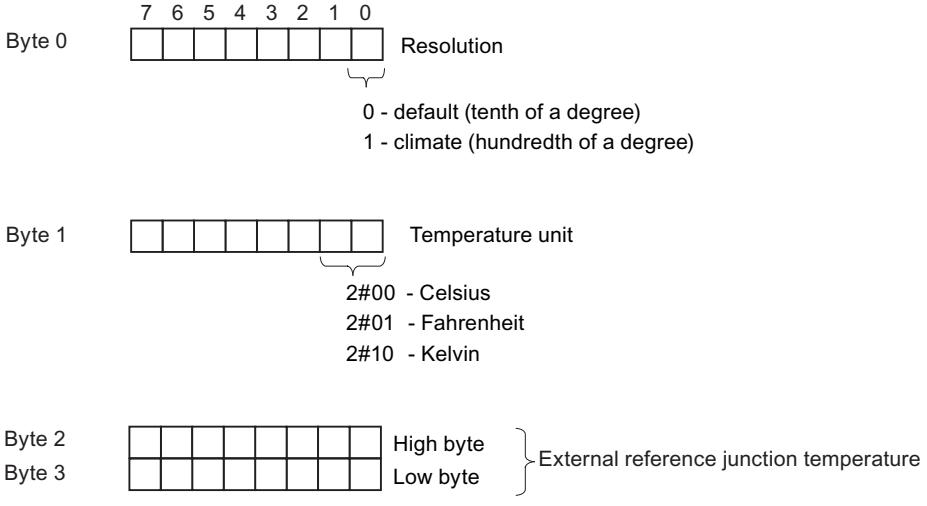


Figure 2-110 Structure of data record 192

Valid values for fixed temperature compensation

The selectable values must lie within the permitted value range. The resolution of the valid values for temperature compensation is a tenth of a degree

Table 2-239 Valid values for temperature compensation via data record

Temperature unit	Decimal	Hexadecimal
Celsius (default)	-1450 ... 1550	$FA56_H$ ... $60E_H$
Fahrenheit (default)	-2290 ... 3110	$F70E_H$ ... $C26_H$
Kelvin (default)	1282 ... 3276	502_H ... CCC_H
Celsius (climatic)	-14500 ... 15500	$C75C_H$ ... $3C8C_H$
Fahrenheit (climatic)	-22900 ... 31100	$A68C_H$ ... $797C_H$
Kelvin (climatic)	12820 ... 32760	3214_H ... $7FF8_H$

NOTE

Thanks to the flexible content of the data records DS 192 - DS 195, you can use a separate reference junction for each channel. The channels can also be combined via the user program in such a way that they use the same reference junction. To this end, you need to specify the same temperature value in the data records for all channels operating with the same reference function temperature.

Additional information

You can find more information on compensation of the reference junction temperature via data record in the function manual SIMATIC analog value processing (https://support.industry.siemens.com/cs/ww/en/view/67989094).

5.5 Address space

The tables below shows the assignment of the address space for the analog input module AI 4xRTD/TC 4xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-240 Address space in the configuration mode AI with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x									Input value channel 0
IB x +1									
IB x +2									Input value channel 1
IB x +3									
IB x +4									Input value channel 2
IB x +5									

* 0 = Value read in at channel is incorrect

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
IB x +6									Input value channel 3
IB x +7									
IB x +8	0	0	0	0					Value status (QI) for inputs on channels 0 ... 3*

* 0 = Value read in at channel is incorrect

Configuration options of the AI 4xRTD/TC 4xM12 analog input module

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

If you enable the value status for the analog input module, then a byte is additionally assigned in the input address space. Bits 0 to 3 in this byte are assigned to a channel and provide information on the validity of the analog value. The value status is independent of whether or not diagnostics was configured.

Bit = 1:

- No error on channel.

Bit = 0:

- Channel is deactivated
- Incorrect wiring
- Applied value at channel is incorrect

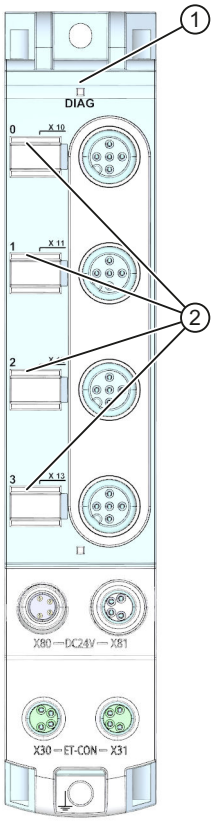
Interrupts/diagnostics alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED display (status and error displays) of the AI 4xRTD/TC 4xM12 analog input module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0, 1, 2 and 3) (green)

Figure 2-111 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 37).

DIAG LED

Table 2-241 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LED for the channel status

Table 2-242 Status display of the LEDs 0, 1, 2 and 3

LED 0, 1, 2 and 3	Meaning
☐ Off	• Channel deactivated • Channel activated and incorrect parameter assignment • Parameter error possible with GSD
■ On	• Channel activated and correct parameter assignment

6.2 Interrupts

The AI 4xRTD/TC 4xM12 analog input module supports diagnostic and hardware interrupts.

Diagnostic interrupt

The table below shows the events for which the analog input module returns a diagnostic interrupt, depending on the parameter assignment.

Table 2-243 Diagnostic interrupts

Measurement type	Diagnostics						
	Wire break	High limit violated	Low limit violated	Error	Parameter assign-ment error	Reference channel error	Hardware interrupt lost
Voltage	-	x	x	x	x	-	x
Resistance	x	x	-	x	x	-	x
Thermal res-istor	x	x	x	x	x	-	x
Thermocouple	x	x	x	x	x	x	x

Hardware interrupt

The analog input module generates a hardware interrupt with the following events:

- Low limit 1 violated
- High limit 1 violated
- Low limit 2 violated
- High limit 2 violated

Detailed information on the event is available in the hardware interrupt organization block with the instruction "RALRM" (Read additional interrupt information) and in the STEP 7 online help.

The start information of the organization block includes information on which channel of the analog input module triggered the hardware interrupt.

NOTE

High limit violation of 2 limits

If two limits are violated at the same time, limit 1 is always signaled first, followed by limit 2.

The figure below shows the assignment to the bits of the local data double word 8.

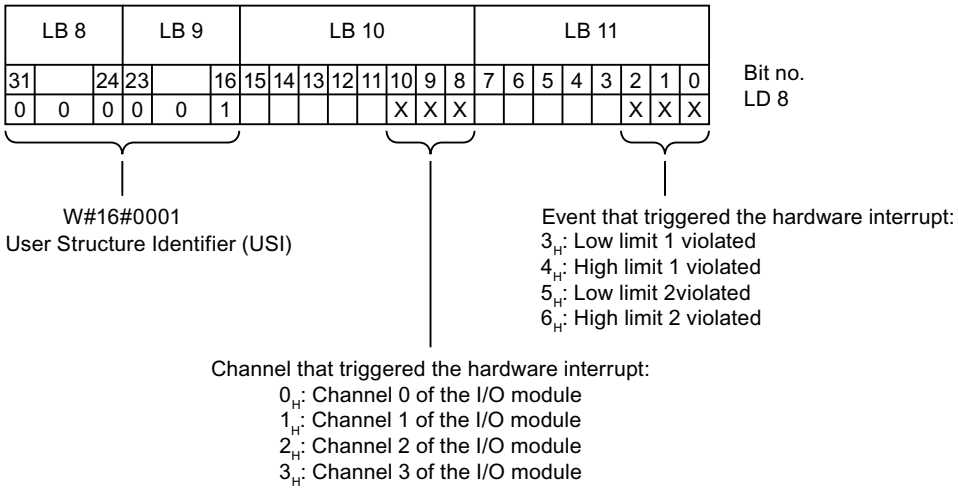


Figure 2-112 Start information of the organization block

Structure of the additional interrupt information

Table 2-244 Structure of the additional interrupt information

Data block name	Contents	Comment	Bytes
USI (User Structure Identifier)	W#16#0001	Additional interrupt info for hardware interrupts of the I/O module	2
The channel that triggered the hardware interrupt follows.			
Channel	B#16#00 to B#16#03	Number of channel which triggered the event	1
The error event that triggered the hardware interrupt follows.			
Event	B#16#03	Low limit 1 violated	1

Data block name	Contents	Comment	Bytes
Event	B#16#04	High limit 1 violated	1
	B#16#05	Low limit 2 violated	
	B#16#06	High limit 2 violated	

6.3 Diagnostics alarms

A diagnostics alarm is output for each diagnostics event. The DIAG LED flashes red on the analog output module. The diagnostics alarms are listed in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

The following tables set out the diagnostics alarms for the set measuring range.

Table 2-245 Diagnostics alarms, their meaning and remedies

Diagnostics alarm	Error code	Meaning	Solution
Wire break	6_H	Wire break between the module and sensor	Connect the cable
		Channel not connected (open)	• Deactivate diagnostics • Connect the channel • Deactivate channel
High limit violated[1]	7_H	Value is above overrange.	Correct interplay between module and sensor
		Wire break[2]	See wire break
Low limit violated[1]	8_H	Value is below underrange.	Correct interplay between module and sensor
Error	9_H	Value is significantly above or below underrange/overrange.	• Correct interplay between module and sensor • Deactivate the unused channels in the parameter assignment.
Parameter error	10_H	• The module cannot evaluate parameters for the channel • Module parameter assignment is faulty	Correct the parameter assignment (wire break diagnostics set only with the permitted measuring ranges).
Reference channel error	15_H	Data record 192 ... 195 was not correctly cyclically received within 5 min	Write data record 192 ... 195

1 = The alarm depends on the configured measuring range.

2 = For resistor and thermal resistor measuring ranges with deactivated diagnostics for "wire break", this is reported by the "Violation of high limit" diagnostic.

3 A diagnostics alarm is output for a signed firmware update.

Diagnostics alarm	Error code	Meaning	Solution
Hardware interrupt lost	16_H	At least one hardware interrupt was not signaled because too many hardware interrupts are pending.	Correct the program or the process
Security event: Firmware has been successfully downloaded and activated for installation.[3]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[3]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

1 = The alarm depends on the configured measuring range.

2 = For resistor and thermal resistor measuring ranges with deactivated diagnostics for "wire break", this is reported by the "Violation of high limit" diagnostic.

3 A diagnostics alarm is output for a signed firmware update.

Technical specifications

7

7.1 Technical specifications

Technical specifications of the AI 4xRTD/TC 4xM12 analog input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7144-5KD50-0BA0/td?dl=en).

Article number	6ES7144-5KD50-0BA0
General information	
Product type designation	AI 4xRTD/TC
HW functional status	FS03
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V16 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 and higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.34
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Input current	
Current consumption (rated value)	30 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Power loss	
Power loss, typ.	1.5 W
Analog inputs	
Number of analog inputs	4
• For voltage measurement	4
• For resistance/resistance thermometer measurement	4
• For thermocouple measurement	4

Article number	6ES7144-5KD50-0BA0
permissible input voltage for voltage input (destruction limit), max.	15 V
Constant measurement current for resistance-type transmitter, typ.	230 ... 300 µA
Cycle time (all channels), min.	90 ms
Technical unit for temperature measurement adjustable	Yes; Degrees Celsius / degrees Fahrenheit / Kelvin
Input ranges (rated values), voltages	
• -80 mV to +80 mV	Yes; 16 bit incl. sign
– Input resistance (-80 mV to +80 mV)	10 MΩ
Input ranges (rated values), thermocouples	
• Type B	Yes; 16 bit incl. sign
– Input resistance (Type B)	10 MΩ
• Type C	Yes; 16 bit incl. sign
– Input resistance (Type C)	10 MΩ
• Type E	Yes; 16 bit incl. sign
– Input resistance (Type E)	10 MΩ
• Type J	Yes; 16 bit incl. sign
– Input resistance (type J)	10 MΩ
• Type K	Yes; 16 bit incl. sign
– Input resistance (Type K)	10 MΩ
• Type L	Yes; 16 bit incl. sign
– Input resistance (Type L)	10 MΩ
• Type N	Yes; 16 bit incl. sign
– Input resistance (Type N)	10 MΩ
• Type R	Yes; 16 bit incl. sign
– Input resistance (Type R)	10 MΩ
• Type S	Yes; 16 bit incl. sign
– Input resistance (Type S)	10 MΩ
• Type T	Yes; 16 bit incl. sign
– Input resistance (Type T)	10 MΩ
• Type U	Yes; 16 bit incl. sign
– Input resistance (Type U)	10 MΩ
Input ranges (rated values), resistance thermometer	
• Ni 100	Yes; Standard/climate
– Input resistance (Ni 100)	10 MΩ
• Ni 1000	Yes; Standard/climate
– Input resistance (Ni 1000)	10 MΩ
• Pt 100	Yes; Standard/climate
– Input resistance (Pt 100)	10 MΩ
• Pt 1000	Yes; Standard/climate
– Input resistance (Pt 1000)	10 MΩ

Article number	6ES7144-5KD50-0BA0
Input ranges (rated values), resistors	
• 0 to 150 ohms	Yes
– Input resistance (0 to 150 ohms)	10 MΩ
• 0 to 300 ohms	Yes
– Input resistance (0 to 300 ohms)	10 MΩ
Thermocouple (TC)	
Temperature compensation	
– parameterizable	Yes
– internal temperature compensation	Yes
– external temperature compensation with compensations socket	Yes
– dynamic reference temperature value	Yes
– fixed reference temperature	Yes
Cable length	
• shielded, max.	30 m
Analog value generation for the inputs	
Measurement principle	integrating
Integration and conversion time/resolution per channel	
• Resolution with overrange (bit including sign), max.	16 bit
• Integration time, parameterizable	Yes; channel by channel
• Integration time (ms)	16.7 / 20 / 60
• Basic conversion time, including integration time (ms)	18 / 21 / 61 ms
– additional conversion time for wire-break monitoring	4 ms
– additional conversion time for resistance measurement	2 ms
• Interference voltage suppression for interference frequency f1 in Hz	60 / 50 / 16.7
Smoothing of measured values	
• parameterizable	Yes
• Step: None	Yes; 1x cycle time
• Step: low	Yes; 4x cycle time
• Step: Medium	Yes; 16x cycle time
• Step: High	Yes; 32x cycle time
Encoder	
Connection of signal encoders	
• for resistance measurement with two-wire connection	Yes
• for resistance measurement with three-wire connection	Yes
• for resistance measurement with four-wire connection	Yes
Errors/accuracies	
Linearity error (relative to input range), (+/-)	0.025 %

Article number	**6ES7144-5KD50-0BA0**
Temperature error (relative to input range), (+/-)	0.01 %/K
Crosstalk between the inputs, max.	-70 dB
Repeat accuracy in steady state at 25 °C (relative to input range), (+/-)	0.01 %; 0.02% for Pt1000
Temperature error of internal compensation	±4 °C
Operational error limit in overall temperature range	
• Voltage, relative to input range, (+/-)	0.35 %
• Resistance, relative to input range, (+/-)	0.25 %
• Resistance thermometer, relative to input range, (+/-)	0.25 %
• Thermocouple, relative to input range, (+/-)	TC type E, J, K, N, C, U, L: 0.35 %; TC type R, S, T: 0.4 %; TC type B: 0.45 %
Basic error limit (operational limit at 25 °C)	
• Voltage, relative to input range, (+/-)	0.25 %
• Resistance, relative to input range, (+/-)	0.15 %
• Resistance thermometer, relative to input range, (+/-)	0.15 %
• Thermocouple, relative to input range, (+/-)	0.25 %
Interference voltage suppression for f = n x (f1 +/- 0.5 %), f1 = interference frequency	
• Series mode interference (peak value of interference < rated value of input range), min.	40 dB
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
• Limit value alarm	Yes; Parameterizable
Diagnoses	
• Wire-break	Yes; Not for ±80 mV
• Overflow/underflow	Yes
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67

Article number	**6ES7144-5KD50-0BA0**
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Suitable for applications according to AMS 2750	Yes; Declaration of Conformity, see online support entry 109757262
Suitable for applications according to CQI-9	Yes; Based on AMS 2750 E
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	168 g

Dimension drawing

A

A.1 Dimension drawing

The figure below shows the dimension drawing of the AI 4xRTD/TC 4xM12 analog input module in the front and side view.

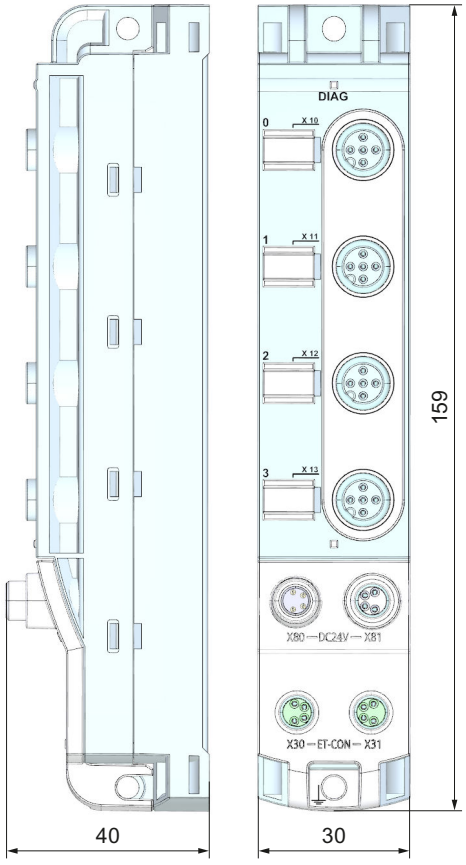


Figure 2-113 Dimension drawing

Representation of analog values

B

B.1 Representation of analog values in voltage measuring range

The table below lists the decimal and hexadecimal values (codes) of the voltage measuring range.

Table 2-246 Voltage measuring range ± 80 mV

Values		Voltage measuring range	Range
Dec.	**Hex.**	**± 80 mV**	
32767	7FFF	> 94.1 mV	Overflow
32511	7EFF	94.1 mV	Overrange
27649	6C01		
27648	6C00	80 mV	Nominal range
20736	5100	60 mV	
1	1	2.89 µV	
0	0	0 mV	
-1	FFFF	-2.89 µV	
-20736	AF00	-60 mV	
-27648	9400	-80 mV	
-27649	93FF		Underrange
-32512	8100	-94.1 mV	
-32768	8000	< -94.1 mV	Underflow

B.2 Representation of analog values for resistance-based sensors

Resistance-based sensor

The following tables list the decimal and hexadecimal values (codes) of the resistance-based sensor.

Table 2-247 Resistance-based sensor of 150 Ω and 300 Ω

Values		Resistance-based sensor range		Range
Dec.	Hex.	150 Ω	300 Ω	
32767	7FFF	>176.38 Ω	>352.77 Ω	Overflow
32511	7EFF	176.38 Ω	352.77 Ω	Overrange
27649	6C01			
27648	6C00	150 Ω	300 Ω	Nominal range
20736	5100	112.5 Ω	225 Ω	
1	1	5.43 mΩ	10.85 mΩ	
0	0	0 Ω	0 Ω	

NOTE

Negative value for 2-wire connection

A negative value is possible in these constellations:

- Configured conductor compensation > sum of conductor resistance and resistance
- Short-circuit on the input and configured conductor compensation

With a negative value the value $7FFF_H$ is generated. The diagnostic message "Violation of high limit" is signaled for the channel in question.

B.3 Representation of analog values for thermal resistors

The tables below list the decimal and hexadecimal values (codes) of the thermal resistors.

Table 2-248 Thermal resistor Pt 100, Pt 1000 Standard

Pt x00 Standard in °C (1 digit = 0.1°C)	Values		Pt x00 Standard in °F (1 digit = 0.1 °F)	Values		Pt x00 Standard in K (1 digit = 0.1 K)	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
>1000.0	32767	7FFF	>1832.0	32767	7FFF	>1273.2	32767	7FFF	Overflow
1000.0 : 850.1	10000 : 8501	2710 : 2135	1832.0 : 1562.1	18320 : 15621	4790 : 3D05	1273.2 : 1123.3	12732 : 11233	31BC : 2BE1	Overrange
850.0 : -200.0	8500 : -2000	2134 : F830	1562.0 : -328.0	15620 : -3280	3D04 : F330	1123.2 : 73.2	11232 : 732	2BE0 : 2DC	Nominal range
-200.1 : -243.0	-2001 : -2430	F82F : F682	-328.1 : -405.4	-3281 : -4054	F32F : F02A	73.1 : 30.2	731 : 302	2DB : 12E	Underrange
<-243.0	-32768	8000	<-405.4	-32768	8000	<30.2	32768	8000	Underflow

Table 2-249 Thermal resistor Pt 100, Pt 1000 Climatic

Pt x00 Climatic in °C (1 digit = 0.01 °C)	**Values**		**Pt x00 Climatic in °F (1 digit = 0.01 °F)**	**Values**		**Range**
	Dec.	**Hex.**		**Dec.**	**Hex.**	
>155.00	32767	7FFF	>311.00	32767	7FFF	Overflow
155.00 : 130.01	15500 : 13001	3C8C : 32C9	311.00 : 266.01	31100 : 26601	797C : 67E9	Overrange
130.00 : -120.00	13000 : -12000	32C8 : D120	266.00 : -184.00	26600 : -18400	67E8 : B820	Nominal range
-120.01 : -145.00	-12001 : -14500	D11F : C75C	-184.01 : -229.00	-18401 : -22900	B81F : A68C	Underrange
<-145.00	-32768	8000	<-229.00	-32768	8000	Underflow

Table 2-250 Thermal resistor Ni 100, Ni 1000 Standard

Ni x00 Standard in °C (1 digit = 0.1 °C)	**Values**		**Ni x00 Standard in °F (1 digit = 0.1 °F)**	**Values**		**Ni x00 Standard in K (1 digit = 0.1 K)**	**Values**		**Range**
	Dec.	**Hex.**		**Dec.**	**Hex.**		**Dec.**	**Hex.**	
> 295.0	32767	7FFF	> 563.0	32767	7FFF	> 568.2	32767	7FFF	Overflow
295.0 : 250.1	2950 : 2501	B86 : 9C5	563.0 : 482.1	5630 : 4821	15FE : 12D5	568.2 : 523.3	5682 : 5233	1632 : 1471	Overrange
250.0 : -60.0	2500 : -600	9C4 : FDA8	482.0 : -76.0	4820 : -760	12D4 : FD08	523.2 : 213.2	5232 : 2132	1470 : 854	Nominal range
-60.1 : -105.0	-601 : -1050	FDA7 : FBE6	-76.1 : -157.0	-761 : -1570	FD07 : F9DE	213.1 : 168.2	2131 : 1682	853 : 692	Underrange
<-105.0	-32768	8000	<-157.0	-32768	8000	< 168.2	32768	8000	Underflow

Table 2-251 Thermal resistor Ni 100, Ni 1000 Climatic

Ni x00 Climatic in °C (1 digit = 0.01 °C)	**Values**		**Ni x00 Climatic in °F (1 digit = 0.01 °F)**	**Values**		**Range**
	Dec.	**Hex.**		**Dec.**	**Hex.**	
>155.00	32767	7FFF	>311.00	32767	7FFF	Overflow
155.00 : 130.01	15500 : 13001	3C8C : 32C9	311.00 : 266.01	31100 : 26601	797C : 67E9	Overrange
130.00 : -60.00	13000 : -6000	32C8 : E890	266.00 : -76.00	26600 : -7600	67E8 : E250	Nominal range
-60.01 : -105.00	-6001 : -10500	E88F : D6FC	-76.01 : -157.00	-7601 : -15700	E24F : C2AC	Underrange
<-105.00	-32768	8000	<-157.00	-32768	8000	Underflow

B.4 Representation of analog values for thermocouples

The tables below list the decimal and hexadecimal values (codes) of the thermocouples.

Table 2-252 Thermocouple type B

Type B in °C	Values		Type B in °F	Values		Type B in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 2070.0	32767	7FFF	> 3276.6	32767	7FFF	> 2343.2	32767	7FFF	Overflow
2070.0 : 1820.1	20700 : 18201	50DC : 4719	3276.6 : 2786.6	32766 : 27866	7FFE : 6CDA	2343.2 : 2093.3	23432 : 20933	5B88 : 51C5	Overrange
1820.0 : 0.0	18200 : 0	4718 : 0000	2786.5 : 32.0	27865 : 320	6CD9 : 0140	2093.2 : 273.2	20932 : 2732	51C4 : 0AAC	Nominal range
-0.1 : -120.0	-1 : -1200	FFFF : FB50	31.9 : -184.0	319 : -1840	013F : F8D0	273.1 : 153.2	2731 : 1532	0AAB : 05FC	Underrange
< -120.0	-32768	8000	< -184.0	-32768	8000	< 153.2	-32768	8000	Underflow

Table 2-253 Thermocouple type C

Type C in °C	Values		Type C in °F	Values		Type C in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 2500.0	32767	7FFF	> 3276.6	32767	7FFF	> 2773.2	32767	7FFF	Overflow
2500.0 : 2315.1	25000 : 23151	61A8 : 5A6F	3276.6 : 2786.6	32766 : 27866	7FFE : 6CDA	2773.2 : 2588.3	27732 : 25883	6C54 : 651B	Overrange
2315.0 : 0.0	23150 : 0	5A6E : 0000	2786.5 : 32.0	27865 : 320	6CD9 : 0140	2588.2 : 273.2	25882 : 2732	651A : 0AAC	Nominal range
-0.1 : -120.0	-1 : -1200	FFFF : FB50	31.9 : -184.0	319 : -1840	013F : F8D0	273.1 : 153.2	2731 : 1532	0AAB : 05FC	Underrange
< -120.0	-32768	8000	< -184.0	-32768	8000	< 153.2	-32768	8000	Underflow

Table 2-254 Thermocouple type E

Type E in °C	Values		Type E in °F	Values		Type E in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 1200.0	32767	7FFF	> 2192.0	32767	7FFF	> 1473.2	32767	7FFF	Overflow
1200.0 : 1000.1	12000 : 10001	2EE0 : 2711	2192.0 : 1832.1	21920 : 18321	55A0 : 4791	1473.2 : 1273.3	14732 : 12733	398C : 31BD	Overrange
1000.0 : -270.0	10000 : -2700	2710 : F574	1832.0 : -454.0	18320 : -4540	4790 : EE44	1273.2 : 3.2	12732 : 32	31BC : 0020	Nominal range
< -270.0	-32768	8000	< -454.0	-32768	8000	< 3.2	-32768	8000	Underflow

Table 2-255 Thermocouple type J

Type J in °C	Values		Type J in °F	Values		Type J in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 1450.0	32767	7FFF	> 2642.0	32767	7FFF	> 1723.2	32767	7FFF	Overflow
1450.0 : 1200.1	14500 : 12001	38A4 : 2EE1	2642.0 : 2192.1	26420 : 21921	6734 : 55A1	1723.2 : 1473.3	17232 : 14733	4350 : 398D	Overrange
1200.0 : -210.0	12000 : -2100	2EE0 : F7CC	2192.0 : -346.0	21920 : -3460	55A0 : F27C	1473.2 : 63.2	14732 : 632	398C : 0278	Nominal range
< -210.0	-32768	8000	< -346.0	-32768	8000	< 63.2	-32768	8000	Underflow

Table 2-256 Thermocouple type K

Type K in °C	Values		Type K in °F	Values		Type K in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 1622.0	32767	7FFF	> 2951.6	32767	7FFF	> 1895.2	32767	7FFF	Overflow
1622.0 : 1372.1	16220 : 13721	3F5C : 3599	2951.6 : 2501.7	29516 : 25017	734C : 61B9	1895.2 : 1645.3	18952 : 16453	4A08 : 4045	Overrange
1372.0 : -270.0	13720 : -2700	3598 : F574	2501.6 : -454.0	25016 : -4540	61B8 : EE44	1645.2 : 3.2	16452 : 32	4044 : 0020	Nominal range
< -270.0	-32768	8000	< -454.0	-32768	8000	< 3.2	-32768	8000	Underflow

Table 2-257 Thermocouple type L

Type L in °C	Values		Type L in °F	Values		Type L in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 1150.0	32767	7FFF	> 2102.0	32767	7FFF	> 1423.2	32767	7FFF	Overflow
1150.0 : 900.1	11500 : 9001	2CEC : 2329	2102.0 : 1652.1	21020 : 16521	521C : 4089	1423.2 : 1173.3	14232 : 11733	3798 : 2DD5	Overrange
900.0 : -200.0	9000 : -2000	2328 : F830	1652.0 : -328.0	16520 : -3280	4088 : F330	1173.2 : 73.2	11732 : 732	2DD4 : 02DC	Nominal range
< -200.0	-32768	8000	< -328.0	-32768	8000	< 73.2	-32768	8000	Underflow

Table 2-258 Thermocouple type N

Type N in °C	Values		Type N in °F	Values		Type N in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 1550.0	32767	7FFF	> 2822.0	32767	7FFF	> 1823.2	32767	7FFF	Overflow
1550.0 : 1300.1	15500 : 13001	3C8C : 32C9	2822.0 : 2372.1	28220 : 23721	6E3C : 5CA9	1823.2 : 1573.3	18232 : 15733	4738 : 3D75	Overrange
1300.0 : -270.0	13000 : -2700	32C8 : F574	2372.0 : -454.0	23720 : -4540	5CA8 : EE44	1573.2 : 3.2	15732 : 32	3D74 : 0020	Nominal range
< -270.0	-32768	8000	< -454.0	-32768	8000	< 3.2	-32768	8000	Underflow

Table 2-259 Thermocouples R and S

Types R, S in °C	Values		Types R, S in °F	Values		Types R, S in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 2019.0	32767	7FFF	> 3276.6	32767	7FFF	> 2292.2	32767	7FFF	Overflow
2019.0 : 1769.1	20190 : 17691	4EDE : 451B	3276.6 : 3216.3	32766 : 32163	7FFE : 7DA3	2292.2 : 2042.3	22922 : 20423	598A : 4FC7	Overrange
1769.0 : -50.0	17690 : -500	451A : FE0C	3216.2 : -58.0	32162 : -580	7DA2 : FDBC	2042.2 : 223.2	20422 : 2232	4FC6 : 08B8	Nominal range
-50.1 : -170.0	-501 : -1700	FE0B : F95C	-58.1 : -274.0	-581 : -2740	FDBB : F54C	223.1 : 103.2	2231 : 1032	08B7 : 0408	Underrange
< -170.0	-32768	8000	< -274.0	-32768	8000	< 103.2	< 1032	8000	Underflow

Table 2-260 Thermocouple type T

Type T in °C	Values		Type T in °F	Values		Type T in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 540.0	32767	7FFF	> 1004.0	32767	7FFF	> 813.2	32767	7FFF	Overflow
540.0 : 400.1	5400 : 4001	1518 : 0FA1	1004.0 : 752.1	10040 : 7521	2738 : 1D61	813.2 : 673.3	8132 : 6733	1FC4 : 1AAD	Overrange
400.0 : -270.0	4000 : -2700	0FA0 : F574	752.0 : -454.0	7520 : -4540	1D60 : EE44	673.2 : 3.2	6732 : 32	1AAC : 0020	Nominal range
< -270.0	-32768	8000	< -454.0	-32768	8000	< 3.2	-32768	8000	Underflow

Table 2-261 Thermocouple type U

Type U in °C	Values		Type U in °F	Values		Type U in K	Values		Range
	Dec.	Hex.		Dec.	Hex.		Dec.	Hex.	
> 850.0	32767	7FFF	> 1562.0	32767	7FFF	> 1123.2	32767	7FFF	Overflow
850.0 : 600.1	8500 : 6001	2134 : 1771	1562.0 : 1112.1	15620 : 11121	2738.0 : 2B71	1123.2 : 873.3	11232 : 8733	2BE0 : 221D	Overrange
600.0 : -200.0	6000 : -2000	1770 : F830	1112.0 : -328.0	11120 : -3280	2B70 : F330	873.2 : 73.2	8732 : 732	221C : 02DC	Nominal range
< -200.0	-32768	8000	< -328.0	-32768	8000	< 73.2	-32768	8000	Underflow

Parameter data record

C

C.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters. The channel parameter blocks are identical and are shown based on the example of channel 0.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Number of parameter structures = 2_D ($0000\ 0010_B$)							
2...3	**Module header information**							
2	Number of module parameter blocks = 1_D ($0000\ 0001_B$)							
3	Module parameter length = 1_D ($0000\ 0001_B$)							
4...5	**Module parameter block**							
4	Reserved[1]		Temperature unit[2] 00_B: Degrees Celsius 01_B: Degrees Fahrenheit 10_B: Kelvin[3]		Reserved[1]			
5	Channel parameter length = 16_D ($0001\ 0000_B$)							
6...21	**Channel 0 channel parameter block**							
6	Measurement type				Measuring range			
	0000_B: Deactivated				0000_B: Deactivated			
	0001_B: Voltage				0010_B: ± 80 mV			
	0100_B: Resistor 4-wire terminal 0101_B: Resistor 3-wire terminal 0110_B: Resistor 2-wire terminal				0001_B: 150 Ω 0010_B: 300 Ω			
	0111_B: Thermal resistor 4-wire terminal 1000_B: Thermal resistor 3-wire terminal 1001_B: Thermal resistor 2-wire terminal				0000_B: Pt 100 climatic range 0001_B: Ni 100 climatic range 0010_B: Pt 100 standard range 0011_B: Ni 100 standard range 0101_B: Pt 1000 standard range 0110_B: Ni 1000 standard range 1001_B: Pt 1000 climatic range 1010_B: Ni 1000 climatic range			
	1010_B: Thermocouple				0000_B: Type B (PtRh-PtRh) 0001_B: Type N (NiCrSi-NiSi) 0010_B: Type E (NiCr-CuNi) 0011_B: Type R (PtRh-Pt) 0100_B: Type S (PtRh-Pt) 0101_B: Type J (Fe-CuNi) 0110_B: Type L (Fe-CuNi) 0111_B: Type T (Cu-CuNi)			

1 Reserved bits must be set to 0

2 Only for thermal resistor and thermocouple measuring type. Otherwise, set the bit to 0

3 Not for "Pt climatic range or Ni climatic range"

4 Only for "Pt climatic range and Pt standard range" measuring type. Otherwise, set the bit to 0

5 Only for "Ni climatic range and Ni standard range" measuring type. Otherwise, set the bit to 0

6 Not for "Resistor" measurement type. Otherwise, set the bit to 0

7 Not for "Voltage" measurement type. Otherwise, set the bit to 0

8 Not for "Thermal resistor" measurement type. Otherwise, set the bit to 0

9 Only for measurement type "Thermocouple" with "Reference junction - Fixed reference temperature". Otherwise, set the bit to 0

10 Only for "Resistor 2-wire terminal" and "Thermal resistor 2-wire terminal" measurement type. Otherwise, set the bit to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
					1000_B: Type K (NiCr-NiAl) 1001_B: Type U (Cu-CuNi) 1010_B: Type C (WRe-WRe)			
7	Reference junction[6]				Temperature coefficient[4, 5]			
	0000_B: Fixed reference temperature 0001_B: Dynamic reference temperature 0011_B: Internal reference junction 0110_B: No compensation				0000_B: Pt 0.003851 (EN 60751)[4] 0001_B: Pt 0.003916[4] 0010_B: Pt 0.003902[4] 0011_B: Pt 0.00392[4] 0100_B: Pt 0.00385[4] 1000_B: Ni 0.00618[5] 1001_B: Ni 0.00672[5]			
8	Interference frequency suppression				Smoothing			
	0001_B: 60 Hz (16.6 ms) 0010_B: 50 Hz (20 ms) 0100_B: 16.6 Hz (60 ms) 1111_B: None				0000_B: None 0001_B: Weak 0010_B: Medium 0011_B: Strong			
9	Hardware interrupt, low limit 1	Hardware interrupt, high limit 1	Hardware interrupt, low limit 2	Hardware interrupt, high limit 2	Diagnostics overflow	Diagnostics underflow[6]	Diagnostics wire break[7]	Reference junction diagnostics[6,7,8]
	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable
10 **11**	Fixed reference temperature[9]: WORD: Value range: -2290 ... 3276_D The permissible value range (min./max.) for the thermocouple measurement type can be found in the table Value ranges for the "reference temperature" for thermocouples..							
12 **13**	High limit 1: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Value ranges of the hardware interrupts.							
14 **15**	Low limit 1: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Value ranges of the hardware interrupts.							
16 **17**	High limit 2: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Value ranges of the hardware interrupts.							
18 **19**	Low limit 2: WORD: The value range depends on the measurement type. The permissible value range (min./max.) for the measurement type can be found in the table Value ranges of the hardware interrupts.							
20 **21**	Conductor resistance [mΩ][10]: WORD: Value range: 0 ... 50000_D							

1 Reserved bits must be set to 0

2 Only for thermal resistor and thermocouple measuring type. Otherwise, set the bit to 0

3 Not for "Pt climatic range or Ni climatic range"

4 Only for "Pt climatic range and Pt standard range" measuring type. Otherwise, set the bit to 0

5 Only for "Ni climatic range and Ni standard range" measuring type. Otherwise, set the bit to 0

6 Not for "Resistor" measurement type. Otherwise, set the bit to 0

7 Not for "Voltage" measurement type. Otherwise, set the bit to 0

8 Not for "Thermal resistor" measurement type. Otherwise, set the bit to 0

9 Only for measurement type "Thermocouple" with "Reference junction - Fixed reference temperature". Otherwise, set the bit to 0

10 Only for "Resistor 2-wire terminal" and "Thermal resistor 2-wire terminal" measurement type. Otherwise, set the bit to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
22...37	**Channel 1 channel parameter block**							
38...53	**Channel 2 channel parameter block**							
54...69	**Channel 3 channel parameter block**							

1 Reserved bits must be set to 0

2 Only for thermal resistor and thermocouple measuring type. Otherwise, set the bit to 0

3 Not for "Pt climatic range or Ni climatic range"

4 Only for "Pt climatic range and Pt standard range" measuring type. Otherwise, set the bit to 0

5 Only for "Ni climatic range and Ni standard range" measuring type. Otherwise, set the bit to 0

6 Not for "Resistor" measurement type. Otherwise, set the bit to 0

7 Not for "Voltage" measurement type. Otherwise, set the bit to 0

8 Not for "Thermal resistor" measurement type. Otherwise, set the bit to 0

9 Only for measurement type "Thermocouple" with "Reference junction - Fixed reference temperature". Otherwise, set the bit to 0

10 Only for "Resistor 2-wire terminal" and "Thermal resistor 2-wire terminal" measurement type. Otherwise, set the bit to 0

See also

Parameters (Page 22)

C.2 Structure of data record 192 for the dynamic reference temperature

The following descriptions relate to the instructions in PROFINET IO and STEP 7. If you are using a different user program or fieldbus, you must adapt the instructions accordingly.

The **WRREC** instruction is used to transfer the reference junction temperature via data record 192 to the I/O device.

The WRREC instruction is described in the online help for STEP 7 and in the MultiFieldbus Function Manual.

If you have set the "Dynamic reference temperature" value for the "Reference junction" parameter, the I/O module expects a new data record at least every 5 minutes. If the I/O module does not receive a new data record within this time, it generates the "Reference channel error" diagnostic message.

Structure of data record 192 for dynamic reference temperature

The following table shows the structure of data record 192 for dynamic reference temperature.

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	**Resolution**							
	0000 0000B: Standard (tenths of a degree) 0000 0001B: Climatic (hundredths of a degree)							
1	**Temperature unit**							
	$0000\ 0000_B$: Degrees Celsius $0000\ 0001_B$: Degrees Fahrenheit $0000\ 0010_B$: Kelvin							

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2...3	**Temperature external reference junction channel 0**							
2	High byte							
3	Low byte							
4...5	**Temperature external reference junction channel 1**							
4	High byte							
5	Low byte							
6...7	**Temperature external reference junction channel 2**							
6	High byte							
7	Low byte							
8...9	**Temperature external reference junction channel 3**							
8	High byte							
9	Low byte							

Valid values for fixed temperature compensation

The selectable values must lie within the permitted value range. The resolution of the valid values for temperature compensation is a tenth of a degree.

Table 2-262 Valid values for temperature compensation via data record

Temperature unit	Decimal	Hexadecimal
Celsius (default)	-1450 ... 1550	$FA56_H$ ... $60E_H$
Fahrenheit (default)	-2290 ... 3110	$F70E_H$ ... $C26_H$
Kelvin (default)	1282 ... 3276	502_H ... CCC_H
Celsius (climatic)	-14500 ... 15500	$C75C_H$ ... $3C8C_H$
Fahrenheit (climatic)	-22900 ... 31100	$A68C_H$ ... $797C_H$
Kelvin (climatic)	12820 ... 32760	3214_H ... $7FF8_H$

NOTE

Thanks to the structure of the DS 192 data records, you can use a separate reference junction for each channel. The channels can also be combined via the user program in such a way that they use the same reference junction. Specify the same temperature value for all channels in the data records that work with the same reference junction temperature.

Additional information

You can find more information on compensation of the reference junction temperature via data record in the function manual SIMATIC analog value processing (https://support.industry.siemens.com/cs/ww/en/view/67989094).

C.3 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" (Page 37) are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-263 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128	DS192
Byte 0	Byte 1	Byte 2	Byte 3				
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓	✓

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128	DS192
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**				
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓	✓
DF	80	E1	02	Invalid diagnostics enable bit set for operating mode.	Check the parameters of the I/O device.	✓	
DF	80	E1	04	Invalid value set for hardware interrupt limit.	Check the parameters of the I/O device.	✓	
DF	80	E1	05	Invalid coding set for measuring range / measurement type.	Check the parameters of the I/O device.	✓	
DF	80	E1	08	Invalid coding set for interference frequency suppression / integration time.	Check the parameters of the I/O device.	✓	
DF	80	E1	09	Invalid coding set for smoothing.	Check the parameters of the I/O device.	✓	
DF	80	E1	0F	Invalid parameter assignment of reference temperature set.	Check the parameters of the I/O device.	✓	✓
DF	80	E1	10	Invalid measurement type set.	Check the parameters of the I/O device.	✓	✓
DF	80	E1	20	Invalid temperature coefficient set.	Check the parameters of the I/O device.	✓	
DF	80	E1	21	Invalid temperature unit set.	Check the parameters of the I/O device.	✓	✓
DF	80	E1	23	Invalid conductor resistance set.	Check the parameters of the I/O device.	✓	

SIEMENS

SIMATIC

ET 200AL
Analog output module AQ 4xU/I 4xM12 (6ES7145-5ND00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Parameters/address space 5

Interrupts/diagnostics alarms 6

Technical specifications 7

PROFIenergy 8

Dimension drawing A

Representation of analog values B

Parameter data record C

10/2024
A5E38687953-AD

Table of contents

1 Introduction 4

1.1 ET 200AL Documentation Guide 5
1.1.1 ET 200AL Documentation Guide 5
1.1.2 Tool support 6
1.2 SIMATIC Technical Documentation 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 11

3.1 Properties 11
3.2 Operator controls and display elements 13

4 Wiring 14

4.1 Terminal and block diagram 14
4.2 Pin assignment 15

5 Parameters/address space 18

5.1 Output ranges 18
5.2 Parameters 18
5.3 Explanation of the parameters 20
5.4 Address space 21

6 Interrupts/diagnostics alarms 23

6.1 Status and error displays 23
6.2 Interrupts 24
6.3 Diagnostics alarms 25

7 Technical specifications 26

8 PROFIenergy 30

8.1 Pause function 30
8.2 Response of analog output module 31

A Dimension drawing 32

B Representation of analog values 33
B.1 Representation of analog values in the voltage output ranges 33
B.2 Representation of analog values in the current output ranges 34

C Parameter data record 36
C.1 Structure of data record 128 for the module parameter assignment 36
C.2 Error transferring the data record 38

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL Documentation Guide

1.1.1 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Observe all relevant cybersecurity information.

Security features of the product	Reference
Data integrity	The topic of data integrity is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

Product overview

3

3.1 Properties

Article number

6ES7145-5ND00-0BA0

View of the module

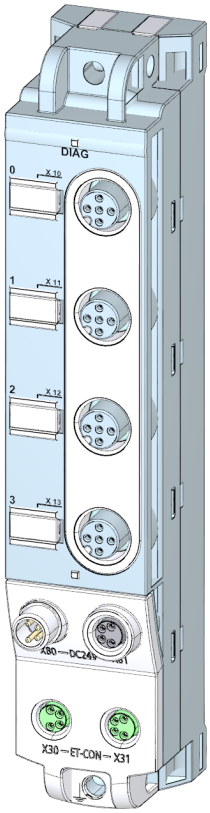


Figure 2-114 View of the analog output module AQ 4xU/I 4xM12

Properties

The module has the following technical properties:

- 4 analog outputs
- M12 sockets for connection of actuators
- Voltage output can be set for each channel
- Current output can be set for each channel
- Resolution: 16-bit
- Dimensions 30 x 159 mm
- Configurable diagnostics can be set for each channel

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)
- PROFIenergy

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

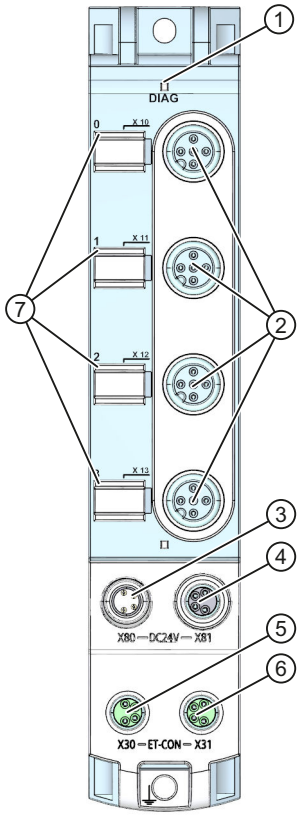
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) system manual.

3.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the AQ 4xU/I 4xM12 analog output module.



① DIAG: LED display for the diagnostic status
② X10 to X13: Sockets for the output signal
③ X80: Connector for infeed of the supply voltage (POWER input)
④ X81: Socket for loop-through of the supply voltage (POWER output)
⑤ X30: Socket for ET-Connection IN
⑥ X31: Socket for ET-Connection OUT
⑦ LED displays 0 to 3 for the channel status

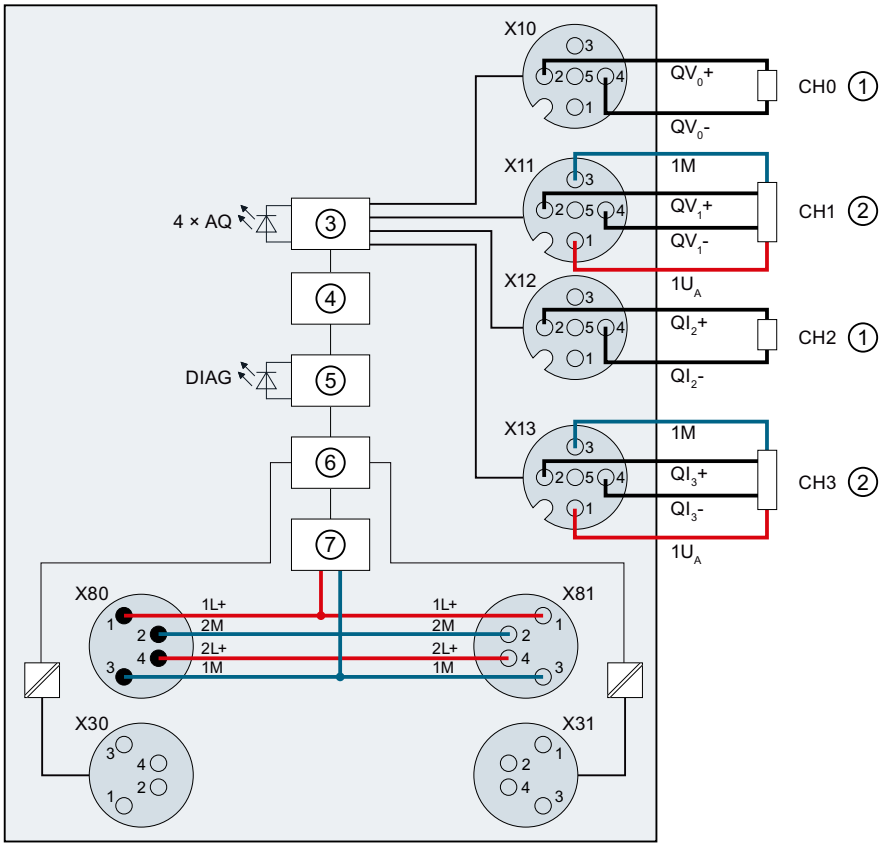
Figure 2-115 Operator controls and display elements

Wiring

4

4.1 Terminal and block diagram

The example in the following figure shows the pin assignment for voltage and current output of the analog output module AQ 4xU/I 4xM12.



①	Voltage/current output as 2-wire connection	X31	Loop-through of the ET-Connection
②	Voltage/current output as 4-wire connection	1L+	Supply voltage 1L+ (non-switched)
③	Output driver	1M	Ground 1M (non-switched)
④	Digital-to-analog converter (DAC)	2L+	Load voltage 2L+ (switched)
⑤	Microcontroller	2M	Ground 2M (switched)
⑥	ET-Connection interface	$1U_A$	24 V actuator supply
⑦	Internal supply voltage	QV_n/QI_n+	Voltage/current output positive, channel n
X10 to X13	Channels 0 to 3	QV_n/QI_n-	Voltage/current output negative, channel n
X80	Infeed of supply voltages	AQ	Channel status LEDs (0, 1, 2 and 3) (green)
X81	Loop-through of supply voltages	DIAG	Diagnostic status LED (red/green)
X30	Infeed of the ET-Connection		

Figure 2-116 Terminal and block diagram for voltage and current output

4.2 Pin assignment

NOTE

Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for analog outputs

The tables below show the pin assignments of the 4 sockets for connection of the analog outputs.

Table 2-264 Pin assignment of the sockets for analog outputs (voltage output)

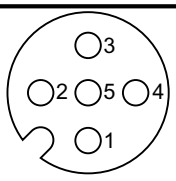
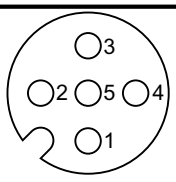
Pin	Assignment **X10 to X13 - sockets for analog outputs (voltage output)**	Front view of the sockets
1	24 V actuator supply $1U_A$ (derived from 1L+ Non-Switched)	
2	Voltage output positive QV_0+: Connector X10 Voltage output positive QV_1+: Connector X11 Voltage output positive QV_2+: Connector X12 Voltage output positive QV_3+: Connector X13	
3	Ground for actuator supply 1M	
4	Voltage output negative QV_0-: Connector X 10 Voltage output negative QV_1-: Connector X11 Voltage output negative QV_2-: Connector X12 Voltage output negative QV_3-: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

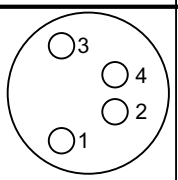
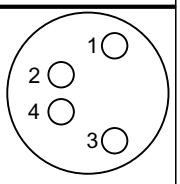
Table 2-265 Pin assignment of the sockets for analog outputs (current output)

Pin	Assignment **X10 to X13 - sockets for analog outputs (current output)**	Front view of the sockets
1	24 V actuator supply $1U_A$ (derived from 1L+ Non-Switched)	
2	Current output positive QI_0+: Connector X10 Current output positive QI_1+: Connector X11 Current output positive QI_2+: Connector X12 Current output positive QI_3+: Connector X13	
3	Ground for actuator supply 1M	
4	Current output negative QI_0-: Connector X10 Current output negative QI_1-: Connector X11 Current output negative QI_2-: Connector X12 Current output negative QI_3-: Connector X13	
5	Functional earth FE	
Shield	Functional earth FE	

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

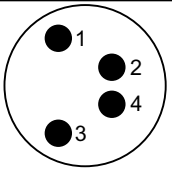
Table 2-266 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the core color of the bus cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	yellow		
2	RXP	TXP	white		
3	RXN	TXN	blue		
4	TXN	RXN	orange		
Shield	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

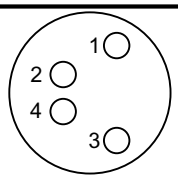
Table 2-267 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the core color of the power cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	brown	
2	Ground 2M (switched)	white	
3	Ground 1M (non-switched)	blue	
4	Load voltage 2L+ (switched)	black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-268 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the core color of the power cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	brown	
2	Ground 2M (switched)	white	
3	Ground 1M (non-switched)	blue	
4	Load voltage 2L+ (switched)	black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the connector for ET-Connection and the connector for the supply voltage can destroy the module.

Parameters/address space

5

5.1 Output ranges

The table below indicates which output types and ranges are configurable.

Output type and output ranges

Table 2-269 Output type and output ranges

Output type	Output range
Disabled	-
Voltage	+/- 10 V 0 V to 10 V 1 V to 5 V
Current	+/- 20 mA 0 mA to 20 mA 4 mA to 20 mA

The tables of the output ranges, overflow, overrange, etc. are provided in the appendix Representation of analog values (Page 33).

5.2 Parameters

Parameters of the AQ 4xU/I 4xM12 analog output module

The table below lists the parameters that can be set. The effective range of the parameters that can be set depends on the type of configuration. The following configurations are possible:

- Distributed operation on PROFINET IO
- Distributed operation with PROFIBUS DP

The following parameter settings are possible:

Table 2-270 Configurable parameters and their defaults

Parameters	Value range	Default	GSD file PROFINET IO	GSD file PROFIBUS DP
Output type/range	• Disabled • Voltage ±10 V • Voltage 0 V to 10 V • Voltage 1 V to 5 V • Current ±20 mA • Current 0 mA to 20 mA • Current 4 mA to 20 mA	Current 4 mA to 20 mA	Channel	Channel
Diagnostics: Actuator supply short circuit to ground	• Disable • Enable	Disable	Module	Module*
Diagnostics: Short circuit to ground (output type voltage)	• Disable • Enable	Disable	Channel	
Diagnostics: Wire break (output type current)	• Disable • Enable	Disable	Channel	Module
Diagnostics: Underflow	• Disable • Enable	Disable	Channel	Module
Diagnostics: Overflow	• Disable • Enable	Disable	Channel	Module
Reaction to CPU/master STOP	• Shut down • Keep last value • Output substitute value	Shut down	Channel	Module
Substitute value	See section Explanation of the parameters (Page 20)	0	Channel	Channel

* = With configuration via PROFIBUS GSD file, the two short-circuit diagnostics ("Diagnostics: Actuator supply short circuit to ground" and "Diagnostics: Short circuit to ground" for voltage outputs) are activated or deactivated using a module-wide parameter “Diagnostics: Short circuit to ground". They cannot be adjusted independently of one another.

Short-circuit detection

The diagnostics for short circuit to ground can be configured for the voltage output type. Short-circuit detection cannot be guaranteed for small output values (between 0.1 V and +0.1 V).

Wire break detection

The diagnostics for wire break can be configured for the current output type. Wire break detection cannot be guaranteed for small output values (between -0.2 mA and +0.2 mA).

5.3 Explanation of the parameters

Output type/range channel n

With this parameter, you set the output type or output range for the channel to control the actuator.

NOTE

Unused channels

"Deactivate" unused channels in the parameter assignment to improve the power consumption of the module.

A deactivated channel always returns the value "no voltage or current".

Diagnostics: Actuator supply short circuit to ground

Enabling of the diagnostics if a short-circuit of the actuator supply to ground occurs.

Diagnostics: Short circuit to ground

Enabling of the diagnostics if a short-circuit of the output to ground occurs.

Diagnostics: Wire break

Enabling of the diagnostics if the line to the actuator is broken.

Diagnostics: Underflow

Enabling of the diagnostics when the output value violates the underrange, falls below the minimum output value or reaches the underflow.

Diagnostics: Overflow

Enabling of the diagnostics when the output value exceeds the overrange.

Reaction to CPU/master STOP

Adjusts the reaction of the module after a CPU/master STOP.

- Shut down: The analog output is de-energized.
- Keep last value: The last value of the analog output remains activated.
- Output substitute value: The channel outputs a configured substitute value.

Substitute value

With this parameter, you set substitute values for the analog outputs.
The table below shows the permitted value ranges for the substitute values:

Table 2-271 Permissible substitute values for the output ranges

Output type	Output range	Valid substitute value
Current	±10 V 0 V to 10 V 1 V to 5 V	-32512 to 32511 0..32511 -6912 to 32511
Voltage	±20 mA 0 mA to 20 mA 4 mA to 20 mA	-29031..29030 0..29030 -692 to 29376

5.4 Address space

The tables below shows the assignment of the address space for the analog output module AQ 4xU/I 4xM12 with value status (Quality Information, QI). If you are using PROFINET and the value status was enabled, the addresses for the value status are available. The value status is not available for PROFIBUS.

Table 2-272 Address space in the configuration mode AQ with value status

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x	0	0	0	0					Value status (QI) for inputs on channels 0 ... 3*
Assignment in the process image output (PIQ)									
QB x									Output value channel 0
QB x +1									
QB x +2									Output value channel 1
QB x +3									
QB x +4									Output value channel 2
QB x +5									
QB x +6									Output value channel 3
QB x +7									

* 0 = Value read in at channel is incorrect

Configuration options of the AQ 4xU/I 4xM12 analog output module

You have the following configuration options:

- Configuration 1: without value status
- Configuration 2: with value status

Evaluating the value status

An additional byte is occupied in the input address space if you enable the value status for the analog output module. Bits 0 to 3 in this byte are assigned to a channel and return information about the validity of the analog values or the channel status.

Bit = 1: No error on channel.

Bit = 0: Error on channel.

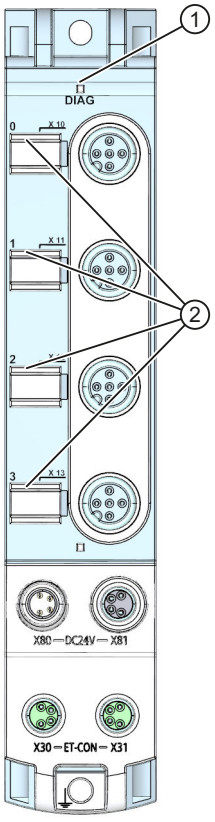
Interrupts/diagnostics alarms

6

6.1 Status and error displays

LED displays

The figure below shows the LED display (status and error displays) of the AQ 4xU/I 4xM12 analog output module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0, 1, 2 and 3) (green)

Figure 2-117 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 25).

DIAG LED

Table 2-273 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no diagnostics
☼ Flashes	Module parameters assigned and diagnostics

LED for the channel status

Table 2-274 Status display of the LEDs 0, 1, 2 and 3

LED 0, 1, 2 and 3	Meaning
☐ Off	• Channel deactivated • Channel activated and incorrect parameter assignment • Parameter error possible with GSD
■ On	• Channel activated and correct parameter assignment

6.2 Interrupts

The AQ 4xU/I 4xM12 analog output module supports diagnostics interrupts.

Diagnostic interrupt

The module generates a diagnostic interrupt at the following events:

- Short-circuit of the actuator supply
- Short-circuit (voltage)
- Wire break (current)
- High limit violated
- Low limit violated
- Parameter assignment error

6.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the analog output module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

The following table shows the diagnostics alarms for all measuring ranges.

Table 2-275 Diagnostics alarms

Diagnostics alarm	Error code	Meaning	Solution
Short-circuit to ground	1_H	• Short-circuit of actuator supply to ground • Short-circuit of output to ground	Correct the process wiring
Wire break	6_H	Actuator circuit impedance too high	Use a different actuator type or modify the wiring, e.g. use cables with larger cross-section
		Wire break between the module and sensor	Connect the cable
		Channel not connected (open)	• Deactivate diagnostics • Connect the channel • Deactivate channel
High limit violated	7_H	The output value set by the user program violates the valid rated range/overrange.	Correct the output value
Low limit violated	8_H	The output value set by the user program violates the valid rated range/underrange.	Correct the output value
Parameter assignment error	10_H	Module parameter assignment is faulty	Correct the parameter assignment
Security event: Firmware has been successfully downloaded and activated for installation.[1]	191_H	Firmware has been successfully downloaded and activated for installation.	-
Security event: The firmware integrity checks failed.[1]	192_H	Security event: The firmware integrity checks failed.	• Verify if the firmware update file you are using comes from a secure source. • Download the firmware again from the Siemens Support Web page. • Repeat the firmware update.

[1] A diagnostics alarm is output for a signed firmware update.

Technical specifications

7

Technical specifications of the AQ 4xU/I 4xM12 analog output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7145-5ND00-0BA0/td?dl=en).

Article number	6ES7145-5ND00-0BA0
General information	
Product type designation	AQ 4xU/I
HW functional status	FS06
Firmware version	V2.0.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V14 or higher
• STEP 7 configurable/integrated from version	V5.5 SP4 Hotfix 7 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; actuator power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	75 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Actuator supply	
Number of outputs	4
Short-circuit protection	Yes; per module, electronic
Output current	
• Rated value	Total current 1 A up to 45 °C; 0.5 A up to 55 °C
Power loss	
Power loss, typ.	2.6 W
Analog outputs	
Number of analog outputs	4
Voltage output, short-circuit protection	Yes
Voltage output, short-circuit current, max.	24 mA

Article number	6ES7145-5ND00-0BA0
Current output, no-load voltage, max.	15 V
Cycle time (all channels) max.	1 ms
Output ranges, voltage	
• 0 to 10 V	Yes; 15 bit
• 1 V to 5 V	Yes; 14 bit
• -10 V to +10 V	Yes; 16 bit incl. sign
Output ranges, current	
• 0 to 20 mA	Yes; 15 bit
• -20 mA to +20 mA	Yes; 16 bit incl. sign
• 4 mA to 20 mA	Yes; 14 bit
Connection of actuators	
• for voltage output two-wire connection	Yes
• for voltage output four-wire connection	Yes
• for current output two-wire connection	Yes
• for current output four-wire connection	Yes
Load impedance (in rated range of output)	
• with voltage outputs, min.	1 kΩ
• with voltage outputs, capacitive load, max.	1 µF
• with current outputs, max.	500 Ω
• with current outputs, inductive load, max.	1 mH
Destruction limits against externally applied voltages and currents	
• Voltages at the outputs towards MANA	16 V
Cable length	
• shielded, max.	30 m
Analog value generation for the outputs	
Integration and conversion time/resolution per channel	
• Resolution with overrange (bit including sign), max.	16 bit
Settling time	
• for resistive load	1 ms
• for capacitive load	1 ms
• for inductive load	1 ms
Errors/accuracies	
Output ripple (relative to output range, bandwidth 0 to 50 kHz), (+/-)	0.02 %
Linearity error (relative to output range), (+/-)	0.1 %
Temperature error (relative to output range), (+/-)	0.005 %/K
Crosstalk between the outputs, max.	-70 dB
Repeat accuracy in steady state at 25 °C (relative to output range), (+/-)	0.03 %
Operational error limit in overall temperature range	
• Voltage, relative to output range, (+/-)	0.25 % from 55 °C to -25 °C and 0.35 % to -30 °C
• Current, relative to output range, (+/-)	0.25 %

Article number	6ES7145-5ND00-0BA0
Basic error limit (operational limit at 25 °C)	
• Voltage, relative to output range, (+/-)	0.15 %
• Current, relative to output range, (+/-)	0.15 %
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Wire-break	Yes; channel-by-channel, only for output type "current"
• Short-circuit	Yes; Actuator supply module by module; channel by channel for output type "voltage"
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS03
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198632
product functions / security / header	
signed firmware update	Yes
data integrity	Yes
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions

Article number	**6ES7145-5ND00-0BA0**
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	175 g

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific response of the analog output module is explained in the section below.

Additional information

You can find more information on working with PROFIenergy in the "PROFIenergy" section of the Equipment Manual IM 157-1 PN interface module (https://support.industry.siemens.com/cs/ww/en/view/89254863) and the "Saving energy with PROFIenergy" section of Function Manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856).

Application examples and manual information are also available on the Internet FAQs (https://support.industry.siemens.com/cs/ww/en/view/109807766).

8.2 Response of analog output module

Display

The channel status LEDs are not affected by PROFIenergy.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following conditions apply to all channels which switch to the pause mode "PE_MODE_SHUTDOWN":

- "Wire break" and "Short circuit" error detection is **not** possible during the pause:
  - Alarms for errors already pending before the "pause" are retained.
  - Incoming and outgoing errors are reported once the "pause" has ended.

The following applies for all channels which switch to a different pause mode:

- "Wire break" and "Short circuit" error recognition is possible during the pause. These errors are reported.
- The selection of an incorrect pause substitute value which does not correspond to the output range may result in the message "High limit violated" or "Low limit violated". The pause substitute output value effective at the channel is limited to the high or low control limit for the output range.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-276 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Actuator supply U_A switched off • Outputs de-energized • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value: • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value • Value status "BAD"

1 As there is only one actuator supply U_A for all channels, the supply can only be switched off during a "pause" if all channel parameters have been set to switch off.

Dimension drawing

A

The figure below shows the dimension drawing of the AQ 4xU/I 4xM12 analog output module in front and side view.

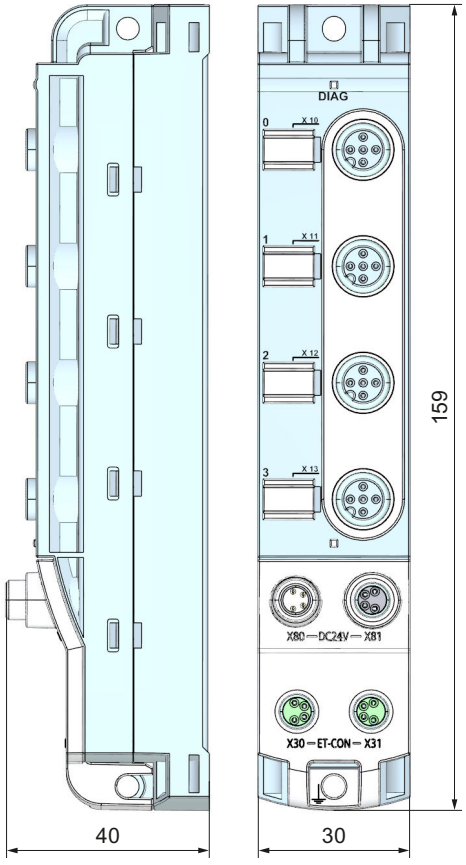


Figure 2-118 Dimension drawing

Representation of analog values

B

This appendix shows the analog values for all output ranges supported by the AQ 4xU/I 4xM12 analog output module.

Measured value resolution

The digitized analog value is the same for all output values at the same nominal range. Analog values are output as fixed point numbers in two's complement.

Table 2-277 Resolution of the analog values

Resolution in bits including sign	Values		Analog value	
	Decimal	Hexadecimal	High byte	Low byte
16	1	1_H	Sign 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1

B.1 Representation of analog values in the voltage output ranges

The tables below list the decimal and hexadecimal values (codes) of the possible voltage output ranges.

Table 2-278 Voltage output range +/-10 V

Values			Voltage output range	Range
	Dec.	Hex.	±10 V	
118.5149%	32767	7FFF	11.76 V	Maximum output value
	32512	7F00		
117.589%	32511	7EFF	11.76 V	Overrange
	27649	6C01		
100%	27648	6C00	10 V	Nominal range
75%	20736	5100	7.5 V	
0.003617%	1	1	361.7 µV	
0%	0	0	0 V	
	-1	FFFF	-361.7 µV	
-75%	-20736	AF00	-7.5 V	
-100%	-27648	9400	-10 V	
	-27649	93FF		Underrange
-117.593%	-32512	8100	-11.76 V	
	-32513	80FF	-11.76	Minimum output value
-118.519%	-32768	8000		

Table 2-279 Voltage output range 0 V to 10 V

Values			Voltage output range	Range
	Dec.	**Hex.**	**0 V to 10 V**	
118.519%	32767	7FFF	11.76 V	Maximum output value
	32512	7F00		
117.589%	32511	7EFF	11.76 V	Overrange
	27649	6C01		
100%	27648	6C00	10 V	Nominal range
75%	20736	5100	7.5 V	
0.003617%	1	1	361.7 µV	
0%	0	0	0 V	
	-1	FFFF	0 V	Minimum output value
-118.519%	-32768	8000		

Table 2-280 Voltage output range 1 to 5 V

Values			Voltage output range	Range
	Dec.	**Hex.**	**1 V to 5 V**	
118.519%	32767	7FFF	5.70 V	Maximum output value
	32512	7F00		
117.589%	32511	7EFF	5.70 V	Overrange
	27649	6C01		
100%	27648	6C00	5 V	Nominal range
75%	20736	5100	4 V	
0.003617%	1	1	1 V + 144.7 µV	
0%	0	0	1 V	
	-1	FFFF	1 V - 144.7 µV	Underrange
-25%	-6912	E500	0 V	
	-6913	E4FF	0 V	Minimum output value
-118.519%	-32768	8000		

B.2 Representation of analog values in the current output ranges

The tables below list the decimal and hexadecimal values (codes) of the possible current output ranges.

Table 2-281 Current output range +/-20 mA

Values			Current output range	Range
	Dec.	**Hex.**	**±20 mA**	
118.5149%	32767	7FFF	21 mA	Maximum output value
	29031	7167		
105%	29030	7166	21 mA	Overrange
	27649	6C01	20 mA + 723.4 nA	
100%	27648	6C00	20 mA	Nominal range
75%	20736	5100	15 mA	

Values			Current output range	Range
0.003617%	1	1	723.4 nA	Nominal range
0%	0	0	0 mA	
	-1	FFFF	-723.4 nA	
-75%	-20736	AF00	-15 mA	
-100%	-27648	9400	-20 mA	
	-27649	93FF	-20 mA + 723.4 nA	Underrange
-105%	-29031	8E99	-21 mA	
	-29032	8E98	-21 mA	Minimum output value
-118.519%	-32768	8000		

Table 2-282 Current output range 0 mA to 20 mA

Values			Current output range	Range
	Dec.	**Hex.**	**0 mA to 20 mA**	
118.5149%	32767	7FFF	21 mA	Maximum output value
	29031	7167		
105%	29030	7166	21 mA	Overrange
	27649	6C01	20 mA + 723.4 nA	
100%	27648	6C00	20 mA	Nominal range
75%	20736	5100	15 mA	
0.003617%	1	1	723.4 nA	
0%	0	0	0 mA	
	-1	FFFF	0 mA	Minimum output value
-118.519%	-32768	8000		

Table 2-283 Current output range 4 mA to 20 mA

Values			Current output range	Range
	Dec.	**Hex.**	**4 mA to 20 mA**	
118.5149%	32767	7FFF	21 mA	Maximum output value
	29377	72C1		
106.25%	29376	72C0	21 mA	Overrange
	27649	6C01	20 mA + 578.7 nA	
100%	27648	6C00	20 mA	Nominal range
75%	19008	4A40	16 mA	
0.003617%	1	1	4 mA + 578.7 nA	
0%	0	0	4 mA	
	-1	FFFF	3.9995 mA	Underrange
-2.5%	-692	FD4C	3.6 mA	
	-693	FD4B	3.6 mA	Minimum output value
-118.519%	-32768	8000		

Parameter data record

C

C.1 Structure of data record 128 for the module parameter assignment

With data record 128, you can reassign the module parameters in your user program, regardless of your programming. This means that you can use all the functions of the module even if you configured the module with a GSD file.

Parameter assignment in the user program

You can reassign the parameters of the module in RUN. For example, you can change the settings of individual channels in RUN without this having an effect on the other channels.

Changing parameters in RUN

The "WRREC" instruction is used to transfer the parameters to the module using data record 128. The parameters set with STEP 7 are not changed in the CPU by this action. After a restart, the parameters set in STEP 7 are still valid.

Output parameter STATUS

If an error occurs during the transfer of the parameters with the "WRREC" instruction, the module continues operation with the previously valid parameter assignment. The STATUS output parameter contains a corresponding error code.

The instruction "WRREC" and the error codes are described in the online help of STEP 7.

Structure of data record 128

The following table shows the structure of data record 128 and the parameters. The channel parameter blocks are identical and are shown based on the example of channel 0.

You activate a parameter by setting the corresponding bit to "1".

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0...1	**Header information**							
0	Reserved[1]		Major Version = 10_B		Minor Version = 0000_B			
1	Number of parameter structures = 2_D ($0000\ 0010_B$)							

1 Reserved bits must be set to 0

2 Only for "Voltage" output type

3 Only for "Current 2-wire terminal" output type

4 Only for "Current 2-wire terminal" output type Otherwise, set the bit to 0

5 Only for "Voltage" output type. Otherwise, set the bit to 0

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
2...3	**Module header information**							
2	Number of module parameter blocks = 1_D ($0000\ 0001_B$)							
3	Module parameter length = 1_D ($0000\ 0001_B$)							
4...5	**Module parameter block**							
4	Reserved[1]					Diagnostics: Actuator supply short circuit to ground	Reserved[1]	
						0_B: Disable 1_B: Enable		
5	Channel parameter length = 6_D ($0000\ 0110_B$)							
6...11	**Channel 0 channel parameter block**							
6	Output type							
	$0000\ 0000_B$: Deactivated $0000\ 0001_B$: Voltage $0000\ 0011_B$: Current 2-wire connection							
7	Output range							
	$0000\ 0000_B$: ±10 V[2] $0000\ 0010_B$: 0 ... 10 V[2] $0000\ 0011_B$: 1 ... 5 V[2]							
	$0000\ 0000_B$: -20 ... +20 mA[3] $0000\ 0001_B$: 0 ... 20 mA[3] $0000\ 0010_B$: 4 ... 20 mA[3]							
8	Diagnostics overflow	Diagnostics underflow	Reserved[1]	Diagnostics wire break[4]	Reserved[1]	Diagnostics short-circuit to ground[5]	Reserved[1]	
	0_B: Disable 1_B: Enable	0_B: Disable 1_B: Enable		0_B: Disable 1_B: Enable		0_B: Disable 1_B: Enable		
9	Reserved[1]						Reaction to CPU/master STOP	
							00_B: Shut down 10_B: Keep last value 11_B: Output substitute value	
10 / **11**	Substitute value: WORD: The value range depends on the output type and output range. The permissible value range (min./max.) can be found in the table Permissible substitute values for the output ranges.							
12...17	**Channel 1 channel parameter block**							
18...23	**Channel 2 channel parameter block**							
24...29	**Channel 3 channel parameter block**							

1 Reserved bits must be set to 0

2 Only for "Voltage" output type

3 Only for "Current 2-wire terminal" output type

4 Only for "Current 2-wire terminal" output type Otherwise, set the bit to 0

5 Only for "Voltage" output type. Otherwise, set the bit to 0

See also

Explanation of the parameters (Page 20)

C.2 Error transferring the data record

If you carry out the parameter settings in STEP 7 (TIA Portal) or in STEP 7 , the parameters are verified before they are transferred to the I/O device. This avoids errors in the parameter assignment.

In other applications, for example with a GSD file, the I/O device verifies the transferred parameter data record. If the I/O device determines impermissible or inconsistent parameter values, an error code (see below) as well as the Diagnostic interrupt "Parameter assignment error" are issued. In this case the new parameter data set is rejected and the current parameter values continue to be used until a valid parameter data set is transferred.

WRREC

You can change the parameter data record in the RUN operating state of the CPU by using the instruction WRREC (Write Record). The WRREC instruction returns corresponding error codes when errors occur in the STATUS parameter.

Example:
Let us assume that the execution of WRREC results in an impermissible value for the operating mode, for example 9, being written to the module. As a result the module rejects the complete parameter data record. You recognize this by evaluating the STATUS output parameter of the WRREC instruction. The STATUS output parameter is output as an ARRAY[1..4] from BYTE data with the value 16#DF80E111:

Example WRREC STATUS data	Address	Meaning
DF_H	STATUS[1]	Error while writing a data record via PROFINET IO (IEC 61158-6)
80_H	STATUS[2]	Error while reading or writing a data record via PROFINET IO (IEC 61158-6)
$E1_H$	STATUS[3]	Module-specific error
11_H	STATUS[4]	Error code from the following table: The parameter "Operating mode" has an invalid value.

Error codes

The Error codes table shows the following:

- The specific error codes of the module
- The meaning of the error code
- A suggestion for correcting the error
- The data record at which the error may occur

Table 2-284 Error codes

Error code in the STATUS parameter (hexadecimal)				Meaning	Solution	DS128
Byte 0	**Byte 1**	**Byte 2**	**Byte 3**			
DF	80	B0	xx	Number of the data record unknown.	Enter a valid number for the data record.	✓
DF	80	B1	xx	Length of the data record incorrect.	Enter a valid value for the data record length.	✓
DF	80	B2	xx	Module slot invalid or cannot be reached.	Check the assigned values for the parameters of the "WRREC" instruction.	✓
DF	80	E0	xx	Wrong version or error in the header information.	Correct the version, length and number of parameter blocks.	✓
DF	80	E1	01	Reserved bit set.	Check the parameters of the I/O device.	✓
DF	80	E1	02	Invalid diagnostics enable bit set for operating mode.	Check the parameters of the I/O device.	✓
DF	80	E1	05	Invalid coding set for measuring range / measurement type.	Check the parameters of the I/O device.	✓
DF	80	E1	06	Invalid coding for substitute value behavior.	Check the parameters of the I/O device.	✓
DF	80	E1	0A	Invalid value set for substitute value.	Check the parameters of the I/O device.	✓

SIEMENS

SIMATIC

ET 200AL
CM 4xIO-Link 4xM12
(6ES7147-5JD00-0BA0)

Equipment Manual

Documentation guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Diagnostics alarms 5

Technical specifications 6

Replacing modules 7

PROFIenergy 8

Dimension drawing A

04/2021
A5E32352322-AE

Preface

Purpose of the documentation

This manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present manual, the system manual and the function manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (https://www.siemens.com/industrialsecurity).

Table of contents

1 Documentation guide 4

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

2.3 Functions 11

2.4 Reset communication module to factory settings 11

3 Wiring 12

3.1 Terminal and block diagram 12

3.2 Pin assignment 13

4 Parameters/address space 16

4.1 Parameters 16

4.2 Explanation of the parameters 17

5 Diagnostics alarms 22

5.1 Status and error displays 22

5.2 Diagnostics alarms 24

6 Technical specifications 26

7 Replacing modules 29

8 PROFIenergy 30

8.1 Pause function 30

8.2 DI operating mode 31

8.3 DQ operating mode 32

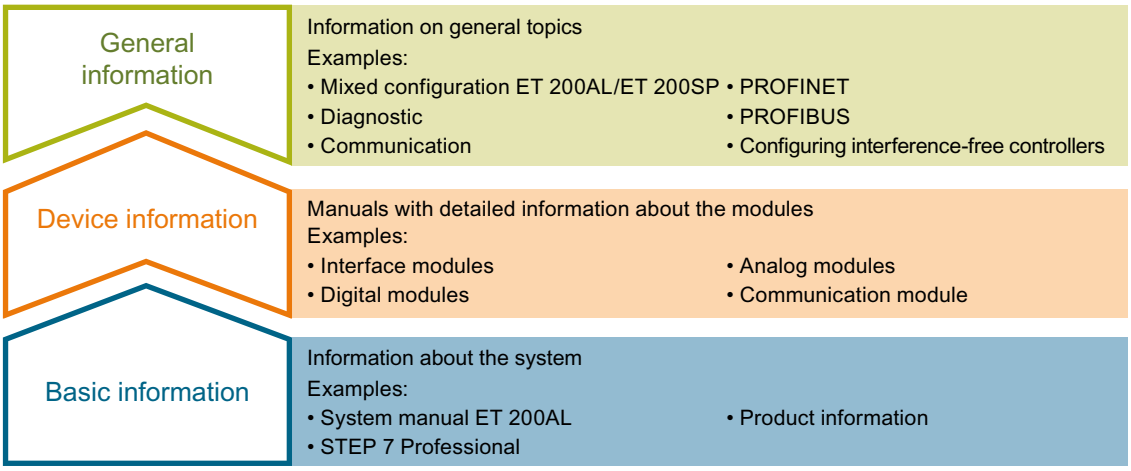
8.4 IO-Link operating mode 33

A Dimension drawing 34

Documentation guide

1

The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The System Manual and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system. The STEP 7 online help supports you in the configuration and programming.

Device information
Product manuals contain a compact description of the module-specific information, such as properties, terminal diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC ET 200AL distributed I/O system, e.g. diagnostics, communication, Motion Control, Web server.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (http://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

In the Documentation area in "mySupport" you can combine entire manuals or only parts of these to your own manual.
You can export the manual as PDF file or in a format that can be edited later.

You can find "mySupport" - Documentation on the Internet (http://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area in "mySupport", you can access the current product data for your CAx or CAe system.

You configure your own download package with a few clicks.

In doing so you can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" - CAx data on the Internet (http://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/sc/ww/en/sc/2054).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (http://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool).

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities simultaneously on different SIMATIC S7 stations as a bulk operation, independently of the TIA Portal.

General function overview:

- Network browsing and creation of a table showing the accessible devices in the network
- Flashing of device LEDs or HMI display to locate a device
- Downloading of addresses (IP, subnet, gateway) to a device
- Downloading the PROFINET name (station name) to a device
- Placing a CPU in RUN or STOP mode
- Setting the time in a CPU to the current time of your PG/PC
- Downloading a new program to a CPU or an HMI device
- Downloading from CPU, downloading to CPU or deleting recipe data from a CPU
- Downloading from CPU or deleting data log data from a CPU
- Backup/restore of data from/to a backup file for CPUs and HMI devices
- Downloading service data from a CPU
- Reading the diagnostics buffer of a CPU
- Performing a CPU memory reset
- Resetting devices to factory settings
- Downloading a firmware update to a device

You can find the SIMATIC Automation Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/98161300).

PRONETA

With SIEMENS PRONETA (PROFINET network analysis), you analyze the system network during commissioning. PRONETA features two core functions:

- The topology overview independently scans the PROFINET network and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a system.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and optimal exploitation of resources

You can find SINETPLAN on the Internet (https://www.siemens.com/sinetplan).

Product overview

2

2.1 Properties

Article number

6ES7147-5JD00-0BA0

View of the module

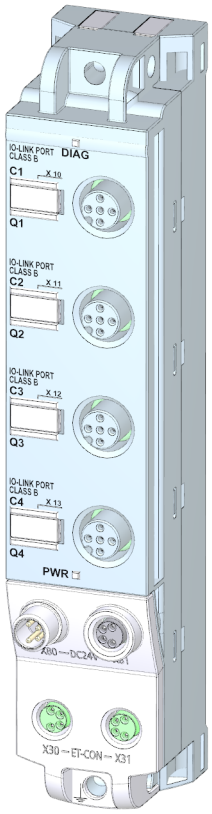


Figure 2-119 View of the CM 4xIO-Link 4xM12 communication module

Properties

The module has the following technical properties:

- IO-Link Master according to IO-Link specification V1.1
- 4 ports, type class B
- 4 M12 connectors

- SIO mode (standard IO mode)
- Supported data transmission rates:
  - COM1 (4.8 kBd)
  - COM2 (38.4 kBd)
  - COM3 (230.4 kBd)
- Configuration limits:
  - Max. 33 bytes of input data and 32 bytes of output data per port
  - Max. 132 bytes of input data and 128 bytes of output data per module
- Automatic backup of device parameters during replacement of the IO-Link device (only for V1.1 devices)
- Suitable for connection of IO-Link devices with 3-wire and 5-wire connection
- Configurable diagnostics can be set for each channel
- Dimensions 30 x 159 mm

The module supports the following functions:

Table 2-285 Version dependencies of the module functions

Function	Firmware version of the module
Firmware update	V1.0 or higher
Identification and maintenance data (I&M)	V1.0 or higher
PROFIenergy	V1.0 or higher
IO-Link port configuration with S7-PCT (as of V3.2)	V1.0 or higher
IO-Link port configuration without S7-PCT	V1.1 or higher
Master backup with "IO_LINK_MASTER" function block	V1.1 or higher
Port Qualifier Information (PQI)	V1.1 or higher
Support of I/O data per module > 32 bytes	V1.2 or higher

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

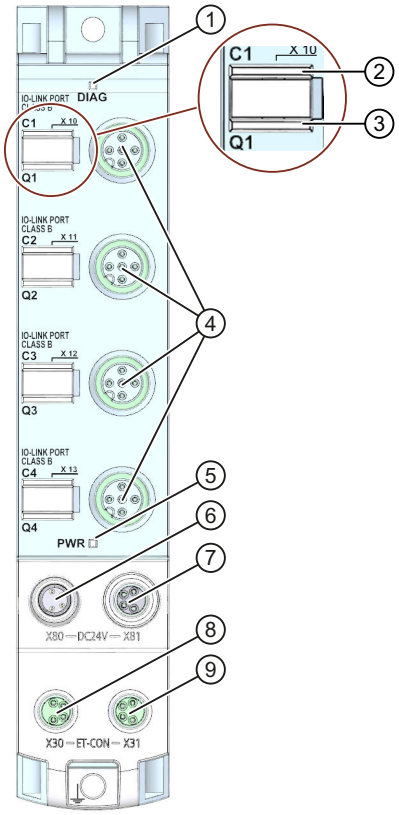
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

2.2 Operator controls and display elements

The following figure shows the operator controls and display elements of the CM 4xIO-Link 4xM12 communication module.



① DIAG: LED display for mode and diagnostic status
② C1 to C4: LED displays for port status
③ Q1 to Q4: LED displays for channel status in SIO mode
④ X10 to X13: Sockets for device connection
⑤ PWR: LED display for the load voltage 2L+
⑥ X80: Connector for infeed of the supply voltage (POWER input)
⑦ X81: Socket for loop-through of the supply voltage (POWER output)
⑧ X30: Socket for ET-Connection IN
⑨ X31: Socket for ET-Connection OUT

Figure 2-120 Operator controls and display elements

2.3 Functions

IO-Link is a point-to-point connection between an IO-Link master and an IO-Link device. On the IO-Link master, you can use IO-Link devices as well as conventional sensors/actuators with unshielded standard cables using proven 3-wire technology. IO-Link is backward compatible to conventional digital sensors or actuators. Switching status channel and data channel are in proven 24 V DC technology.

Reference

For more information on the IO-Link system, please see the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) function manual.

2.4 Reset communication module to factory settings

Effects of resetting to the factory settings

Use the "Reset to factory settings" function to restore the parameter assignments of your CM 4xIO-Link 4xM12 communication module made with S7-PCT to the factory state.

After a "Reset to factory settings", the parameters of the CM 4xIO-Link 4xM12 communication module are assigned as follows:

- The ports are in DI mode
- The ports are mapped to the relative addresses 0.0 ... 0.3
- The PortQualifier is disabled
- The I&M data 1 ... 3 are deleted

NOTE

The device parameters are deleted and the factory state is restored.
You should reset a removed CM 4xIO-Link 4xM12 communication module to the factory settings before you place it in storage.

Procedure

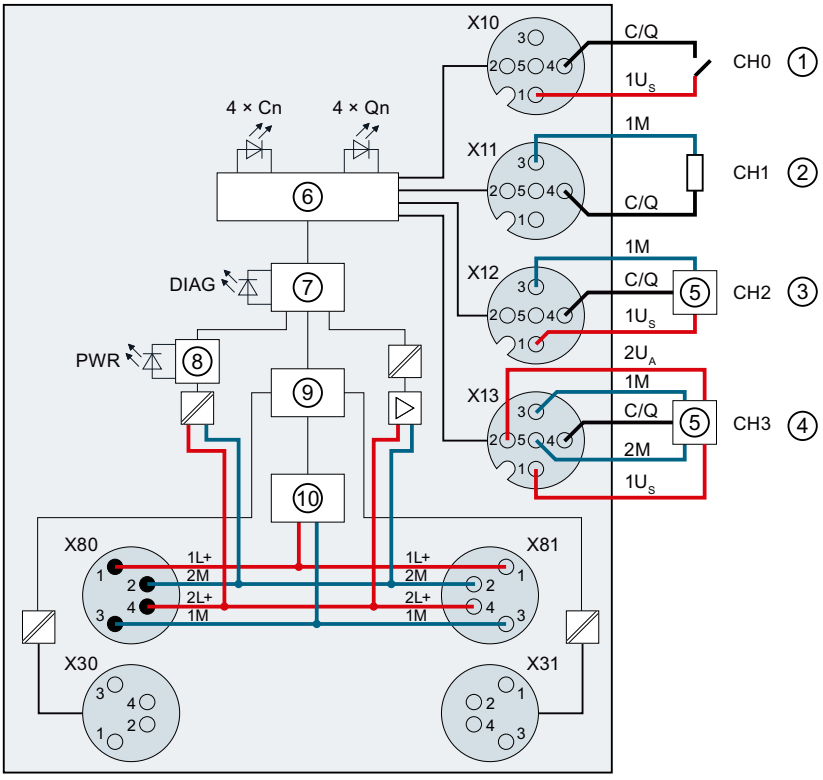
To perform a "Reset to factory settings", proceed as described in the S7-PCT online help.

Wiring

3

3.1 Terminal and block diagram

The following figure shows an example of the pin assignment for Port Class A (Type A) and Port Class B (Type b).



①	SIO input	X31	Loop-through of the ET-Connection
②	SIO output	1L+	Supply voltage 1L+ (non-switched)
③	Port Class A (Type A)	1M	Ground 1M (non-switched)
④	Port Class B (Type B)	2L+	Load voltage 2L+ (switched)
⑤	IO-Link device	2M	Ground 2M (switched)
⑥	IO-Link switching	1U$_S$	24 V encoder supply
⑦	Microcontroller	2U$_A$	24 V actuator supply
⑧	Monitoring	1M	Ground for encoder supply
⑨	ET-Connection interface	2M	Ground for actuator supply
⑩	Internal supply voltage	C/Q	Port n
X10 to X13	Channels 0 to 3	Cn	LEDs channel status (green)
X80	Infeed of supply voltages	Qn	LED status in SIO mode (green)
X81	Loop-through of supply voltages	DIAG	LED diagnostic status (red/green)
X30	Infeed of the ET-Connection	PWR	LED supply voltage 2L+ (green)

Figure 2-121 Terminal and block diagram

3.2 Pin assignment

NOTE

Color coding
The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

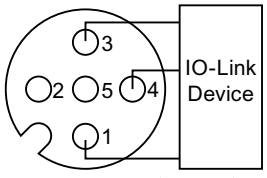
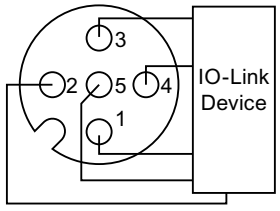
Pin assignment of the IO-Link sockets

NOTE

Port Class B
The pin assignment of the IO-Link interface corresponds to the IO-Link specification as per Port Class B. Port Class B is specially suited for the connection of actuators with additional supply (e.g. valve terminals).
To connect devices with Port Class A (e.g. sensors) to the communication module CM 4xIO-Link 4xM12, a 3-wire connection cable should be used (Port Class A compatibility).

The table below shows the pin assignments of the 4 sockets for the connection of IO-Link.

Table 2-286 Pin assignment of the IO-Link

Pin	Assignment	Front view of the sockets
	X10 to X13 - sockets for IO-Link	
1	24 V encoder supply $1U_S$ (from 1L+)	Port Class A (Type A)*  Port Class B (Type B) 
2	24 V actuator supply $2U_A$ (from 2L+)	
3	Encoder supply ground 1M	
4	Port 1 (C/Q): Connector X10 Port 2 (C/Q): Connector X11 Port 3 (C/Q): Connector X12 Port 4 (C/Q): Connector X13	
5	Ground for actuator supply 2M	
* If you use the sockets for IO-Link as Port Class A, you may not place any signals on pins 2 and 5.		

The M12 connectors are designed according to IO-Link specification as port type Class B. Pins 2 and 5 contain an additional power supply.

Reaction-free connection of devices with different port types (Class A and Class B) is possible using a 3-wire connecting cable (assignment of pins 1, 3 and 4).

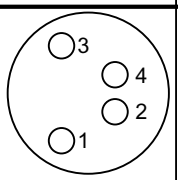
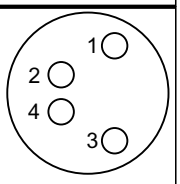
NOTICE

24 V encoder supply $1U_S$
For the supply of devices, only use the 24 V $1U_S$ encoder supply provided by the communication device.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

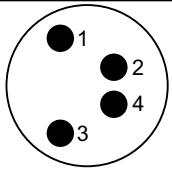
Table 2-287 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

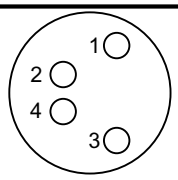
Table 2-288 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-289 Pin assignment of the supply voltage socket

Pin	Assignment **X81 socket (POWER output)**	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the connector for ET-Connection and the connector for the supply voltage can destroy the module.

Parameters/address space

4

4.1 Parameters

Parameters

The following table shows the general parameters for the communication module CM 4xIO-Link 4xM12.

Table 2-290 General parameters

Parameters	Range of values	Default	Scope
Diagnostics			
Diagnostics: No supply voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics port 1	• Disable • Enable	Disable	Channel
Diagnostics port 2	• Disable • Enable	Disable	Channel
Diagnostics port 3	• Disable • Enable	Disable	Channel
Diagnostics port 4	• Disable • Enable	Disable	Channel
Configuration			
Input / output type	See table in section Explanation of the parameters (Page 17)	32I/32O	Module
Port configuration without S7-PCT	• Disable • Enable	Disable	Module
Port Qualifier Information (PQI)	• Disable • Enable	Enable	Module

The following table shows the port parameters for the communication module CM 4xIO-Link 4xM12 with firmware version V1.1.

Table 2-291 Port parameters

Parameters	Range of values	Default
Port configuration		
Operating mode	• IO-Link autostart • IO-Link manual • DI • DQ • Disabled	IO-Link autostart
Length of input data (without PQI)	Depending on the total length of the module*	Depending on the total length of the module*
Length of output data	Depending on the total length of the module*	Depending on the total length of the module*
Vendor ID**	Vendor ID of the connected IO-Link device	0
Device ID**	Device ID of the connected IO-Link device	0
Testing accuracy / data storage**	• Same type (V1.0) without Backup&Restore • Type compatible (V1.1) without Backup&Restore • Type compatible (V1.1) with Backup&Restore • Type compatible (V1.1) with Restore	Type compatible (V1.1) with Backup&Restore

* Make sure that you do not exceed the maximum possible length of the input or output data for all ports that you selected.
Example:
You selected the 64I/64O configuration. You have assigned 16 bytes of input data to the first port. You can still assign a total of 48 bytes of input data for the remaining three ports.

** Only in effect when "IO-Link manual" port mode is used.

4.2 Explanation of the parameters

Diagnostics: No supply voltage 2L+

Enabling of the diagnostics for no or insufficient supply voltage 2L+.

Diagnostics port

This parameter enables the diagnostics for the selected port.
The diagnostics possible depends on the IO-Link device in use. Additional information about the diagnostic interrupts can be found in the description of the utilized IO-Link device.

Input / output type

This parameter sets the maximum length of the input and output data of the module.

Port configuration without S7-PCT

This parameter releases the port configuration without S7-PCT for the module.

Port Qualifier Information

This parameter releases the Port Qualifier Information (PQI).
The PQI provides information on the device status of the port and IO-Link.

Operating mode

This parameter determines the mode in which the selected port should be operated.
You can select from the following options:

- IO-Link autostart
- IO-Link manual
- DI
- DQ
- Disabled

IO-Link autostart

The connected IO-Link device starts automatically (Plug&Play functionality). The IO-Link device is immediately ready for operation.

IO-Link manual

The connected IO-Link device is **not** started automatically.
You must store the Vendor ID and Device ID of the connected IO-Link device in STEP 7.
In addition, you can select the inspection severity for data storage:

- Identical type (V1.0) without Backup&Restore
- Type-compatible (V1.1) without Backup&Restore
- Type-compatible (V1.1) with Backup&Restore
- Type-compatible (V1.1) with Restore

You can find the Vendor ID and Device ID on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).

DI

The port is operating as a standard digital input.

DQ

The port is operating as a standard digital output.

Disabled

The port is disabled.

Configuration options of the communication module CM 4xIO-Link 4xM12

The CM 4xIO-Link 4xM12 communication module supports a variable address space for I/O data.

The following table provides an overview of the configuration options for the supported address spaces for I/O data:

Table 2-292 Configuration options of the communication module CM 4xIO-Link 4xM12

Module configuration/ supporting address space for I/O data	IO-Link Master with Firmware V1.0	IO-Link Master with Firmware V1.1	IO-Link master with firmware V1.2
1-byte input/1-byte output	X		
2-byte inputs/2-byte outputs	X		
4-byte inputs/4-byte outputs	X	X*	X*
8-byte inputs/0-byte outputs		X	X
8-byte inputs/8-byte outputs	X	X	X
12-byte inputs/8-byte outputs		X	X
16-byte inputs/16-byte outputs	X	X	X
20-byte inputs/16-byte outputs		X	X
32-byte inputs/32-byte outputs	X	X	X
36-byte inputs/32-byte outputs			X
48-byte inputs/48-byte outputs			X
52-byte inputs/48-byte outputs			X
64-byte inputs/64-byte outputs			X
68-byte inputs/64-byte outputs			X
80-byte inputs/80-byte outputs			X
84-byte inputs/80-byte outputs			X
96-byte inputs/96-byte outputs			X
100-byte inputs/96-byte outputs			X
112-byte inputs/112-byte outputs			X
116-byte inputs/112-byte outputs			X
128-byte inputs/128-byte outputs			X
132-byte inputs/128-byte outputs			X

* No PortQualifierInformation is transferred with this configuration.

Port configuration

You can use a CM 4xIO-Link 4xM12 communication module as of firmware version V1.1 to commission the IO-Link ports of the IO-Link master or the connected IO-Link devices in two different ways:

- Port configuration without S7-PCT
- Port configuration with S7-PCT

Port configuration without S7-PCT

Requirement

You have enabled the check box "Port configuration without S7-PCT" for the configuration of the IO-Link master in STEP 7.

Procedure

You configure the IO-Link master directly in STEP 7:

- Enabling of the diagnostics
- Configuration of the I/O data lengths per port
- Enabling of the Port Qualifier Information (PQI)
- Port mode:
  - Operation in "IO-Link autostart" mode (default)
  - Operation in "IO-Link manual" mode
  - Operated as DI
  - Operated as DQ
  - Disabled

Port configuration with S7-PCT

Requirement

You deselected the "Port configuration without S7-PCT" check box in the configuration of the IO-Link master in STEP 7.

Procedure

You configure the port configuration of the IO-Link master using the port configuration tool S7-PCT as of V3.2.

Port Qualifier Information (PQI)

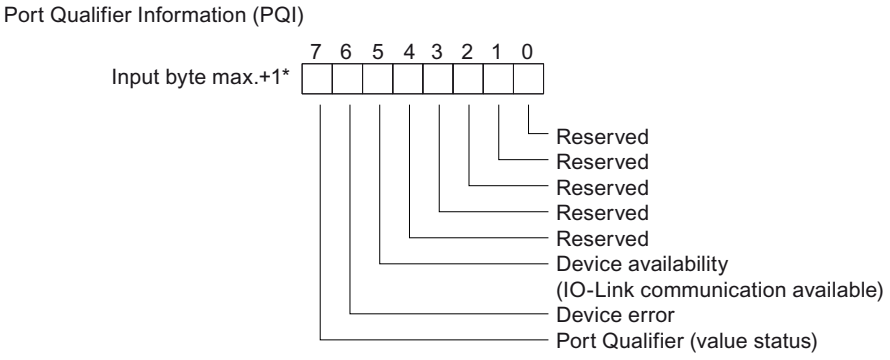
You can enable the Port Qualifier Information (PQI) for your IO-Link master as of firmware version V1.1.

NOTE

Port Qualifier Information (PQI)

If you have enabled the Port Qualifier Information (PQI), this information is always sent with the size of 1 byte together with the input data of the IO-Link device.

The following figure show the structure of the PQI byte.
You enable a parameter by setting the corresponding bit to "1".



* The PQI byte is always located after the last input byte of the port.

Figure 2-122 Structure of the PQI byte

Reference

For more information, please refer to the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) function manual.

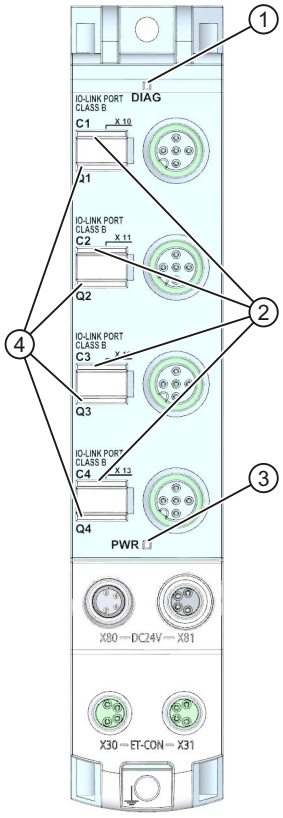
Diagnostics alarms

5

5.1 Status and error displays

LED displays

The following figure shows the LED display of the CM 4xIO-Link 4xM12 communication module.



①	Diagnostics (DIAG)	(green/red)
②	Port status / IO-Link status (Cn)	(green)
③	Load voltage 2L+ (PWR)	(green)
④	Channel status in SIO mode (Qn)	(green)

Figure 2-123 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 24).

DIAG LED

Table 2-293 Error display of the DIAG LED

DIAG LED	Meaning
▫ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

LEDs Cn

Valid for IO-Link port in IO-Link mode.

Table 2-294 Status displays of the C1, C2, C3, and C4 LEDs

C1, C2, C3, or C4 LED	Meaning
▫ Off	Port disabled or in SIO mode
☼ Flashes	Port in IO-Link mode, device not connected or port not connected with the configured device
■ On	Port in IO-Link mode, device not connected

PWR LED

Table 2-295 Status display of the PWR LED

PWR LED	Meaning
▫ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

LEDs Qn

Valid for IO-Link port in SIO mode.

Table 2-296 Status displays of the Q1, Q2, Q3, and Q4 LEDs

Q1, Q2, Q3, and Q4 LEDs	Meaning
□ Off	Process signal = 0 in SIO mode, deactivated or in IO-Link mode
■ On	Process signal = 1 in SIO mode

5.2 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the communication module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-297 Error types

Diagnostics alarm	Error code	Meaning (IO-Link error code)	IO-Link master	IO-Link device
Short-circuit	1_H	• Short-circuit at the process cables on the IO-Link device (1804_H)	X	
		• Short-circuit on IO device (7710_H)		X
Undervoltage	2_H	• Supply voltage too low (5111_H, 5112_H)		X
Overvoltage	3_H	• Supply voltage too high (5110_H)		X
Overtemperature	5_H	• Temperature exceeded on master (1805_H)	X	
		• Temperature exceeded on device (4000_H, 4210_H)		X
Wire break	6_H	• No IO-Link device connected • There is a break on the signal line to the IO-Link device • IO-Link device cannot communicate due to a different error (1800_H)	X	
Overflow	7_H	• Process tag range exceeded ($8C10_H$) • Measuring range exceeded ($8C20_H$)		X
Underflow	8_H	• Process tag range too low ($8C30_H$)		X
Error	9_H	• All IO-Link error codes which are not listed here are mapped to this PROFIBUS DP error		X
Parameter assignment error	10_H	• Incorrect device (1802_H) • Vendor ID and Device ID not defined (1817_H) • Process data length of the IO-Link device exceeded (1818_H) • No cycle time configured (1819_H) • IO-Link master could not be configured (1882_H, 1883_H) • Memory error (1886_H) • Process data length exceeded (1887_H) • PQI not supported (1889_H)	X	
		• Device was not configured correctly (6320_H, 6321_H, 6350_H)		X
Supply voltage missing	11_H	• 24 V encoder supply $1U_S$ (of 1L+) for device missing (1806_H) • 24 V encoder supply $1U_S$ (of 1L+) for device too low (<20 V) (1807_H) • Load voltage 2L+ (switched) missing (1888_H) • 24 V actuator supply 2 UA (of 2L+) for device missing ($180E_H$)	X	

Diagnostics alarm	Error code	Meaning (IO-Link error code)	IO-Link master	IO-Link device
Defective fuse	12_H	• Fuse on device is defective (5101_H)		X
Safety shutdown	19_H	• Serious error (master has to be replaced) (1880_H)	X	
External fault	$1A_H$	• Error during data backup (1809_H, $180A_H$, $180B_H$, $180C_H$, $180D_H$) • More than six errors are pending simultaneously on the IO-Link device (1808_H) • Consistency error in electronic coding element (1885_H) • Process data length exceeded (1887_H)	X	

Technical specifications

6

Technical specifications of the CM 4xIO-Link 4xM12 communication module

The following table shows the technical specifications as of 03/2021. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7147-5JD00-0BA0/td?dl=en).

Article number	6ES7147-5JD00-0BA0
General information	
Product type designation	CM 4x IO-Link
HW functional status	FS05
Firmware version	V1.2.x
Product function	
• I&M data	Yes; I&M0 to I&M3
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V13 SP1 or higher
• STEP 7 configurable/integrated from version	From V5.5 SP4 Hotfix 3
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.3.1
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction; load increasing
Input current	
Current consumption (rated value)	40 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	4
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	1.4 A; Total current of all ports
Power loss	
Power loss, typ.	2.6 W

Article number	6ES7147-5JD00-0BA0
IO-Link	
Number of ports	4
• of which simultaneously controllable	4
IO-Link protocol 1.0	Yes
IO-Link protocol 1.1	Yes
Transmission rate	4.8 kBaud (COM1); 38.4 kBaud (COM2), 230 kBaud (COM3)
Size of process data, input per port	32 byte
Size of process data, input per module	132 byte
Size of process data, output per port	32 byte
Size of process data, output per module	128 byte
Memory size for device parameter	2 kbyte; for each port
Master backup	Possible with function block IO_LINK_MASTER
Configuration without S7-PCT	Possible; autostart/manual function
Cable length unshielded, max.	20 m
Operating modes	
• IO-Link	Yes
• DI	Yes
• DQ	Yes; max. 100 mA
Connection of IO-Link devices	
• Port type A	Yes; via 3-core cable
• Port type B	Yes; Additional device supply: 1.6 A total current of all ports
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Monitoring the supply voltage	Yes
• Wire-break	Yes
• Short-circuit	Yes
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01

Article number	6ES7147-5JD00-0BA0
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SILCL according to IEC 62061	SILCL 2
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pole
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

Replacing modules

7

What do you need to know when replacing modules?

When you replace the communication module CM 4xIO-Link 4xM12, you must transfer the IO-Link parameter settings (master/device) again. You can transfer the IO-Link configuration using S7-PCT or save it with the Master Backup function.

Master Backup

The "IO_LINK_MASTER" function block is used to read all relevant IO-Link device and IO-Link master parameters. These can be stored retentively at a central location, such as in a data block in the IO controller.

The status of the IO-Link devices or IO-Link ports stored in the IO-Link master can be restored with the "IO_LINK_MASTER" function block.
As a result, the IO-Link ports and the IO-Link master are configured with the values stored in the master backup.

A typical application is the restoration of parameters after replacement of the IO-Link master.

NOTE

Availability
Note that the Master Backup function is available only for IO-Link devices that are specified for the IO-Link Standard as of V1.1.

You will find information on the Master Backup and Master Restore functions in section "Master backup" of chapter "Integration into the automation system" of the IO-Link System (https://support.industry.siemens.com/cs/ww/en/view/65949252) function manual.

Reference

You will find additional information on replacing modules in the system manual ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) in the "Module" section.

You will find additional information on replacing IO-Link masters in the S7-PCT online help.

PROFIenergy

8

8.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- Controller failure
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the communication module is explained in the following sections.

Additional information

You can find additional information on working with PROFIenergy in the "PROFIenergy" section of the manual IM 157-1 PN interface module (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of function manual PROFINET with STEP 7 V13 (http://support.automation.siemens.com/WW/view/en/49948856).

Application examples (http://support.automation.siemens.com/WW/view/en/41986454) are also available on the Internet.

8.2 DI operating mode

Display

If no external supply voltage is connected, switching off supply voltages $1U_S$ and $2U_A$ also leads to switching off the associated channel status LED Qn.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Load voltage 2L+" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-298 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: Configured pause substitute value • Value status "BAD"

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.

If all channels require switching off during the pause, all supply voltages are switched off if no channel is assigned in PE_MODE_PROCEED.

8.3 DQ operating mode

Display

The channel status LEDs Qn show the output value.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Load voltage 2L+ missing" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-299 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off in the pause, the supply voltages are switched off.

8.4 IO-Link operating mode

Display

Switching off the supply voltage $1U_S$ also switches off the associated port status LED Cn.

Response to error detection

All channels which are set to "PE_MODE_PROCEED" and "PE_MODE_LAST_VALUE" in pause mode report errors as in productive operation.

The following conditions apply to all channels (ports) which switch to a different pause mode ("PE_MODE_SHUTDOWN" and "PE_MODE_SUBST_VALUE"):

- Switching off the supply voltage U_{Sn} (port) upon starting the "pause" does not lead to generation of the alarms "Wire break" and "Short circuit".
- Error detection is not possible during the "pause" (no IO-Link device communication):
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-300 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off[1] • Pause substitute value (input): 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltages $1U_S$ and $2U_A$ off[1] • Pause substitute value (input): 0_B • Value status "BAD"

1 Supply voltage $1U_S$ of the assigned port is switched off. Result: The IO-Link device is no longer supplied with voltage.

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.

If all channels require switching off in the pause, the supply voltages are switched off.

Dimension drawing

A

The following figure shows the dimension drawing of the CM 4xIO-Link 4xM12 communication module in front and side view.

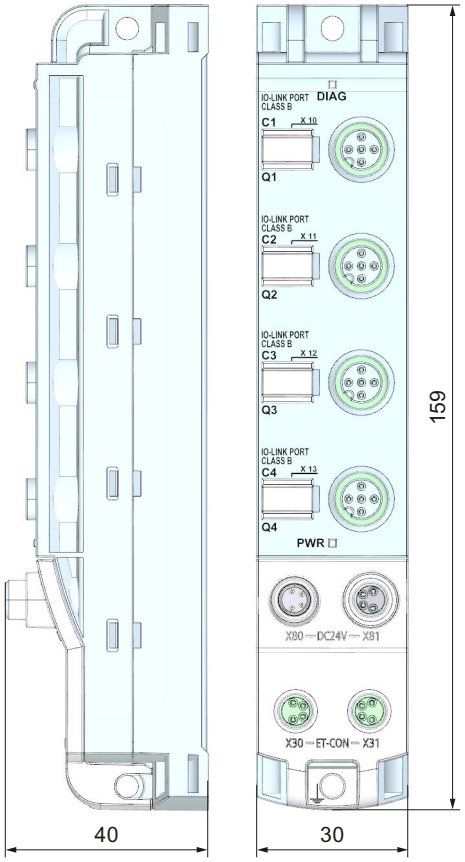


Figure 2-124 Dimension drawing

SIEMENS

SIMATIC

ET 200AL
CM 4xIO-Link 4xM12
(6ES7147-5JD01-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Single subslot/multi-subslot 5

Technical specifications 6

PROFIenergy 7

Dimension drawing A

08/2025
A5E54086399-AA

Table of contents

1 Introduction 4

1.1 ET 200AL IO-Link Documentation Guide 4
1.1.1 ET 200AL IO-Link I/O Modules Documentation Guide 4
1.1.2 SIMATIC Technical Documentation 5
1.1.3 Tool support 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 12

3.1 Properties 12
3.2 Operator controls and display elements 14
3.3 Functions 15

4 Wiring 17

4.1 Terminal and block diagram 17
4.2 Pin assignment 19

5 Single subslot/multi-subslot 22

5.1 Introduction: Single subslot and multi-subslot mode 22
5.2 Single subslot mode 23
5.2.1 Parameters/address space 23
5.2.1.1 Parameters 23
5.2.1.2 Explanation of parameters 24
5.2.1.3 Address space 26
5.2.2 Interrupts/diagnostic messages 29
5.2.2.1 Status and error displays 29
5.2.2.2 Interrupts 31
5.2.2.3 Diagnostics alarms 32
5.2.3 Resetting to factory settings in single subslot mode 33
5.2.3.1 Effects of resetting to factory settings 33
5.2.3.2 Procedure 33
5.3 Multi-subslot mode 33
5.3.1 Parameters/address space 33
5.3.1.1 Parameter 33
5.3.1.2 Explanation of parameters 34
5.3.1.3 Address space 36

5.3.2 Interrupts/diagnostic messages 38
5.3.2.1 Status and error displays 38
5.3.2.2 Interrupts 40
5.3.2.3 Diagnostic messages 41
5.3.3 Resetting to factory settings in multi-subslot mode 43
5.3.3.1 Effects of resetting to factory settings 43
5.3.3.2 Procedure 43

6 Technical specifications 44

7 PROFIenergy 47

7.1 Pause function 47
7.2 DI operating mode 48
7.3 DQ operating mode 49
7.4 IO-Link operating mode 50

A Dimension drawing 52

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL IO-Link Documentation Guide

1.1.1 ET 200AL IO-Link I/O Modules Documentation Guide



The documentation for the SIMATIC ET 200AL IO-Link I/O modules is divided into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL IO-Link distributed I/O system.

- ET 200AL IO-Link I/O Modules System Manual

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

- IO-Link I/O Modules Equipment Manual

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC IO-Link system.

- IO-Link System Function Manual

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International
(https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.

Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

1.1.3 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

SIMATIC S7-PCT

The Port Configuration Tool (PCT) is PC-based software for the parameter assignment of Siemens IO-Link Master modules and IO-Link devices from any manufacturer.

You integrate IO-devices using the standardized device description "IODD", which you get from the respective device manufacturer. S7-PCT supports version 1.0 and V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link Master from STEP 7. When STEP 7 is not used or the IO-Link Master is not operated on a SIMATIC controller, "standalone"-operation is also possible.

You can find more information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Industrial cybersecurity

2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual (http://support.automation.siemens.com/WW/view/en/89254965) for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

NOTE

Security-relevant changes to software or devices are documented in the New properties/functions chapter.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Pay attention to all relevant cybersecurity information.

Topics with cybersecurity-relevant information	Reference
Operational application environment and security assumptions	
Requirements for the operational application environment of the system and security assumptions	This section is found in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Security properties of the product	
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity chapter of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Supported Ethernet services	Information about supported services can be found in the Technical specifications chapter. You can find detailed information on the supported Ethernet services in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Interfaces, ports, protocols and services	
Information on the following is security-relevant: • Communications layer and communication role • Default states • Enabling/disabling of ports and services	You can find detailed information on these topics in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Secure operation	
Recommendations for secure operation	You can find cross-system information on the secure operation of I/O devices in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Corrective measures for known risks	Corrective measures for known risks are announced on the Siemens ProductCERT and Siemens CERT (https://siemens.com/productcert) web page. You can find more information on SIEMENS ProductCERT in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Security checks	You can find descriptions of specific security measures, such as cyclic checks of the configuration via checksums, in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Secure decommissioning Products that contain security-relevant data must be safely decommissioned before disposal or resale.	You can find information on secure decommissioning in the Secure operation of the system section in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

See also

PROFINET Function Manual (https://support.industry.siemens.com/cs/us/en/view/49948856)

Product overview

3

3.1 Properties

Article number

6ES7147-5JD01-0BA0

View of the module



Figure 2-125 View of the CM 4xIO-Link 4xM12 communications module

Properties

The module has the following technical properties:

- IO-Link Master according to IO-Link specification V1.1
- 4 IO-Link ports, type Class B
- 4 M12 connectors
- SIO mode (standard IO mode)
- Supported data transmission rates:
  - COM1 (4.8 kBd)
  - COM2 (38.4 kBd)
  - COM3 (230.4 kBd)

- Configuration limits:
  - Max. 33 bytes of input data and 32 bytes of output data per port
  - Max. 132 bytes of input data and 128 bytes of output data per module
- Automatic backup of device parameters during replacement of the IO-Link device (only for V1.1 devices)
- Suitable for connection of IO-Link devices with 3-wire and 5-wire connection
- Configurable diagnostics can be set for each channel
- Dimensions 30 x 159 mm
- Degrees of protection IP65 and IP67

The module supports the following functions:

- Firmware update
- Identification and maintenance data (I&M)
- PROFIenergy
- IO-Link port configuration with S7-PCT (as of V3.5 SP4)
- IO-Link port configuration without S7-PCT
- Master backup with function block "LIOLink_Master"
- Port Qualifier Information (PQI)
- Support of I/O data per module > 32 bytes

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

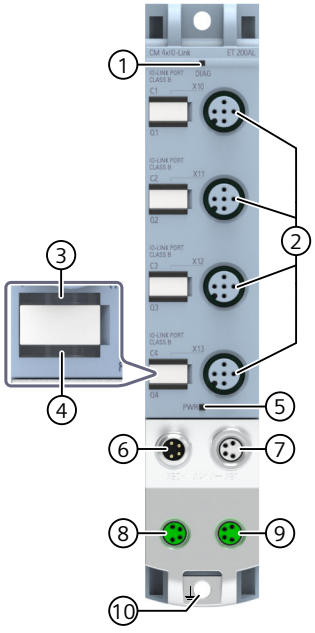
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The following figure shows the operator controls and display elements of the CM 4xIO-Link 4xM12 communication module.



① DIAG: LED display for mode and diagnostic status
② X10 to X13: Sockets for device connection
③ C1 to C4: LED displays for port status
④ Q1 to Q4: LED displays for channel status in SIO mode
⑤ PWR: LED display for load voltage 2L+
⑥ X80: Connector for infeed of the supply voltage (POWER input)
⑦ X81: Socket for loop-through of the supply voltage (POWER output)
⑧ X30: Socket for ET-Connection IN
⑨ X31: Socket for ET-Connection OUT
⑩ Functional earth (FE)

Figure 2-126 Operator controls and display elements

3.3 Functions

IO-Link is a point-to-point connection between an IO-Link master and an IO-Link device. On the IO-Link master, you can use IO-Link devices as well as conventional sensors/actuators with unshielded standard cables using proven 3-wire technology. IO-Link is downward-compatible to conventional digital sensors and actuators. The switching status and data channel are designed with proven 24 V DC technology.

Master Backup

The "LIOLink_Master" function block is used to read all relevant IO-Link device and IO-Link master parameters. These can be stored retentively at a central location, such as in a data block in the IO controller.

The status of the IO-Link devices or IO-Link ports stored in the IO-Link master can be restored with the "LIOLink_Master" function block.
As a result, the IO-Link ports and the IO-Link master are configured with the values stored in the master backup.

A typical application is the restoration of parameters after replacement of the IO-Link master.

NOTE
Availability
Note that the Master Backup function is available only for IO-Link devices that are specified for the IO-Link Standard as of V1.1.

You will find more information on the Master Backup and Master Restore functions in section "Master backup" of chapter "Integration into the automation system" of the IO-Link System (http://support.automation.siemens.com/WW/view/en/65949252) Function Manual.

Port Qualifier Information (PQI)

Each port has Port Qualifier Information (PQI). This PQI provides information on the device status of the port and IO-Link. The PQI is transmitted cyclically with the process data.

Port configuration

With an IO-Link master CM 4xIO-Link 4xM12, you can commission the IO-Link submodules (ports) of the IO-Link master or the connected IO-Link devices in two different ways:

- Port configuration without S7-PCT
- Port configuration with S7-PCT

Port configuration without S7-PCT

Requirements

You have selected the "Port configuration without S7-PCT" check box in the configuration of the IO-Link master submodule in STEP 7.

Procedure

You configure the IO-Link master submodules directly in STEP 7:

- Enabling of the diagnostics
- Port mode:
  - Operation in "IO-Link autostart" mode (default)
  - Operation in "IO-Link manual" mode

Port configuration with S7-PCT

Requirements

You have **cleared** the "Port configuration without S7-PCT (PDCT)" check box in the configuration of all IO-Link master submodules in STEP 7 (default).

Procedure

You configure the IO-Link master with the Port Configuration Tool S7-PCT (PDCT) V3.5 SP4 or higher.

Reference

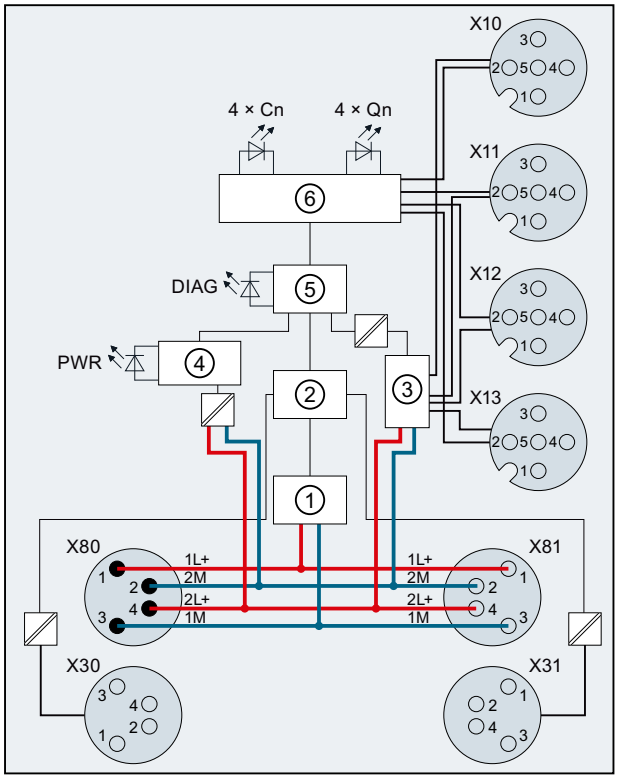
For more information on the IO-Link system, please see the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) function manual.

Wiring

4

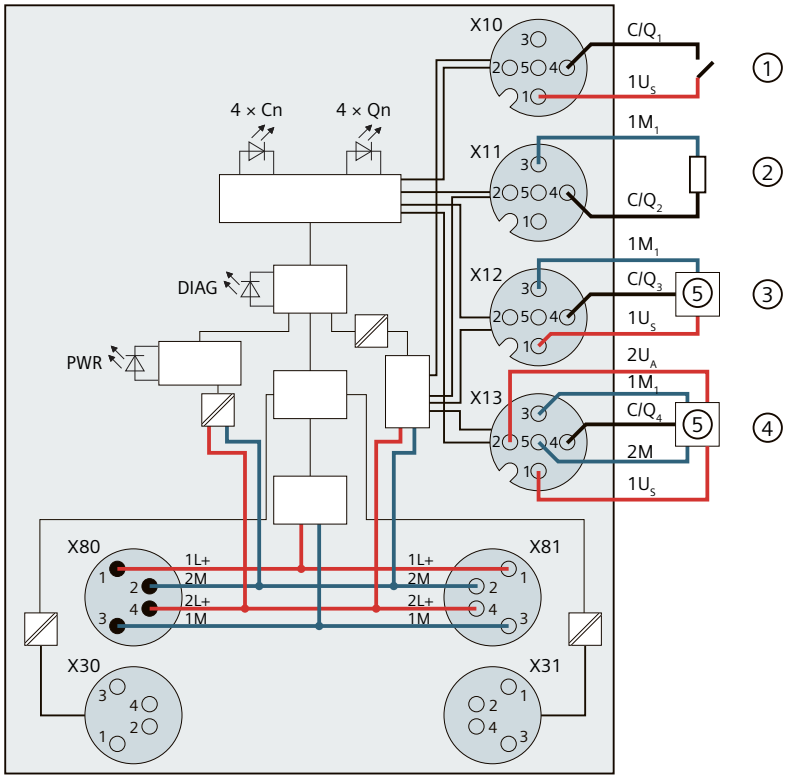
4.1 Terminal and block diagram

The figures below show an example of the connections and components of the module.



①	Internal supply voltage	X31	Loop-through of the ET-Connection
②	ET Connection interface	DIAG	LED diagnostic status (red/green)
③	Additional power supply ($2U_a$)	PWR	Supply voltage 2L+ LED (green)
④	Monitoring	1L+	Supply voltage 1L+ (non-switched)
⑤	Microcontroller	1M	Ground 1M (non-switched)
⑥	IO-Link circuit (1L+, $1M_1$)	2L+	Load voltage 2L+ (switched)
X10 to X13	Ports 1 to 4	2M	Ground 2M (switched)
X80	Infeed of supply voltages	Cn	LEDs channel status (green)
X81	Loop-through of supply voltages	Qn	LED status in SIO mode (green)
X30	Infeed of the ET-Connection		

Figure 2-127 Schematic circuit diagram



①	Class A, C/Q - DI	PWR	Supply voltage 2L+ LED (green)
②	Class A, C/Q - DQ	1L+	Supply voltage 1L+ (non-switched)
③	Class A, C/Q - IO-Link	1M	Ground 1M (non-switched)
④	Class B, $1U_s$, $2U_a$, C/Q - IO-Link	$1M_1$	Ground with reverse polarity protection, derived from 1 M (non-switched)
⑤	IO-Link device	2L+	Load voltage 2L+ (switched)
X10 to X13	Ports 1 to 4	2M	Ground 2M (switched)
X80	Infeed of supply voltages	Cn	LEDs channel status (green)
X81	Loop-through of supply voltages	Qn	LED status in SIO mode (green)
X30	Infeed of the ET-Connection	C/Q_n	IO-Link port n
X31	Loop-through of the ET-Connection	$1U_s$	24 V encoder supply (from 1L+)
DIAG	LED diagnostic status (red/green)	$2U_a$	24 V actuator supply (from 2L+)

Figure 2-128 Terminal circuit diagram

4.2 Pin assignment

NOTE

Color coding
The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

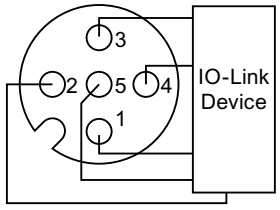
Pin assignment of the IO-Link sockets

NOTICE

Compatibility Port Class A/Port Class B
The pin assignment of the IO-Link interface corresponds to the IO-Link specification as per Port Class B. Port Class B is specially suited for the connection of actuators with additional supply (e.g. valve terminals).
To connect devices with Port Class A (e.g. sensors) to the communications module CM 4xIO-Link 4xM12, a 3-wire connecting cable should be used (Port Class A compatibility).

The table below shows the pin assignments of the 4 sockets for the connection of IO-Link.

Table 2-301 Pin assignment of the IO-Link sockets

Pin	Assignment **X10 to X13 - sockets for IO-Link**	Front view of the sockets
1	24 V encoder supply $1U_S$ (from 1L+)	Port Class B (X10 bis X13) 
2	24 V actuator supply $2U_A$ (from 2L+)	
3	Encoder supply ground $1M_1$	
4	Port 1 (C/Q): Connector X10 Port 2 (C/Q): Connector X11 Port 3 (C/Q): Connector X12 Port 4 (C/Q): Connector X13	
5	Ground for actuator supply 2M	

In the IO-Link specification, the M12 plugs are defined in Class B port type. Pins 2 and 5 contain an additional power supply.

NOTICE

24 V encoder supply $1U_S$
For the supply of devices, only use the 24 V $1U_S$ encoder supply provided by the communications module.

NOTICE

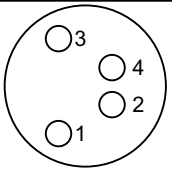
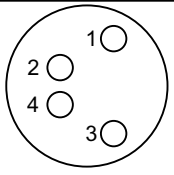
Reverse polarity protection
To guarantee reverse polarity protection, use the ground $1M_1$ supplied by the I/O device at pin 3 of the respective socket. Reverse polarity protection is deactivated when connecting 1M at X80/X81 and $1M_1$ at X10 bis X13.
For Port Class B, it must be ensured that the encoder and actuator supplies are electrically isolated.

NOTICE
Port Class B The pin assignment of the IO-Link interface of the sockets X10 to X13 corresponds to the IO-Link specification as per Port Class B. Port Class B is especially suitable for the connection of actuators with additional supply (e.g. valve terminals). You can connect devices with Port Class A (e.g. sensors) to Port Class B sockets. To connect devices with Port Class A to the communications module CM 4xIO-Link 4xM12, use a 3-wire connecting cable (Port Class A compatibility). More information about IO-Link can be found in the IO-Link System (https://support.industry.siemens.com/cs/us/en/view/65949252) Function Manual.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

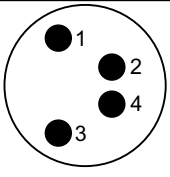
Table 2-302 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

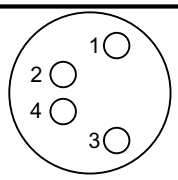
Table 2-303 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-304 Pin assignment of the supply voltage socket

Pin	Assignment **X81 socket (POWER output)**	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE
ET-Connection/supply voltage Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the connector for ET-Connection and the connector for the supply voltage can destroy the module.

See also

Safety-related shutdown of ET200AL standard modules (Page %getreference)

Single subslot/multi-subslot

5

5.1 Introduction: Single subslot and multi-subslot mode

The module can be operated in single subslot or multi-subslot mode in PROFINET. You can make the corresponding configuration in the TIA Portal.

Single subslot mode

The single subslot mode corresponds to the original implementation of IO-Link in PROFINET. It is a manufacturer-specific implementation of older IO-Link products on the market. Since they do not consider the PROFINET specification for IO-Link integration, some functionalities are limited in single subslot mode, as shown in the table below.

The single subslot mode is mandatory for PROFIBUS interface modules and all modules that do not support multi-subslot configuration. PLCs can also only be configured in single subslot mode. This device offers you the option to choose between single subslot and multi-subslot configuration in its settings, making it also compatible with such devices.

In single subslot mode, all process data is transmitted over PROFINET in a shared data record. You can adjust the data mapping in the TIA Portal.

Multi-subslot mode

The multi-subslot mode corresponds to the current IO-Link implementation according to the specification "IO-Link integration to Profinet". Each IO-Link master port represents an independent and standalone unit (subslot) in PROFINET, which is not influenced by the other units. This allows you to benefit from the latest technologies and features, such as advanced diagnostics, shared device or pull-plug technology. In the multi-subslot configuration, the identification data (I&M0) of the connected IO-Link devices can additionally be read from the subslots.

Multi-subslot mode requires connection to a suitable interface module and is therefore not supported by some older devices on the market or by PROFIBUS.

Process data is sent independently for respective subslots. The data mapping does not need to be specified additionally.

	Single subslot mode	**Multi-subslot mode**
Process data	• One shared data record for all channels	• Independent data records for the respective channels
Diagnostics	• Diagnostics are sent for the entire module • The distinction is made using the channels	• Diagnostics are sent independently for each subslot. • Support of extended diagnostics with detailed information
Parameter assignment	• One parameter assignment for the entire module	• Each subslot is parameterized separately, enabling advanced features (e.g. shared device, I&M0)
Extra features compared to previous modules	-	• Shared Device • Extended diagnostics • Pull-plug alarm • I&M0 data per channel

To use the multi-subslot mode, it is necessary to configure compatible modules.

NOTE

Switchover between single and multi-subslot mode
If "Port configuration without S7-PCT" is disabled, perform reconfiguration in the S7-PCT tool after the switchover.

5.2 Single subslot mode

5.2.1 Parameters/address space

5.2.1.1 Parameters

The following table shows the general parameters for the CM 4xIO-Link 4xM12 communications module in single subslot mode:

Table 2-305 General parameters

Parameters	**Range of values**	**Default**	**Scope**
Diagnostics			
Diagnostics: No supply voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Port 1	• Disable • Enable	Disable	Channel
Diagnostics: Port 2	• Disable • Enable	Disable	Channel
Diagnostics: Port 3	• Disable • Enable	Disable	Channel
Diagnostics: Port 4	• Disable • Enable	Disable	Channel

Parameters	Range of values	Default	Scope
Configuration			
Input / output type	See table in section Address space (Page 26)	32I/32O	Module
Port configuration without S7-PCT	• Disable • Enable	Disable	Module
Port Qualifier Information (PQI)	• Disable • Enable	Enable	Module

The following table shows the port parameters for the CM 4xIO-Link 4xM12 communications module in single subslot mode.

Table 2-306 Port parameters

Parameters	Range of values	Default
Port configuration		
Operating mode	• IO-Link autostart • IO-Link manual • DI • DQ • Disabled	IO-Link autostart
Length of input data (without PQI)	Depending on the total length of the module*	Depending on the total length of the module*
Length of output data	Depending on the total length of the module*	Depending on the total length of the module*
Vendor ID**	Vendor ID of the connected IO-Link device	0
Device ID**	Device ID of the connected IO-Link device	0
Inspection severity / data storage**	• Same type (V1.0) without Backup&Restore • Type-compatible (V1.1) without Backup&Restore • Type-compatible (V1.1) with Backup&Restore • Type-compatible (V1.1) with Restore	Type-compatible (V1.1) with Backup&Restore

* Make sure that you do not exceed the maximum possible length of the input or output data for all ports that you selected.
Example:
You selected the 64I/64O configuration. You have assigned 16 bytes of input data to the first port.
You can still assign a total of 48 bytes of input data for the remaining three ports.

** Only in effect when "IO-Link manual" port mode is used.

5.2.1.2 Explanation of parameters

Diagnostics: No supply voltage 2L+

The diagnostic message is enabled for missing or insufficient supply voltage 2L+.

Diagnostics: Port

This parameter enables the diagnostics for the selected IO-Link port.
The diagnostics possible depends on the IO-Link device in use. Additional information about the diagnostic interrupts can be found in the description of the utilized IO-Link device.

Input/output type

This parameter sets the maximum length of the input and output data of the module.

Port configuration without S7-PCT

This parameter releases the port configuration without S7-PCT for the module.

NOTE

Changes to the port configuration
If you have assigned the IO-Link device parameters via port configuration without S7-PCT, or have configured the port as a digital input, digital output or deactivated, you can no longer change the port configuration via S7-PCT.

PortQualifierInformation

This parameter releases the Port Qualifier Information (PQI).
The PQI provides information on the device status of the port and IO-Link.

Operating mode

This parameter determines the mode in which the selected port should be operated.
You can select from the following options:

- IO-Link autostart
- IO-Link manual
- DI
- DQ
- Disabled

IO-Link autostart

The connected IO-Link device starts automatically (Plug&Play functionality). The IO-Link device is immediately ready for operation.

IO-Link manual

The connected IO-Link device is **not** started automatically.
You must store the Vendor ID and Device ID of the connected IO-Link device in STEP 7.

DI

The port is operating as a standard digital input.

DQ

The port is operating as a standard digital output.

Disabled

The port is disabled.

Inspection severity / data storage

You can select the inspection severity for data storage:

- Same type (V1.0) without Backup&Restore
- Type-compatible (V1.1) without Backup&Restore
- Type-compatible (V1.1) with Backup&Restore
- Type-compatible (V1.1) with Restore

See also

You can find out more about the vendor ID and the device ID of an IO-Link device on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).

5.2.1.3 Address space

Configuration options of the communications module CM 4xIO-Link 4xM12

The CM 4xIO-Link 4xM12 communications module supports a variable address space for I/O data.

The following configuration options for the supported address spaces for I/O data of the IO-Link master with firmware version 2.0 or higher are available:

- 4-byte input/4-byte output
- 8-byte input/0-byte output
- 8-byte input/8-byte output
- 12-byte input/8-byte output
- 16-byte input/16-byte output
- 20-byte input/16-byte output
- 32-byte input/32-byte output
- 36-byte input/32-byte output
- 48-byte input/48-byte output
- 52-byte input/48-byte output
- 64-byte input/64-byte output
- 68-byte input/64-byte output
- 80-byte input/80-byte output
- 84-byte input/80-byte output
- 96-byte input/96-byte output
- 100-byte input/96-byte output
- 112-byte input/112-byte output
- 116-byte input/112-byte output
- 128-byte input/128-byte output
- 132-byte input/128-byte output

Port configuration

You can use a CM 4xIO-Link 4xM12 communications module as of firmware version V2.0 to commission the IO-Link ports of the IO-Link master or the connected IO-Link devices in two different ways:

- Port configuration without S7-PCT
- Port configuration with S7-PCT

Port configuration without S7-PCT

Requirement

You have enabled the check box "Port configuration without S7-PCT" for the configuration of the IO-Link master in STEP 7.

Procedure

You configure the IO-Link master directly in STEP 7:

- Enabling of the diagnostics
- Configuration of the I/O data lengths per port
- Enabling of the Port Qualifier Information (PQI)
- Port mode:
  - Operation in "IO-Link autostart" mode (default)
  - Operation in "IO-Link manual" mode
  - Operated as DI
  - Operated as DQ
  - Disabled

Port configuration with S7-PCT

Requirement

You deselected the "Port configuration without S7-PCT" check box in the configuration of the IO-Link master in STEP 7.

Procedure

You configure the IO-Link master with the Port Configuration Tool S7-PCT V3.5 SP4 or higher.

Port Qualifier Information (PQI)

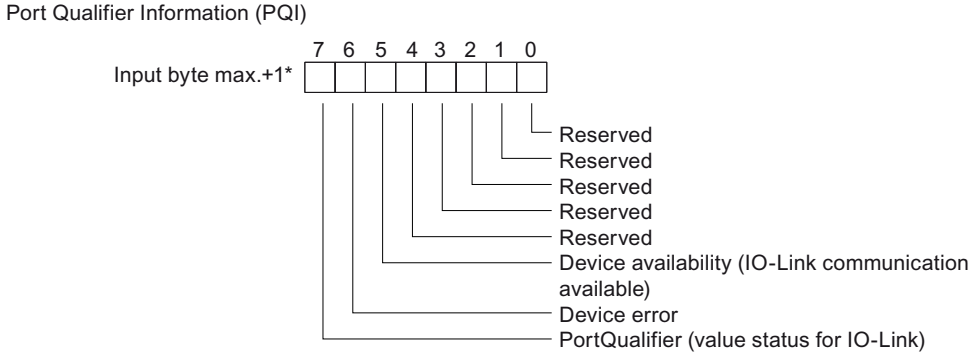
You can enable the PortQualifierInformation (PQI) for your IO-Link master.

NOTE

Port Qualifier Information (PQI)

If you have enabled the Port Qualifier Information (PQI), this information is always sent with the size of 1 byte together with the input data of the IO-Link device.

The figure below shows the structure of the PQI byte.



* The PQI byte is always located after the last input byte of the port.

Figure 2-129 Structure of the PQI byte

Reference

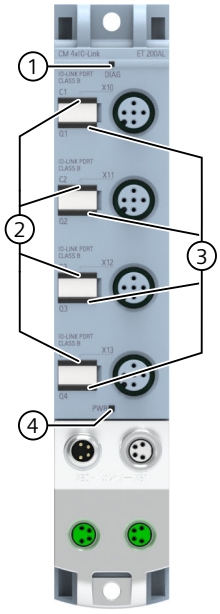
For more information, please refer to the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) function manual.

5.2.2 Interrupts/diagnostic messages

5.2.2.1 Status and error displays

LED displays

The following figure shows the LED display of the CM 4xIO-Link 4xM12 communications module.



①	Diagnostics (DIAG)	(green/red)
②	Port status/IO-Link status (C_n)	(green)
③	Channel status in SIO mode (Q_n)	(green)
④	Load voltage 2L+ (PWR)	(green)

Figure 2-130 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostic messages can be found in the section Diagnostic messages (Page 32).

DIAG LED

Table 2-307 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

Channel status LEDs C_n

Valid for IO-Link port in IO-Link mode.

Table 2-308 Status displays of the C_1, C_2, C_3, and C_4 LEDs

C_1, C_2, C_3, or C_4 LED	Meaning
☐ Off	Port disabled or in SIO mode
☼ Flashes	Port in IO-Link mode, device not connected or port not connected with the configured device
■ On	Port in IO-Link mode, device not connected

Channel status LEDs Q_n

Valid for IO-Link port in SIO mode.

Table 2-309 Status displays of the Q_1, Q_2, Q_3, and Q_4 LEDs

Q_1, Q_2, Q_3, and Q_4 LEDs	Meaning
☐ Off	Process signal = 0 in SIO mode, deactivated or in IO-Link mode
■ On	Process signal = 1 in SIO mode

PWR LED

Table 2-310 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.2.2.2 Interrupts

Interrupts

The IO-Link master CM 4xIO-Link 4xM12 supports the following interrupts in single subslot mode:

- Diagnostic interrupts

In case of an interrupt, the CPU of the IO controller automatically calls interrupt OBs. Information on the cause and class of the error is available, based on the OB number and start information.

Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).

Diagnostic interrupts

The I/O device generates a diagnostic interrupt on the following events:

- Wire break
- Internal module fault
- Parameter assignment error
- Short-circuit
- Low voltage 1L+

All IO-Link events of the type Error are mapped to the diagnostic interrupts of the assigned submodule. If you have parameterized the IO-Link master accordingly, it triggers a diagnostic interrupt for an incoming or outgoing event (alarm).
The coding of the events corresponds to the PROFINET standard of the channel diagnostics (USI=0x8000).

The CPU interrupts user program execution and processes the diagnostic interrupt OB (OB 82). You can determine the error events (channel diagnostics) with the "RALRM" instruction.

5.2.2.3 Diagnostics alarms

For each diagnostic event, a diagnostic message is issued and the DIAG LED flashes red on the communications module. You can read out the diagnostic messages for example, in the diagnostic buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-311 Error types

Diagnostics alarm	Error code	Meaning (IO-Link error code)	IO-Link master	IO-Link device
Short-circuit	1_H	• Short-circuit at the process cables on the IO-Link device (1804_H)	X	
		• Short-circuit on IO device (7710_H)		X
Undervoltage	2_H	• Supply voltage too low (5111_H, 5112_H)		X
Overvoltage	3_H	• Supply voltage too high (5110_H)		X
Overtemperature	5_H	• Temperature exceeded on master (1805_H)	X	
		• Temperature exceeded on device (4000_H, 4210_H)		X
Wire break	6_H	• No IO-Link device connected • There is a break on the signal line to the IO-Link device • IO-Link device cannot communicate due to a different error (1800_H)	X	
Overflow	7_H	• Process tag range exceeded ($8C10_H$) • Measuring range exceeded ($8C20_H$)		X
Underflow	8_H	• Process tag range too low ($8C30_H$)		X
Error	9_H	• All IO-Link error codes which are not listed here are mapped to this PROFIBUS DP error		X
Parameter assignment error	10_H	• Incorrect device (1802_H) • Vendor ID and Device ID not defined (1817_H) • Process data length of the IO-Link device exceeded (1818_H) • No cycle time configured (1819_H) • IO-Link master could not be configured (1882_H, 1883_H) • Memory error (1886_H) • Process data length exceeded (1887_H) • PQI not supported (1889_H)	X	
		• Device was not configured correctly (6320_H, 6321_H, 6350_H)		X
Supply voltage missing	11_H	• 24 V encoder supply $1U_S$ (of 1L+) for device missing (1806_H) • 24 V encoder supply $1U_S$ (of 1L+) for device too low (<20 V) (1807_H) • Load voltage 2L+ (switched) missing (1888_H) • 24 V actuator supply 2 UA (of 2L+) for device missing ($180E_H$)	X	
Defective fuse	12_H	• Fuse on device is defective (5101_H)		X
Safety shutdown	19_H	• Serious error (master has to be replaced) (1880_H)	X	
External fault	$1A_H$	• Error during data backup (1809_H, $180A_H$, $180B_H$, $180C_H$, $180D_H$) • More than six errors are pending simultaneously on the IO-Link device (1808_H) • Process data length exceeded (1887_H)	X	

5.2.3 Resetting to factory settings in single subslot mode

5.2.3.1 Effects of resetting to factory settings

Use the function "Reset to factory settings" to restore the parameter assignments of your CM 4xIO-Link 4xM12 communications module made with S7-PCT to the delivery state.

After a "Reset to factory settings" in single subslot mode, the parameters of the CM 4xIO-Link 4xM12 communications module are assigned as follows:

- The ports are in DI mode
- The ports are mapped to the relative addresses 0.0 ... 0.3
- The PortQualifier is disabled
- The I&M data 1 ... 3 is deleted

NOTE

The device parameters are deleted and the factory state is restored.
You should reset a removed CM 4xIO-Link 4xM12 communications module to the factory settings before you place it in storage.

5.2.3.2 Procedure

To perform a "Reset to factory settings", proceed as described in the S7-PCT online help.

5.3 Multi-subslot mode

5.3.1 Parameters/address space

5.3.1.1 Parameter

The following table shows the parameters for the CM 4xIO-Link 4xM12 communications module in multi-subslot mode:

Table 2-312 Diagnostics and port parameter IO-Link port

Parameter	Range of values	Default	Scope with configuration software, for example, MFCT
Diagnostics			
Diagnostics: Low voltage 1L+	• Disable • Enable	Disable	Channel
Diagnostics: No supply voltage 2L+	• Disable • Enable	Disable	Channel
Diagnostics: Port	• Disable • Enable	Disable	Channel
Port configuration			

* Only in effect when "IO-Link manual" port mode is used.

Parameter	Range of values	Default	Scope with configuration software, for example, MFCT
Port configuration without S7-PCT	• Disable • Enable	Disable	Channel
Operating mode	• IO-Link autostart • IO-Link manual	IO-Link autostart	Channel
Vendor ID*	Vendor ID of the connected IO-Link device	0	Channel
DeviceID*	Device ID of the connected IO-Link device	0	Channel
Inspection severity / data storage*	• Same type (V1.0) without Backup&Restore • Type-compatible (V1.1) without Backup&Restore • Type-compatible (V1.1) with Backup&Restore • Type-compatible (V1.1) with Restore	Type-compatible (V1.1) with Backup&Restore	Channel
Port cycle time*	-	As short as possible	Channel

* Only in effect when "IO-Link manual" port mode is used.

5.3.1.2 Explanation of parameters

Diagnostics: Low voltage 1L+

Enabling of the diagnostics for insufficient supply voltage 1L+.

Diagnostics: No supply voltage 2L+

The diagnostic message is enabled for missing or insufficient supply voltage 2L+.

Diagnostics: Port

This parameter enables the diagnostics for the selected IO-Link port.
The diagnostics possible depends on the IO-Link device in use. Additional information about the diagnostic interrupts can be found in the description of the utilized IO-Link device.

Port configuration without S7-PCT

This parameter releases the port configuration without S7-PCT for the module.

NOTE

Changes to the port configuration
If you have assigned the IO-Link device parameters via port configuration without S7-PCT, or have configured the port as a digital input, digital output or deactivated, you can no longer change the port configuration via S7-PCT.

Operating mode

This parameter determines the mode in which the selected port should be operated.
You can select from the following options:

- IO-Link autostart
- IO-Link manual

IO-Link autostart

The connected IO-Link device starts automatically (Plug&Play functionality). The IO-Link device is immediately ready for operation.

IO-Link manual

The connected IO-Link device is **not** started automatically.
You must store the Vendor ID and Device ID of the connected IO-Link device in STEP 7.
In addition, you can select the inspection severity for data storage:

- Same type (V1.0) without Backup&Restore
- Type-compatible (V1.1) without Backup&Restore
- Type-compatible (V1.1) with Backup&Restore
- Type-compatible (V1.1) with Restore

Port cycle time

Set the IO-Link cycle time at the corresponding port.

ET 200AL IO-Link devices configured on the IO-Link submodules

You can find the parameters for the ET 200AL IO-Link modules that can be selected as IO-Link submodules in the manual for the respective module:

- ET 200AL DI 16x24VDC 8xM12 (6ES7141-5AH00-0BL0)
- ET 200AL DI 8x24VDC 8xM8 (6ES7141-5BF00-0BL0)
- ET 200AL DQ 8x24VDC/2A 8xM12 (6ES7142-5AF00-0BL0)
- ET 200AL DIQ 16x24 V DC/0.5 A, 8x M12 (6ES7143-5AH00-0BL0),
- ET 200AL DIQ 4+DQ 4x 24 V DC/0.5 A (6ES7143-5BF00-0BL0)

See also

You can find out more about the vendor ID and the device ID of an IO-Link device on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).

5.3.1.3 Address space

The IO-Link master CM 4xIO-Link 4xM12 has four ports. Each port is represented by a submodule in multi-slot mode.

Configuration of the IO-Link ports of the IO-Link master CM 4xIO-Link 4xM12

The different operating modes of each IO-Link port are defined by configuring a corresponding submodule:

- As a digital input by configuring a digital input submodule
  - The address space is 1 byte input and the digital input value can be found in Bit 0 (without PQI).
- As a digital output by configuring a digital output submodule
  - The address space is 1 byte output and the digital output value can be found in Bit 0 (without PQI).
- as IO-Link device by configuring an IO-Link submodule,
- Port disabled:
  - In STEP 7 (TIA Portal): By deactivating the port enable.
  - with GSD: By plugging in a disabled IO-Link submodule (plugging in the submodule from the catalog, simply deleting an existing submodule is not sufficient)

The IO-Link ports are preconfigured as 2I + PQI.

When configuring IO-Link submodules, you can select the address spaces for I/O data in the following byte scales:

- ET 200AL DI 16x24VDC 8xM12
- ET 200AL DI 8x24VDC 8xM8
- ET 200AL DQ 8x24VDC/2A 8xM12
- ET 200AL DIQ 16x24 V DC/0.5 A, 8x M12
- ET 200AL DIQ 4+DQ 4x 24 V DC/0.5 A
- IO-Link 1 I/1 O + PQI
- IO-Link 2 I + PQI
- IO-Link 2 I/2 O + PQI
- IO-Link 4 I/4 O + PQI
- IO-Link 8 I/8 O + PQI
- IO-Link 16 I/16 O + PQI
- IO-Link 32 I/32 O + PQI

Port Qualifier Information (PQI)

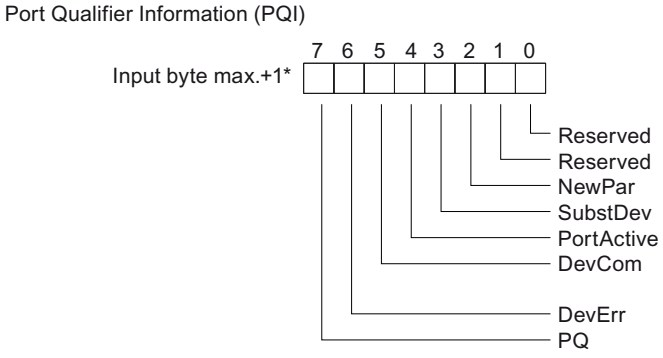
NOTE

Port Qualifier Information (PQI)

In multi-subslot mode, the PortQualifierInformation (PQI) for IO-Link submodules is always activated. The Port Qualifier Information (PQI) with the size 1 byte is always transmitted together with the input data of the IO-Link device.

	Designation	Value	Meaning
Bit0	-	-	Reserved
Bit1	-	-	Reserved
Bit2	NewPar*	0	No update of the device parameters detected
		1	Device parameter update detected
Bit3	SubstDev*	0	No backup device detected (identical serial number)
		1	Backup device detected (different serial number)
Bit4	PortActive	0	Port disabled
		1	Port enabled
Bit5	DevCom	0	IO-Link device is not available
		1	IO-Link device is in the "Preoperate" or "Operate" state
Bit6	DevErr	0	No error
		1	An error or warning has occurred.
Bit7	PQ	0	The data of the IO-Link device is invalid
		1	The data of the IO-Link device is valid

* Bits are reset with function block "LIOLink_Master"



* The PQI byte is always after the last input byte of the port.

Figure 2-131 Structure of the PQI byte

Reference

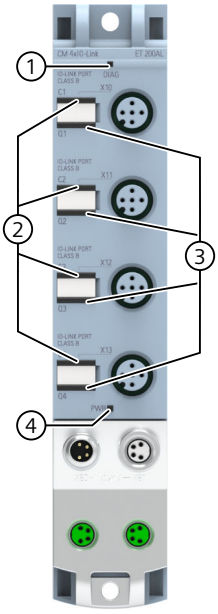
For more information, please refer to the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) Function Manual.

5.3.2 Interrupts/diagnostic messages

5.3.2.1 Status and error displays

LED displays

The following figure shows the LED display of the CM 4xIO-Link 4xM12 communications module.



①	Diagnostics (DIAG)	(green/red)
②	Port status/IO-Link status (C_n)	(green)
③	Channel status in SIO mode (Q_n)	(green)
④	Load voltage 2L+ (PWR)	(green)

Figure 2-132 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostic messages can be found in the section Diagnostic messages (Page 41).

DIAG LED

Table 2-313 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
On	Module parameters assigned and no module diagnostics
Flashes	Module parameters assigned and module diagnostics

Channel status LEDs C_n

Valid for IO-Link port in IO-Link mode.

Table 2-314 Status displays of the C_1, C_2, C_3, and C_4 LEDs

C_1, C_2, C_3, or C_4 LED	Meaning
Off	Port disabled or in SIO mode
Flashes	Port in IO-Link mode, device not connected or port not connected with the configured device
On	Port in IO-Link mode, device not connected

Channel status LEDs Q_n

Valid for IO-Link port in SIO mode.

Table 2-315 Status displays of the Q_1, Q_2, Q_3, and Q_4 LEDs

Q_1, Q_2, Q_3, and Q_4 LEDs	Meaning
Off	Process signal = 0 in SIO mode, deactivated or in IO-Link mode
On	Process signal = 1 in SIO mode

PWR LED

Table 2-316 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.3.2.2 Interrupts

Interrupts

The IO-Link master CM 4xIO-Link 4xM12 supports the following interrupts in multi-subslot mode:

- Diagnostic interrupts
- Pull/plug interrupt (at submodule port)

In case of an interrupt, the CPU of the IO controller automatically calls interrupt OBs. Information on the cause and class of the error is available, based on the OB number and start information.

Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).

Diagnostic interrupts

The I/O device generates a diagnostic interrupt on the following events:

- Wire break
- Internal module fault
- Parameter assignment error
- Short-circuit
- Low voltage 1L+

All IO-Link events of the type Error or Warning are mapped to the diagnostic interrupts of the assigned submodule. If you have parameterized the IO-Link master accordingly, it triggers a diagnostic interrupt for an incoming or outgoing event (alarm).
The coding of the events corresponds to the PROFINET standard of the extended channel diagnostics (USI=0x8002).

The CPU interrupts user program execution and processes the diagnostic interrupt OB (OB 82). You can determine the error events (channel diagnostics) with the "RALRM" instruction.

Pull/plug interrupts

If you remove an IO-Link device or the IO-Link communication is interrupted, a pull alarm is generated by the assigned submodule.
As soon as you plug the IO-Link device back in or the IO-Link communication is re-established, a plug alarm is generated.

When an insert/remove module interrupt occurs, the CPU interrupts execution of the user program and processes the insert/remove module interrupt OB (OB 83). The event that triggered the interrupt is set in the start information of the insert/remove OB.

5.3.2.3 Diagnostic messages

For each diagnostic event, a diagnostic message is issued and the DIAG LED flashes red on the communications module. You can read out the diagnostic messages for example, in the diagnostic buffer of the CPU. You can evaluate the error codes with the user program.

The IO-Link master can generate diagnostic alarms on behalf of the IO-Link device or the IO-Link port.

- Alarms of the "Diagnostics" type indicate a malfunction of the IO-Link device / port and should be corrected immediately.

IO-Link master error types

All IO-Link events of the type Error generated by the IO-Link device or port are mapped to the PROFINET diagnostic message of the type (severity) "Diagnosis" of the assigned submodule.

IO-Link device diagnostics

The IO-Link master generates PROFINET channel diagnostics (CET, ECET) from the IO-Link events of an IO-Link device according to the following mapping regulations:

In the "IO-Link Device Diagnostics - Page 1" (CET $0x9500_H$) the IO-Link event codes in the range 0x0000 - $0x7FFF_H$ are displayed directly:
$ECET_H$ = IO-Link Event $Code_H$

In the "IO-Link Device Diagnostics - Page 2" (CET $0x9501_H$) the IO-Link event codes in the range 0x8000 - $0xFFFF_H$ are displayed directly:
$ECET_H$ = (IO-Link Event $Code_H$ – $0x8000_H$)

Table 2-317 Overview of error types IO-Link device diagnostics

IO-Link event code	Error type (CET)	Extended error type (ECET)	Error text	Meaning
0x0000 - $0x7FFF_H$	$0x9500_H$ (38144_D)	0x0000 - $0x7FFF_H$ (0 - 32767_D)	Error / warning	See the manual of the IO-Link device or IODD file used.
0x8000 - $0xFFFF_H$	$0x9501_H$ (38145_D)	0x0000 - $0x7FFF_H$ (0 - 32767_D)	Error / warning	See the manual of the IO-Link device or IODD file used.

Example of displaying the IO-Link event codes:

An IO-Link device generates event code $0x4000_H$ (type "Error").
The channel diagnostics from the event code:

- PROFINET channel diagnostics type: Diagnosis, CET: $0x9500_H$, ECET: $0x4000_H$
  Diagnostic message "IO-Link Device Diagnostics - Page 1, Temperature fault - Overload", generated from the IO-Link event code $0x4000_H$.

IO-Link port diagnostics

The IO-Link master generates channel diagnostics for each port. The port-specific channel diagnostics are shown in the port diagnostics (CET $0x9502_H$).

The following table gives you an overview of the possible diagnostic events and their meaning.

Table 2-318 Overview of error types IO-Link port diagnostics

Error type (CET)	Extended error type (ECET)	Error text	Meaning
$0x9502_H$ (38146_D)	$0x17FF_H$ (6143_D)	Process data mismatch	Check submodule configuration
	$0x1800_H$ (6144_D)	Device does not exist	Communication cancelled
	$0x1801_H$ (6145_D)	Configuration error in start-up	Check parameter assignment
	$0x1802_H$ (6146_D)	Wrong device VendorID	Check device
	$0x1803_H$ (6147_D)	Wrong device DeviceID	Check device
	$0x1804_H$ (6148_D)	Short-circuit to C/Q	Check port connection
	$0x1805_H$ (6149_D)	IO-Link PHY overtemperature	Temperature on PCB too high
	$0x1806_H$ (6150_D)	Short-circuit to L+	Check port connection
	$0x1808_H$ (6152_D)	Event overflow on the device	More events present than can currently be processed
	$0x1809_H$ (6153_D)	Backup failed	Memory outside the range 2k
	$0x180A_H$ (6154_D)	Backup invalid	Mismatch when identifying data storage
	$0x180B_H$ (6155_D)	Backup invalid	Unspecified data storage error
	$0x180C_H$ (6156_D)	Backup invalid	Upload error
	$0x180D_H$ (6157_D)	Backup invalid	Download error
	$0x6000_H$ (24576_D)	Cycle time invalid	Check cycle time
	$0x6001_H$ (24577_D)	Revision error	Incompatible protocol version
	$0x6002_H$ (24578_D)	ISDU batch failed	Parameter inconsistency

5.3.3 Resetting to factory settings in multi-subslot mode

5.3.3.1 Effects of resetting to factory settings

Use the function "Reset to factory settings" to restore the parameter assignments of your CM 4xIO-Link 4xM12 communications module made with S7-PCT to the delivery state.

After a "Reset to factory settings" in single subslot mode, the parameters of the CM 4xIO-Link 4xM12 communications module are assigned as follows:

- The ports are in DI mode
- The I&M data 1 ... 3 is deleted

NOTE

The device parameters are deleted and the factory state is restored.
You should reset a removed CM 4xIO-Link 4xM12 communications module to the factory settings before you place it in storage.

5.3.3.2 Procedure

To perform a "Reset to factory settings", proceed as described in the S7-PCT online help.

Technical specifications

6

Technical specifications of the communications module CM 4xIO-Link 4xM12

The following table lists the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7147-5JD01-0BA0/td?dl=en).

Article number	6ES7147-5JD01-0BA0
General information	
Product type designation	CM 4x IO-Link
HW functional status	FS01
Firmware version	V2.0.0
Product function	
• I&M data	Yes; I&M0 to I&M4
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V18 or higher
• STEP 7 configurable/integrated from version	STEP 7 V5.7 or higher SP1 or higher
• PROFIBUS from GSD version/GSD revision	GSD as of Revision 5
• PROFINET from GSD version/GSD revision	GSDML V2.4.x
Operating mode	
• IO-Link	Yes
• DI	Yes
• DQ	Yes; max. 100 mA
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; actuator power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	30 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value

Article number	6ES7147-5JD01-0BA0
Encoder supply	
Number of outputs	4
24 V encoder supply	
• Short-circuit protection	Yes; per channel, electronic
• Output current, max.	4 A; total current of all ports, max. 2 A per channel
Power loss	
Power loss, typ.	3 W
Address area	
Address space per module	
• Inputs	132 byte
• Outputs	128 byte
IO-Link	
Number of ports	4
• of which simultaneously controllable	4
IO-Link protocol 1.0	Yes
IO-Link protocol 1.1	Yes
Transmission rate	4.8 kBaud (COM1); 38.4 kBaud (COM2), 230 kBaud (COM3)
Cycle time, min.	2 ms
Size of process data, input per port	33 byte
Size of process data, input per module	132 byte
Size of process data, output per port	32 byte
Size of process data, output per module	128 byte
Memory size for device parameter	2 kbyte; for each port
Master backup	possible with LIOLink_Master function block
Configuration without S7-PCT	Possible; autostart/manual function
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type A	Yes; via 3-core cable
• Port type B	Yes; additional device supply: max. 1.6 A per port, max. 4 A per module
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Monitoring the supply voltage	Yes
• Wire-break	Yes
• Short-circuit	Yes
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes

Article number	6ES7147-5JD01-0BA0
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	No
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pin, A-coded
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	145 g

PROFIenergy 7

7.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- CPU stop
- CPU start
- Firmware update
- Station stop
- Station start
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the communication module is explained in the following sections.

NOTICE
Reconfiguration/factory reset in the PROFIenergy pause Reconfiguration or factory reset with S7-PCT is not permitted during a PE pause.

Additional information

You can find additional information on working with PROFIenergy in the "PROFIenergy" section of the manual IM 157-1 PN interface module (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of function manual PROFINET with STEP 7 V13 (http://support.automation.siemens.com/WW/view/en/49948856).

Application examples (http://support.automation.siemens.com/WW/view/en/41986454) are also available on the Internet.

7.2 DI operating mode

Display

If no external supply voltage is connected, switching off supply voltages $1U_S$ and $2U_A$ also leads to switching off the associated channel status LED Qn.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Load voltage 2L+" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-319 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: Configured pause substitute value • Value status "BAD"

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off during the pause, all supply voltages are switched off if no channel is assigned in PE_MODE_PROCEED.

7.3 DQ operating mode

Display

The channel status LEDs Qn show the output value.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Load voltage 2L+ missing" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-320 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off in the pause, the supply voltages are switched off.

7.4 IO-Link operating mode

Display

Switching off the supply voltage $1U_S$ also switches off the associated port status LED Cn.

Response to error detection

All channels which are set to "PE_MODE_PROCEED" and "PE_MODE_LAST_VALUE" in pause mode report errors as in productive operation.

The following conditions apply to all channels (ports) which switch to a different pause mode ("PE_MODE_SHUTDOWN" and "PE_MODE_SUBST_VALUE"):

- Switching off the supply voltage U_{Sn} (port) upon starting the "pause" does not lead to generation of the alarms "Wire break" and "Short circuit".
- Error detection is not possible during the "pause" (no IO-Link device communication):
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-321 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off[1] • Pause substitute value (input): 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltages $1U_S$ and $2U_A$ off[1] • Pause substitute value (input): 0_B • Value status "BAD"

[1] Supply voltage $1U_S$ of the assigned port is switched off. Result: The IO-Link device is no longer supplied with voltage.

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off in the pause, the supply voltages are switched off.

Dimension drawing

A

The following figure shows the dimension drawing of the CM 4xIO-Link 4xM12 communication module in front and side view.

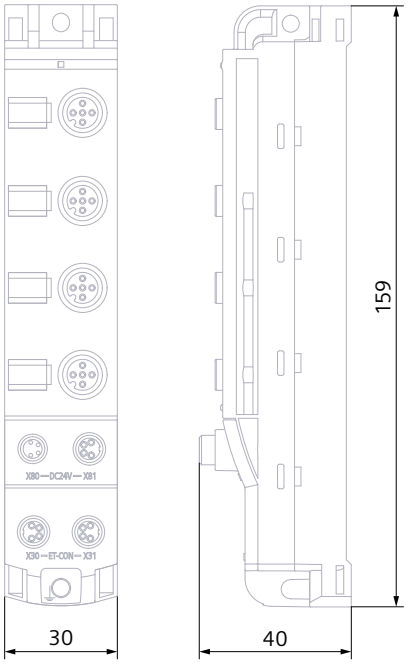


Figure 2-133 Dimension drawing

SIEMENS

SIMATIC

ET 200AL
CM 8xIO-Link + DIQ 6x24VDC/0.5A 8xM12 (6ES7147-5JJ00-0BA0)

Equipment Manual

Introduction 1

Industrial cybersecurity 2

Product overview 3

Wiring 4

Single subslot/multi-subslot 5

Technical specifications 6

PROFIenergy 7

Dimension drawing A

08/2025
A5E53131188-AA

Table of contents

1 Introduction 4

1.1 ET 200AL IO-Link Documentation Guide 4
1.1.1 ET 200AL IO-Link I/O Modules Documentation Guide 4
1.1.2 SIMATIC Technical Documentation 5
1.1.3 Tool support 7

2 Industrial cybersecurity 9

2.1 Introduction to industrial cybersecurity 9
2.2 Cybersecurity information 9
2.3 Cybersecurity-relevant information 10

3 Product overview 12

3.1 Properties 12
3.2 Operator controls and display elements 15
3.3 Functions 16

4 Wiring 18

4.1 Terminal and block diagram 18
4.2 Pin assignment 20

5 Single subslot/multi-subslot 24

5.1 Introduction: Single subslot and multi-subslot mode 24
5.2 Single subslot mode 25
5.2.1 Parameters/address space 25
5.2.1.1 Parameters 25
5.2.1.2 Explanation of parameters 27
5.2.1.3 Address space 28
5.2.2 Interrupts/diagnostic messages 31
5.2.2.1 Status and error displays 31
5.2.2.2 Interrupts 33
5.2.2.3 Diagnostics alarms 34
5.2.3 Resetting to factory settings in single subslot mode 35
5.2.3.1 Effects of resetting to factory settings 35
5.2.3.2 Procedure 35
5.3 Multi-subslot mode 35
5.3.1 Parameters/address space 35
5.3.1.1 Parameter 35
5.3.1.2 Explanation of the parameters 36
5.3.1.3 Address space 39

5.3.2 Interrupts/diagnostic messages ... 43
5.3.2.1 Status and error displays ... 43
5.3.2.2 Interrupts ... 45
5.3.2.3 Diagnostic messages ... 46
5.3.3 Resetting to factory settings in multi-subslot mode ... 48
5.3.3.1 Effects of resetting to factory settings ... 48
5.3.3.2 Procedure ... 49

6 Technical specifications ... 50

7 PROFIenergy ... 54

7.1 Pause function ... 54
7.2 DI operating mode ... 55
7.3 DQ operating mode ... 56
7.4 IO-Link operating mode ... 57

A Dimension drawing ... 59

Introduction

1

Purpose of the documentation

This Equipment Manual supplements the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) System Manual. Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present Equipment Manual, the System Manual and the Function Manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For ecologically sustainable recycling and disposal of your old device, contact a certified disposal service for electronic scrap and dispose of the device in accordance with the regulations in your country.

1.1 ET 200AL IO-Link Documentation Guide

1.1.1 ET 200AL IO-Link I/O Modules Documentation Guide



The documentation for the SIMATIC ET 200AL IO-Link I/O modules is divided into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL IO-Link distributed I/O system.

- ET 200AL IO-Link I/O Modules System Manual

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

- IO-Link I/O Modules Equipment Manual

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC IO-Link system.

- IO-Link System Function Manual

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International
(https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.

Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

1.1.3 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

SIMATIC S7-PCT

The Port Configuration Tool (PCT) is PC-based software for the parameter assignment of Siemens IO-Link Master modules and IO-Link devices from any manufacturer.

You integrate IO-devices using the standardized device description "IODD", which you get from the respective device manufacturer. S7-PCT supports version 1.0 and V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link Master from STEP 7. When STEP 7 is not used or the IO-Link Master is not operated on a SIMATIC controller, "standalone"-operation is also possible.

You can find more information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Industrial cybersecurity 2

2.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual (http://support.automation.siemens.com/WW/view/en/89254965) for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to your SIMATIC device.

NOTE

Security-relevant changes to software or devices are documented in the New properties/functions chapter.

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

2.3 Cybersecurity-relevant information

Pay attention to all relevant cybersecurity information.

Topics with cybersecurity-relevant information	Reference
Operational application environment and security assumptions	
Requirements for the operational application environment of the system and security assumptions	This section is found in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Security properties of the product	
Signed firmware update	The topic of signed firmware updates is described in the Industrial cybersecurity chapter of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Supported Ethernet services	Information about supported services can be found in the Technical specifications chapter. You can find detailed information on the supported Ethernet services in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Interfaces, ports, protocols and services	
Information on the following is security-relevant: • Communications layer and communication role • Default states • Enabling/disabling of ports and services	You can find detailed information on these topics in the Communication Function Manual (https://support.industry.siemens.com/cs/us/en/view/59192925).
Secure operation	
Recommendations for secure operation	You can find cross-system information on the secure operation of I/O devices in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Corrective measures for known risks	Corrective measures for known risks are announced on the Siemens ProductCERT and Siemens CERT (https://siemens.com/productcert) web page. You can find more information on SIEMENS ProductCERT in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Security checks	You can find descriptions of specific security measures, such as cyclic checks of the configuration via checksums, in the Industrial cybersecurity section of the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).
Secure decommissioning Products that contain security-relevant data must be safely decommissioned before disposal or resale.	You can find information on secure decommissioning in the Secure operation of the system section in the System Manual (http://support.automation.siemens.com/WW/view/en/89254965).

See also

PROFINET Function Manual (https://support.industry.siemens.com/cs/us/en/view/49948856)

Product overview

3

3.1 Properties

Article number

6ES7147-5JJ00-0BA0

View of the module

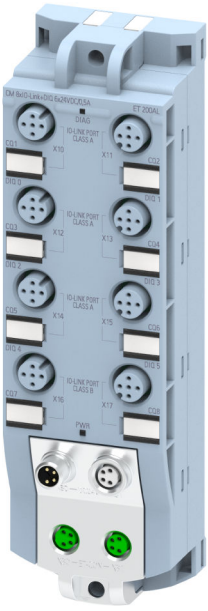


Figure 2-134 View of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module

Properties

The module has the following technical properties:

- IO-Link Master according to IO-Link specification V1.1
- 6 IO-Link Ports Class A + 2 IO-Link Ports Class B
- 6 digital inputs/digital outputs, depending on parameter assignment
- 8 M12 sockets for connection of sensors or actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Configurable diagnostics can be set for each channel
  - Suitable for switches and proximity switches

- Digital outputs:
  - Rated load voltage 24 V DC
  - Configurable diagnostics can be set for each channel
  - Output current per output 0.5 A
  - Suitable for solenoid valves, DC contactors, and indicator lights
- SIO mode (standard IO mode)
- Supported data transmission rates:
  - COM1 (4.8 kBd)
  - COM2 (38.4 kBd)
  - COM3 (230.4 kBd)
- Configuration limits:
  - Max. 33 bytes of input data and 32 bytes of output data per port
  - Max. 237 bytes of input data and 237 bytes of output data per module
- Automatic backup of device parameters during replacement of the IO-Link device (only for V1.1 devices)
- Suitable for connection of IO-Link devices with 3-wire and 5-wire connection
- Configurable diagnostics can be set for each channel
- Dimensions 159 x 45 x 40 mm
- Degrees of protection IP65 and IP67

The module supports the following functions:

- Firmware update
- Identification and maintenance data (I&M)
- PROFIenergy
- IO-Link port configuration with S7-PCT as of V3.5 SP4
- IO-Link port configuration without S7-PCT
  - IO-Link autostart
  - IO-Link manual
- Master backup with function block "LIOLink_Master"
- Port Qualifier Information (PQI)
- Support of I/O data per module > 32 bytes

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

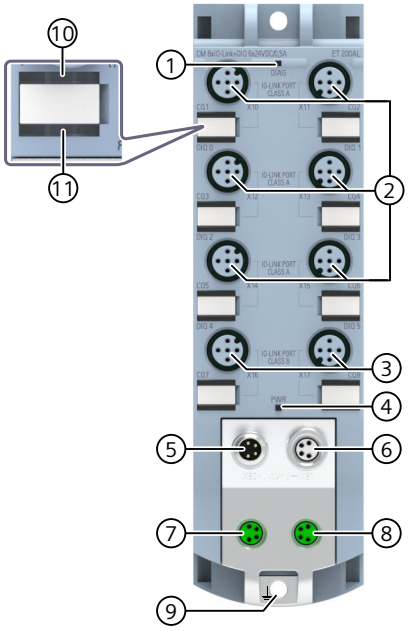
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (http://support.automation.siemens.com/WW/view/en/89254965) system manual.

3.2 Operator controls and display elements

The following figure shows the operator controls and display elements of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module.



① DIAG: LED display for mode and diagnostic status
② X10 to X15: Socket for device connection, IO-Link Port Class A
③ X16 and X17: Socket for device connection, IO-Link Port Class B
④ PWR: LED display for load voltage 2L+
⑤ X80: Connector for infeed of the supply voltage (POWER input)
⑥ X81: Socket for loop-through of the supply voltage (POWER output)
⑦ X30: Socket for ET-Connection IN
⑧ X31: Socket for ET-Connection OUT
⑨ Functional earth (FE)
⑩ CQ1 to CQ8: LED displays for channel status IO-Link
⑪ DIQ0 to DIQ5: LED displays for channel status digital input/digital output

Figure 2-135 Operator controls and display elements

3.3 Functions

IO-Link is a point-to-point connection between an IO-Link master and an IO-Link device. On the IO-Link master, you can use IO-Link devices as well as conventional sensors/actuators with unshielded standard cables using proven 3-wire technology. IO-Link is downward-compatible to conventional digital sensors and actuators. The switching status and data channel are designed with proven 24 V DC technology.

Master Backup

The "LIOLink_Master" function block is used to read all relevant IO-Link device and IO-Link master parameters. These can be stored retentively at a central location, such as in a data block in the IO controller.

The status of the IO-Link devices or IO-Link ports stored in the IO-Link master can be restored with the "LIOLink_Master" function block.
As a result, the IO-Link ports and the IO-Link master are configured with the values stored in the master backup.

A typical application is the restoration of parameters after replacement of the IO-Link Master.

NOTE
Availability
Note that the Master Backup function is available only for IO-Link devices that are specified for the IO-Link Standard as of V1.1.

You will find more information on the Master Backup and Master Restore functions in section "Master backup" of chapter "Integration into the automation system" of the IO-Link System (http://support.automation.siemens.com/WW/view/en/65949252) Function Manual.

Port Qualifier Information (PQI)

Each port has Port Qualifier Information (PQI). This PQI provides information on the device status of the port and IO-Link. The PQI is transmitted cyclically with the process data. The PQI can only be deactivated in single subslot mode.

Port configuration

With an IO-Link master CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12, you can commission the IO-Link submodules (ports) of the IO-Link master or the connected IO-Link devices in two different ways:

- Port configuration without S7-PCT
- Port configuration with S7-PCT

Port configuration without S7-PCT

Requirements

You have selected the "Port configuration without S7-PCT" check box in the configuration of the IO-Link master submodule in STEP 7.

Procedure

You configure the IO-Link master submodules directly in STEP 7:

- Enabling of the diagnostics
- Port mode:
  - Operation in "IO-Link autostart" mode (default)
  - Operation in "IO-Link manual" mode

Port configuration with S7-PCT

Requirements

You have **cleared** the "Port configuration without S7-PCT (PDCT)" check box in the configuration of all IO-Link master submodules in STEP 7 (default).

Procedure

You configure the IO-Link master with the Port Configuration Tool S7-PCT (PDCT) V3.5 SP4 or higher.

Reference

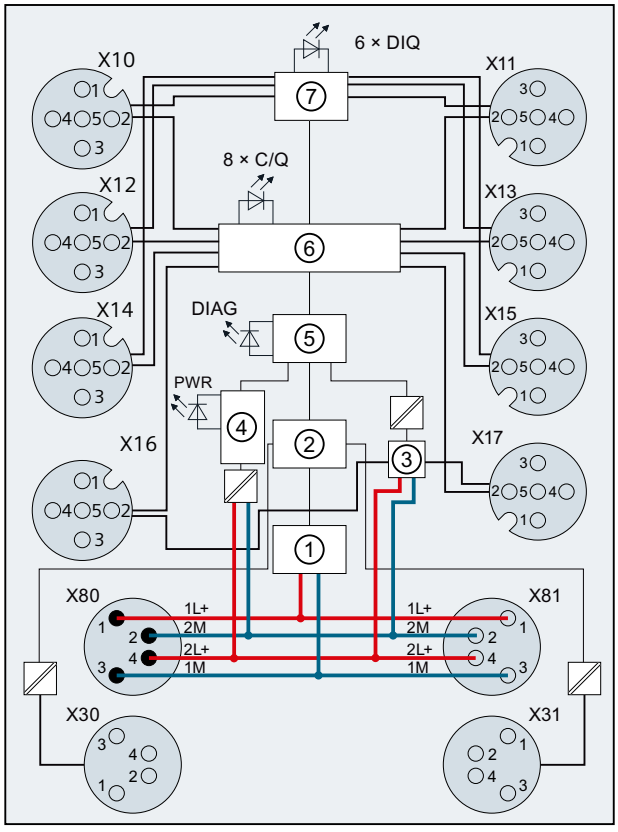
For more information on the IO-Link system, please see the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) function manual.

Wiring

4

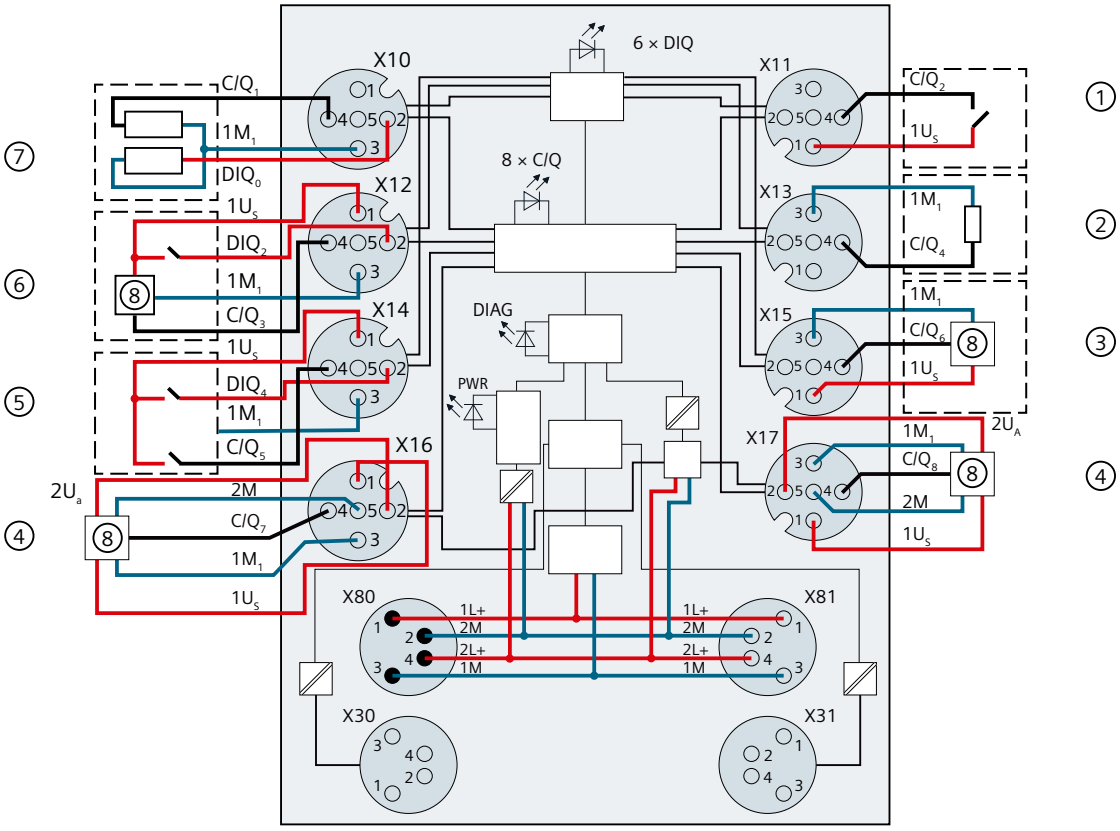
4.1 Terminal and block diagram

The figures below show an example of the connections and components of the module.



①	Internal supply voltage	X30	Infeed of the ET-Connection
②	ET Connection interface	X31	Loop-through of the ET-Connection
③	Additional power supply ($2U_a$)	DIAG	LED diagnostic status (red/green)
④	Monitoring	PWR	Supply voltage 2L+ LED (green)
⑤	Microcontroller	1L+	Supply voltage 1L+ (non-switched)
⑥	IO-Link circuit (1L+, $1M_1$)	1M	Ground 1M (non-switched)
⑦	DIQ circuit (1L+, $1M_1$)	2L+	Load voltage 2L+ (switched)
X10 to X17	Ports 1 to 8	2M	Ground 2M (switched)
X80	Infeed of supply voltages	C/Q	IO-Link port
X81	Loop-through of supply voltages	DIQ	Input signal / output signal

Figure 2-136 Schematic circuit diagram



①	Class A, C/Q - DI	DIAG	LED diagnostic status (red/green)
②	Class A, C/Q - DQ	PWR	Supply voltage 2L+ LED (green)
③	Class A, C/Q - IO-Link	1L+	Supply voltage 1L+ (non-switched)
④	Class B, $1U_S$, $2U_a$, C/Q - IO-Link	1M	Ground 1M (non-switched)
⑤	Class A, C/Q - DI, DIQ - DI	$1M_1$	Ground with reverse polarity protection, derived from 1 M (non-switched)
⑥	Class A, C/Q - IO-Link, DIQ - DI	2L+	Load voltage 2L+ (switched)
⑦	Class A, C/Q - DQ, DIQ - DQ	2M	Ground 2M (switched)
⑧	IO-Link device	C/Q	IO-Link port
X10 to X17	Ports 1 to 8	C/Q_n	IO-Link port n
X80	Infeed of supply voltages	DIQ	Input signal / output signal
X81	Loop-through of supply voltages	$1U_s$	24 V encoder supply (from 1L+)
X30	Infeed of the ET-Connection	$2U_a$	24 V actuator supply (from 2L+)
X31	Loop-through of the ET-Connection		

Figure 2-137 Terminal circuit diagram

4.2 Pin assignment

NOTE

Color coding
The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

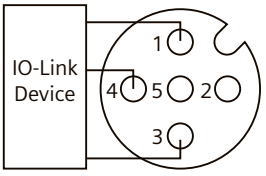
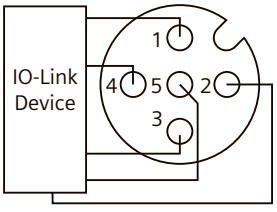
Pin assignment of the IO-Link sockets and digital inputs / digital outputs

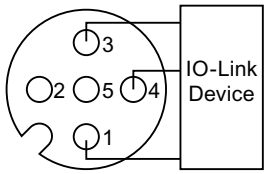
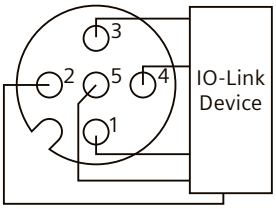
NOTICE

Compatibility Port Class A/Port Class B
The pin assignment of the IO-Link interface on X16 and X17 corresponds to the IO-Link specification as per Port Class B. Port Class B is especially suitable for the connection of actuators with additional supply (e.g. valve terminals).
To connect devices with Port Class A (e.g. sensors) to the communications module CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12, a 3-wire connecting cable should be used (Port Class A compatibility).

The table below shows the pin assignments of the 8 sockets for the connection of IO-Link and digital inputs/outputs.

Table 2-322 Pin assignment of the IO-Link sockets and digital inputs / digital outputs

Pin	Assignment		Front view of the sockets	
	Port Class A (Sockets X10 to X15)	**Port Class B (Sockets X16 to X17)**		
1	24 V encoder supply $1U_S$ (from 1L+)		Port Class A (X10, X12, X14)	Port Class B (X16)
2	Connector X10: Input/output signal DIQ_0 Connector X11: Input/output signal DIQ_1 Connector X12: Input/output signal DIQ_2 Connector X13: Input/output signal DIQ_3 Connector X14: Input/output signal DIQ_4 Connector X15: Input/output signal DIQ_5	24 V actuator supply $2U_A$ (from 2L+)		

Pin	Assignment		Front view of the sockets	
	Port Class A (Sockets X10 to X15)	**Port Class B (Sockets X16 to X17)**		
3	Encoder supply ground $1M_1$		Port Class A (X11, X13, X15) 	Port Class B (X17) 
4	Port 1 (C/Q): Connector X10 Port 2 (C/Q): Connector X11 Port 3 (C/Q): Connector X12 Port 4 (C/Q): Connector X13 Port 5 (C/Q): Connector X14 Port 6 (C/Q): Connector X15	Port 7 (C/Q): Connector X16 Port 8 (C/Q): Connector X17		
5	Not used	Ground for actuator supply 2M		

In the IO-Link specification, the M12 plugs are defined in Class B port type. Pins 2 and 5 contain an additional power supply.

NOTICE

24 V encoder supply $1U_S$
For the supply of devices, only use the 24 V $1U_S$ encoder supply provided by the communications module.

NOTICE

Reverse polarity protection
To guarantee reverse polarity protection, use the ground $1M_1$
supplied by the I/O device at pin 3 of the respective socket. Reverse polarity protection is deactivated when connecting 1M at X80/X81 and $1M_1$ at X10 bis X17.
For Port Class B, it must be ensured that the encoder and actuator supplies are electrically isolated.

NOTE

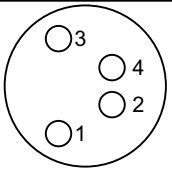
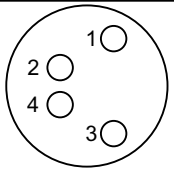
Number of IO channels
Each of the six sockets X10 to X15 can be assigned a maximum of two signals for Port Class A: IO-Link + Standard DIQ. IO-Link can also be configured as DI or DQ in SIO mode. Thus, the module can be used for a maximum of 14 digital channels (sum of DI, DQ and IO-Link ports in SIO mode). In such a case, the IO-Link ports cannot be used as IO-Link simultaneously.

NOTICE
Port Class B The pin assignment of the IO-Link interface of the sockets X16 and X17 corresponds to the IO-Link specification as per Port Class B. Port Class B is especially suitable for the connection of actuators with additional supply (e.g. valve terminals). You can connect devices with Port Class A (e.g. sensors) to Port Class B sockets. To connect devices with Port Class A to the communications module CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12, use a 3-wire connecting cable (Port Class A compatibility). More information about IO-Link can be found in the IO-Link System (https://support.industry.siemens.com/cs/us/en/view/65949252) Function Manual.

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the 2 sockets for the connection of ET-Connection.

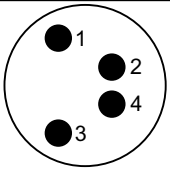
Table 2-323 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus line cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shield	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage.

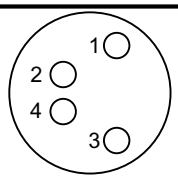
Table 2-324 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage.

Table 2-325 Pin assignment of the supply voltage socket

Pin	Assignment **X81 socket (POWER output)**	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

ET-Connection/supply voltage
Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage. Mixing up the connector for ET-Connection and the connector for the supply voltage can destroy the module.

Single subslot/multi-subslot

5

5.1 Introduction: Single subslot and multi-subslot mode

Single subslot mode

The single subslot mode corresponds to the original implementation of IO-Link in PROFINET. It is a manufacturer-specific implementation of older IO-Link products on the market. Since they do not consider the PROFINET specification for IO-Link integration, some functionalities are limited in single subslot mode, as shown in the table below.

The single subslot mode is mandatory for PROFIBUS interface modules and all modules that do not support multi-subslot configuration. PLCs can also only be configured in single subslot mode. This device offers you the option to choose between single subslot and multi-subslot configuration in its settings, making it also compatible with such devices.

In single subslot mode, all process data is transmitted over PROFINET in a shared data record. You can adjust the data mapping in the TIA Portal.

NOTE

Use of additional DIQs is not possible

The single subslot configuration does not allow modeling. The additional DIQs of this device are therefore not visible in the process image and parameter assignment and are thus not usable.

Multi-subslot mode

The multi-subslot mode corresponds to the current IO-Link implementation according to the specification "IO-Link integration to Profinet". Each IO-Link master port represents an independent and standalone unit (subslot) in PROFINET, which is not influenced by the other units. This allows you to benefit from the latest technologies and features, such as advanced diagnostics, shared device or pull-plug technology. In the multi-subslot configuration, the identification data (I&M0) of the connected IO-Link devices can additionally be read from the subslots.

Multi-subslot mode requires connection to a suitable interface module and is therefore not supported by some older devices on the market or by PROFIBUS.

Process data is sent independently for respective subslots. The data mapping does not need to be specified additionally.

	Single subslot mode	Multi-subslot mode
Process data	• One shared data record for all channels	• Independent data records for the respective channels
Diagnostics	• Diagnostics are sent for the entire module • The distinction is made using the channels	• Diagnostics are sent independently for each subslot. • Support of extended diagnostics with detailed information
Parameter assignment	• One parameter assignment for the entire module	• Each subslot is parameterized separately, enabling advanced features (e.g. shared device, I&M0)
Extra features compared to previous modules	-	• Shared Device • Extended diagnostics • Pull-plug alarm • Additional DIQ channels can be used • I&M0 data per channel

To use the multi-subslot mode, it is necessary to configure compatible modules.

NOTE

Switchover between single and multi-subslot mode
If "Port configuration without S7-PCT" is disabled, perform reconfiguration in the S7-PCT tool after the switchover.

5.2 Single subslot mode

5.2.1 Parameters/address space

5.2.1.1 Parameters

The following table shows the general parameters for the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module in single subslot mode.

Table 2-326 General parameters

Parameters	Range of values	Default	Scope
Diagnostics			
Diagnostics: No supply voltage 2L+	• Disable • Enable	Disable	Module
Diagnostics: Port 1	• Disable • Enable	Disable	Channel
Diagnostics: Port 2	• Disable • Enable	Disable	Channel
Diagnostics: Port 3	• Disable • Enable	Disable	Channel
Diagnostics: Port 4	• Disable • Enable	Disable	Channel
Diagnostics: Port 5	• Disable • Enable	Disable	Channel

Parameters	Range of values	Default	Scope
Diagnostics: Port 6	• Disable • Enable	Disable	Channel
Diagnostics: Port 7	• Disable • Enable	Disable	Channel
Diagnostics: Port 8	• Disable • Enable	Disable	Channel
Configuration			
Input / output type	See table in section Address space (Page 28)	32I/32O	Module
Port configuration without S7-PCT	• Disable • Enable	Disable	Module
Port Qualifier Information (PQI)	• Disable • Enable	Enable	Module

The following table shows the port parameters for the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module in single subslot mode.

Table 2-327 Port parameters

Parameters	Range of values	Default
Port configuration		
Operating mode	• IO-Link autostart • IO-Link manual • DI • DQ • Disabled	IO-Link autostart
Length of input data (without PQI)	Depending on the total length of the module*	Depending on the total length of the module*
Length of output data	Depending on the total length of the module*	Depending on the total length of the module*
Vendor ID**	Vendor ID of the connected IO-Link device	0
Device ID**	Device ID of the connected IO-Link device	0
Inspection severity / data storage**	• Same type (V1.0) without Backup&Restore • Type-compatible (V1.1) without Backup&Restore • Type-compatible (V1.1) with Backup&Restore • Type-compatible (V1.1) with Restore	Type-compatible (V1.1) with Backup&Restore

* Make sure that you do not exceed the maximum possible length of the input or output data for all ports that you selected.
Example:
You selected the 64I/64O configuration. You have assigned 16 bytes of input data to the first port.
You can still assign a total of 48 bytes of input data for the remaining seven ports.

** Only in effect when "IO-Link manual" port mode is used.

5.2.1.2 Explanation of parameters

Diagnostics: No supply voltage 2L+

The diagnostic message is enabled for missing or insufficient supply voltage 2L+.

Diagnostics: Port

This parameter enables the diagnostics for the selected IO-Link port.
The diagnostics possible depends on the IO-Link device in use. Additional information about the diagnostic interrupts can be found in the description of the utilized IO-Link device.

Input/output type

This parameter sets the maximum length of the input and output data of the module.

Port configuration without S7-PCT

This parameter releases the port configuration without S7-PCT for the module.

NOTE

Changes to the port configuration
If you have assigned the IO-Link device parameters via port configuration without S7-PCT, or have configured the port as a digital input, digital output or deactivated, you can no longer change the port configuration via S7-PCT.

PortQualifierInformation

This parameter releases the Port Qualifier Information (PQI).
The PQI provides information on the device status of the port and IO-Link.

Operating mode

This parameter determines the mode in which the selected port should be operated.
You can select from the following options:

- IO-Link autostart
- IO-Link manual
- DI
- DQ
- Disabled

IO-Link autostart

The connected IO-Link device starts automatically (Plug&Play functionality). The IO-Link device is immediately ready for operation.

IO-Link manual

The connected IO-Link device is **not** started automatically.
You must store the Vendor ID and Device ID of the connected IO-Link device in STEP 7.

DI

The port is operating as a standard digital input.

DQ

The port is operating as a standard digital output.

Disabled

The port is disabled.

Inspection severity / data storage**

You can select the inspection severity for data storage:

- Same type (V1.0) without Backup&Restore
- Type-compatible (V1.1) without Backup&Restore
- Type-compatible (V1.1) with Backup&Restore
- Type-compatible (V1.1) with Restore

See also

You can find out more about the vendor ID and the device ID of an IO-Link device on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).

5.2.1.3 Address space

Configuration options of the communications module CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12

The CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module supports a variable address space for I/O data in single subslot mode.

The following configuration options for the supported address spaces for I/O data of the IO-Link master with firmware version 2.0 or higher are available:

- 0-byte input/16-byte output
- 8-byte input/8-byte output
- 16-byte input/16-byte output
- 24-byte input/16-byte output
- 32-byte input/32-byte output
- 64-byte input/64-byte output
- 72-byte input/64-byte output
- 128-byte input/128-byte output
- 136-byte input/128-byte output
- 237-byte input/237-byte output

Port configuration

You can use a CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module to commission the IO-Link ports of the IO-Link master or the connected IO-Link devices in two different ways:

- Port configuration without S7-PCT
- Port configuration with S7-PCT

Port configuration without S7-PCT

Requirement

You have enabled the check box "Port configuration without S7-PCT" for the configuration of the IO-Link master in STEP 7.

Procedure

You configure the IO-Link master directly in STEP 7:

- Enabling of the diagnostics
- Configuration of the I/O data lengths per port
- Enabling of the Port Qualifier Information (PQI)
- Port mode:
  - Operation in "IO-Link autostart" mode (default)
  - Operation in "IO-Link manual" mode
  - Operated as DI
  - Operated as DQ
  - Disabled

Port configuration with S7-PCT

Requirement

You deselected the "Port configuration without S7-PCT" check box in the configuration of the IO-Link master in STEP 7.

Procedure

You configure the IO-Link master with the Port Configuration Tool S7-PCT V3.5 SP4 or higher.

Port Qualifier Information (PQI)

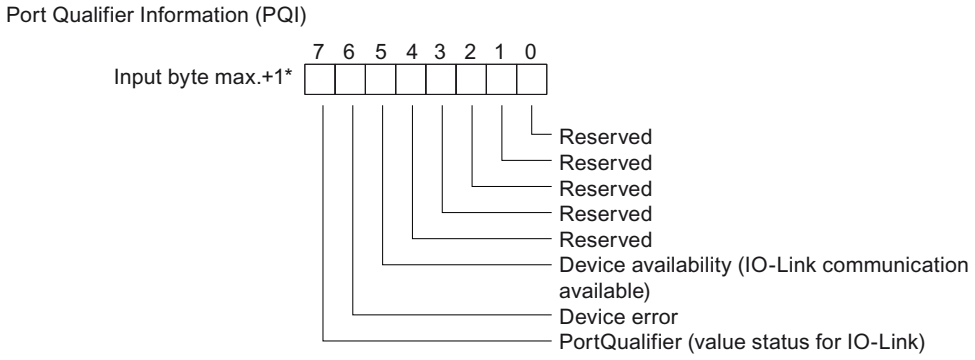
You can enable the PortQualifierInformation (PQI) for your IO-Link master.

NOTE

Port Qualifier Information (PQI)

If you have enabled the Port Qualifier Information (PQI), this information is always sent with the size of 1 byte together with the input data of the IO-Link device.

The following figure show the structure of the PQI byte.
You enable a parameter by setting the corresponding bit to "1".



* The PQI byte is always located after the last input byte of the port.

Figure 2-138 Structure of the PQI byte

Reference

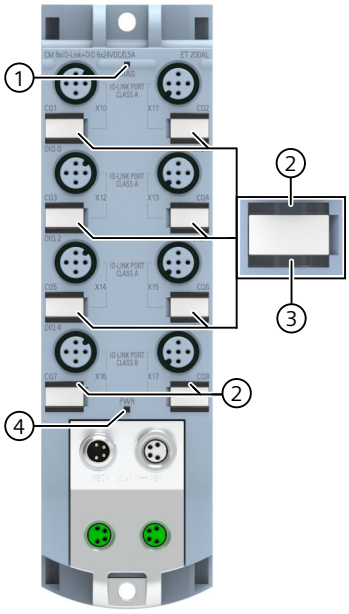
For more information, please refer to the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) function manual.

5.2.2 Interrupts/diagnostic messages

5.2.2.1 Status and error displays

LED displays

The following figure shows the LED display of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module.



①	Diagnostics (DIAG)	(green/red)
②	LED displays for port status (C/Q_n)	(green)
③	LED displays for channel status (DIQ_n)	(green)
④	Load voltage 2L+ (PWR)	(green)

Figure 2-139 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostic messages can be found in the section Diagnostic messages (Page 34).

DIAG LED

Table 2-328 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

Channel status LEDs CQ_n

Valid for IO-Link port in IO-Link mode:

Table 2-329 Status displays of the LEDs CQ_1 to CQ_8

LED CQ_1 to CQ_8	Meaning
☐ Off	Port disabled or in SIO mode
☼ Flashes	Port in IO-Link mode, device not connected or port not connected with the configured device
■ On	Port in IO-Link mode, device not connected

Valid for IO-Link port in SIO mode:

Table 2-330 Status displays of the LEDs CQ_1 to CQ_8

LED CQ_1 to CQ_8	Meaning
☐ Off	Process signal = 0
■ On	Process signal = 1

Channel status LEDs DIQ_n

LEDs Channel status/channel error	Meaning
☐ Off	Process value = 0
■ On	Process value = 1

PWR LED

Table 2-331 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.2.2.2 Interrupts

Interrupts

The IO-Link master CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 supports the following interrupts in single subslot mode:

- Diagnostic interrupts

In case of an interrupt, the CPU of the IO controller automatically calls interrupt OBs. Information on the cause and type of the error is available, based on the OB number and start information.

Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).

Diagnostic interrupts

The I/O device generates a diagnostic interrupt on the following events:

- Wire break
- Internal module fault
- Parameter assignment error
- Short-circuit
- Low voltage 1L+

All IO-Link events of the type Error are mapped to the diagnostic interrupts of the assigned submodule. If you have parameterized the IO-Link master accordingly, it triggers a diagnostic interrupt for an incoming or outgoing event (alarm).
The coding of the events corresponds to the PROFINET standard of the channel diagnostics (USI=0x8000).

The CPU interrupts user program execution and processes the diagnostic interrupt OB (OB 82). You can determine the error events (channel diagnostics) with the "RALRM" instruction.

5.2.2.3 Diagnostics alarms

For each diagnostic event, a diagnostic message is issued and the DIAG LED flashes red on the communications module. You can read out the diagnostic messages for example, in the diagnostic buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-332 Error types

Diagnostics alarm	Error code	Meaning (IO-Link error code)	IO-Link master	IO-Link device
Short-circuit	1_H	• Short-circuit at the process cables on the IO-Link device (1804_H)	X	
		• Short-circuit on IO device (7710_H)		X
Undervoltage	2_H	• Supply voltage too low (5111_H, 5112_H)		X
Overvoltage	3_H	• Supply voltage too high (5110_H)		X
Overtemperature	5_H	• Temperature exceeded on master (1805_H)	X	
		• Temperature exceeded on device (4000_H, 4210_H)		X
Wire break	6_H	• No IO-Link device connected • There is a break on the signal line to the IO-Link device • IO-Link device cannot communicate due to a different error (1800_H)	X	
Overflow	7_H	• Process tag range exceeded ($8C10_H$) • Measuring range exceeded ($8C20_H$)		X
Underflow	8_H	• Process tag range too low ($8C30_H$)		X
Error	9_H	• All IO-Link error codes which are not listed here are mapped to this PROFIBUS DP error		X
Parameter assignment error	10_H	• Incorrect device (1802_H) • Vendor ID and Device ID not defined (1817_H) • Process data length of the IO-Link device exceeded (1818_H) • No cycle time configured (1819_H) • IO-Link master could not be configured (1882_H, 1883_H) • Memory error (1886_H) • Process data length exceeded (1887_H) • PQI not supported (1889_H)	X	
		• Device was not configured correctly (6320_H, 6321_H, 6350_H)		X
Supply voltage missing	11_H	• 24 V encoder supply $1U_S$ (of 1L+) for device missing (1806_H) • 24 V encoder supply $1U_S$ (of 1L+) for device too low (<20 V) (1807_H) • Load voltage 2L+ (switched) missing (1888_H) • 24 V actuator supply 2 UA (of 2L+) for device missing ($180E_H$)	X	
Defective fuse	12_H	• Fuse on device is defective (5101_H)		X
Safety shutdown	19_H	• Serious error (master has to be replaced) (1880_H)	X	
External fault	$1A_H$	• Error during data backup (1809_H, $180A_H$, $180B_H$, $180C_H$, $180D_H$) • More than six errors are pending simultaneously on the IO-Link device (1808_H) • Process data length exceeded (1887_H)	X	

5.2.3 Resetting to factory settings in single subslot mode

5.2.3.1 Effects of resetting to factory settings

Use the function "Reset to factory settings" to restore the parameter assignments of your CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module made with S7-PCT to the delivery state.

After a "Reset to factory settings" in single subslot mode, the parameters of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module are assigned as follows:

- The ports are in DI mode
- The ports are mapped to the relative addresses 0.0 ... 0.7
- The PortQualifier is disabled
- The I&M data 1 ... 3 is deleted

NOTE

The device parameters are deleted and the factory state is restored.
You should reset a removed CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module to the factory settings before you place it in storage.

5.2.3.2 Procedure

To perform a "Reset to factory settings", proceed as described in the S7-PCT online help.

5.3 Multi-subslot mode

5.3.1 Parameters/address space

5.3.1.1 Parameter

The following table shows the parameters for the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module in multi-subslot mode:

Table 2-333 Diagnostics and port parameter IO-Link port

Parameter	Range of values	Default	Scope with configuration software, for example, MFCT
Diagnostics			
Diagnostics: Low voltage 1L+	• Disable • Enable	Disable	Channel
Diagnostics: No supply voltage 2L+	• Disable • Enable	Disable	Channel
Diagnostics: Port	• Disable • Enable	Disable	Channel
Port configuration			

* Only in effect when "IO-Link manual" port mode is used.

Parameter	Range of values	Default	Scope with configuration software, for example, MFCT
Port configuration without S7-PCT	• Disable • Enable	Disable	Channel
Operating mode	• IO-Link autostart • IO-Link manual	IO-Link autostart	Channel
Vendor ID*	Vendor ID of the connected IO-Link device	0	Channel
DeviceID*	Device ID of the connected IO-Link device	0	Channel
Inspection severity / data storage*	• Same type (V1.0) without Backup&Restore • Type-compatible (V1.1) without Backup&Restore • Type-compatible (V1.1) with Backup&Restore • Type-compatible (V1.1) with Restore	Type-compatible (V1.1) with Backup&Restore	Channel
Port cycle time*	-	As short as possible	Channel

* Only in effect when "IO-Link manual" port mode is used.

Table 2-334 Configurable parameters of digital input and outputs and their defaults (GSD file)

Parameters	Range of values	Default	Scope with configuration software, for example, MFCT
Diagnostics: Low voltage 1L+	• Disable • Enable	Disable	Module
Diagnostics: Short-circuit	• Disable • Enable	Disable	Module
Diagnostics: Wire break detection and alarm	• Disable • Enable	Disable	Channel (Digital inputs)
Configuration mode	• DI • DQ	DI	Channel
Reaction to CPU STOP	• Shutdown • Keep last value • Output substitute value	Shutdown	Channel (Digital outputs)
Substitute value channel 0 ... 5	• 0 • 1	0	Channel (digital outputs)

5.3.1.2 Explanation of the parameters

Diagnostics: Low voltage 1L+

Enabling of the diagnostics for insufficient supply voltage 1L+.

Diagnostics: No supply voltage 2L+

The diagnostic message is enabled for missing or insufficient supply voltage L+.

Diagnostics: Port

This parameter enables the diagnostics for the selected IO-Link port.
The diagnostics possible depends on the IO-Link device in use. Additional information about the diagnostic interrupts can be found in the description of the utilized IO-Link device.

Diagnostics: Short-circuit (only for DIQ)

Enable diagnostics:

- On short-circuit of the encoder supply to ground.
- On short-circuit of the output to ground.
- On short-circuit of the output to 1L+.

Diagnostics: Open-circuit detection and open-circuit alarm (only for DIQ)

Activates wire-break detection and enabling of diagnostics for the digital input. In the event of an interruption of the cable between the encoder and I/O device, a diagnostic message is generated.

NOTE

- This diagnostics is only available for channels configured as inputs.
- Influence on the value status:
  If the parameter is deactivated, wire break detection is switched off. A wire break does not have an effect on the value status.

Configuration mode (only for DIQ)

Specifies whether the channel operates as digital input (DI) or digital output (DQ).

Reaction to CPU STOP (only for DIQ)

With this parameter, you set the reaction of the digital outputs of the I/O device after a CPU STOP:

- Shutdown: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Port configuration without S7-PCT

This parameter releases the port configuration without S7-PCT for the module.

NOTE

Changes to the port configuration
If you have assigned the IO-Link device parameters via port configuration without S7-PCT, or have configured the port as a digital input, digital output or deactivated, you can no longer change the port configuration via S7-PCT.

Operating mode

This parameter determines the mode in which the selected port should be operated.
You can select from the following options:

- IO-Link autostart
- IO-Link manual

IO-Link autostart

The connected IO-Link device starts automatically (Plug&Play functionality). The IO-Link device is immediately ready for operation.

IO-Link manual

The connected IO-Link device is **not** started automatically.
You must store the Vendor ID and Device ID of the connected IO-Link device in STEP 7.
In addition, you can select the inspection severity for data storage:

- Same type (V1.0) without Backup&Restore
- Type-compatible (V1.1) without Backup&Restore
- Type-compatible (V1.1) with Backup&Restore
- Type-compatible (V1.1) with Restore

Port cycle time

Set the IO-Link cycle time at the corresponding port.

ET 200AL IO-Link devices configured on the IO-Link submodules

You can find the parameters for the ET 200AL IO-Link modules that can be selected as IO-Link submodules in the manual for the respective module:

- ET 200AL DI 16x24VDC 8xM12 (6ES7141-5AH00-0BL0)
- ET 200AL DI 8x24VDC 8xM8 (6ES7141-5BF00-0BL0)
- ET 200AL DQ 8x24VDC/2A 8xM12 (6ES7142-5AF00-0BL0)
- ET 200AL DIQ 16x24 V DC/0.5 A, 8x M12 (6ES7143-5AH00-0BL0),
- ET 200AL DIQ 4+DQ 4x 24 V DC/0.5 A (6ES7143-5BF00-0BL0)

See also

You can find out more about the vendor ID and the device ID of an IO-Link device on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).

5.3.1.3 Address space

The IO-Link master CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 has eight ports. Each port is represented by a submodule in multi-slot mode.

Configuration of the IO-Link ports of the IO-Link master CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12

The different operating modes of each IO-Link port are defined by configuring a corresponding submodule:

- As a digital input by configuring a digital input submodule
  - The address space is 1 byte input and the digital input value can be found in Bit 0 (without PQI).
- As a digital output by configuring a digital output submodule
  - The address space is 1 byte output and the digital output value can be found in Bit 0 (without PQI).
- as IO-Link device by configuring an IO-Link submodule,
- Port disabled:
  - In STEP 7 (TIA Portal): By deactivating the port enable.
  - with GSD: By plugging in a disabled IO-Link submodule (plugging in the submodule from the catalog, simply deleting an existing submodule is not sufficient)

The IO-Link ports are preconfigured as 2I + PQI.

When configuring IO-Link submodules, you can select the address spaces for I/O data in the following byte scales:

- ET 200AL DI 16x24VDC 8xM12
- ET 200AL DI 8x24VDC 8xM8
- ET 200AL DQ 8x24VDC/2A 8xM12
- ET 200AL DIQ 16x24 V DC/0.5 A, 8x M12
- ET 200AL DIQ 4+DQ 4x 24 V DC/0.5 A
- IO-Link 1 I/1 O + PQI
- IO-Link 2 I + PQI
- IO-Link 2 I/2 O + PQI
- IO-Link 4 I/4 O + PQI
- IO-Link 8 I/8 O + PQI
- IO-Link 16 I/16 O + PQI
- IO-Link 32 I/32 O + PQI

NOTE

Maximum data configuration

The following maximum data configurations are possible:

- 6x 32/32+PQI + 1x16/16+PQI + 1x2/2+PQI + IO-Link proxy with DIQ6+QI
- 6x 32/32+PQI + 1x16/16+PQI + 1x4/4+PQI + IO-Link proxy with DIQ6
- 6x 32/32+PQI + 1x16/16+PQI + 1x4/4+PQI + IO-Link proxy without DIQ

Port Qualifier Information (PQI)

NOTE

Port Qualifier Information (PQI)

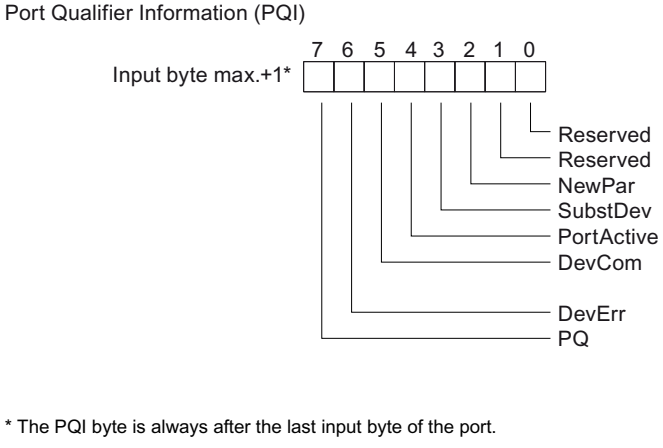
In multi-subslot mode, the PortQualifierInformation (PQI) for IO-Link submodules is always activated. This information is always transmitted with the size 1 byte together with the input data of the IO-Link device.

	Designation	Value	Meaning
Bit0	-	-	Reserved
Bit1	-	-	Reserved
Bit2	NewPar*	0	No update of the device parameters detected
		1	Device parameter update detected
Bit3	SubstDev*	0	No backup device detected (identical serial number)
		1	Backup device detected (different serial number)
Bit4	PortActive	0	Port disabled
		1	Port enabled
Bit5	DevCom	0	IO-Link device is not available
		1	IO-Link device is in the "Preoperate" or "Operate" state

* Bits are reset with function block "LIOLink_Master"

	Designation	Value	Meaning
Bit6	DevErr	0	No error
		1	An error or warning has occurred.
Bit7	PQ	0	The data of the IO-Link device is invalid
		1	The data of the IO-Link device is valid

* Bits are reset with function block "LIOLink_Master"



* The PQI byte is always after the last input byte of the port.

Figure 2-140 Structure of the PQI byte

Address space for configuration as 1 x 6-channel DIQ 6x24VDC

The device can be configured as DIQ6 or DIQ6+QI. Perform the following steps:

1. Delete the preset master proxy submodule in the GSD and configure an option from the hardware catalog.
2. Enable DIQ functionality in the HSP.

The following figure shows the address space allocation with configuration as 6-channel I/O device with digital inputs/digital outputs without value status. The addresses of the channels are derived from the start address.

Bit → / Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x	0	0							Input values at channels 0 ... 5
Assignment in the process image output (PIQ)									
QB x	0	0							Output values at channels 0 ... 5

* 0 = Value read in at channel is incorrect

Value status (Quality Information, QI)

The value status is always returned with the following configuration options:

- DIQ 6x24VDC, QI

Evaluating the value status

An additional 2 bytes are occupied in the input address space if you enable the value status for the I/O device. Bits 0 to 6 are assigned to a channel and provide information about the validity of the digital input/digital output value.

Bit = 1: No error on channel.

Bit = 0: Error on channel.

Address space for configuration as 1 x 6-channel DIQ 6x24VDC QI

The following figure shows the address space allocation with configuration as 6-channel I/O device with digital inputs/digital outputs with value status. The addresses of the channels are derived from the start address.

Bit → Byte ↓	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Description
Assignment in the process image input (PII)									
IB x	0	0							Input values at channels 0 ... 5
IB x +1	0	0							Value status (QI) for inputs at channels 0 ... 5*
IB x +2	0	0							Value status (QI) for outputs at channels 0 ... 5*
Assignment in the process image output (PIQ)									
QB x	0	0							Output values at channels 0 ... 5

* 0 = Value read in at channel is incorrect

Reference

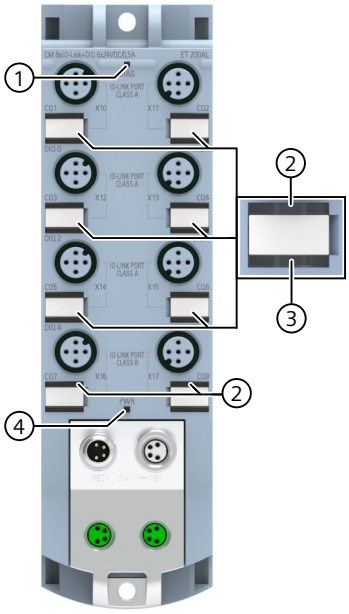
For more information, please refer to the IO-Link system (http://support.automation.siemens.com/WW/view/en/65949252) Function Manual.

5.3.2 Interrupts/diagnostic messages

5.3.2.1 Status and error displays

LED displays

The following figure shows the LED display of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module.



①	Diagnostics (DIAG)	(green/red)
②	LED displays for port status (C/Q_n)	(green)
③	LED displays for channel status (DIQ_n)	(green)
④	Load voltage 2L+ (PWR)	(green)

Figure 2-141 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostic messages can be found in the section Diagnostic messages (Page 34).

DIAG LED

Table 2-335 Error display of the DIAG LED

DIAG LED	Meaning
▫ Off	No supply voltage 1L+
☼ Flashes	• Module parameters not assigned (after switching on the supply voltage 1L+) • Loading firmware (while the firmware update is being performed, all LEDs retain their current status) • No connection to the ET-Connection and/or the fieldbus
■ On	Module parameters assigned and no module diagnostics
☼ Flashes	Module parameters assigned and module diagnostics

Channel status LEDs CQ_n

Valid for IO-Link port in IO-Link mode:

Table 2-336 Status displays of the LEDs CQ_1 to CQ_8

LED CQ_1 to CQ_8	Meaning
▫ Off	Port disabled or in SIO mode
☼ Flashes	Port in IO-Link mode, device not connected or port not connected with the configured device
■ On	Port in IO-Link mode, device not connected

Valid for IO-Link port in SIO mode:

Table 2-337 Status displays of the LEDs CQ_1 to CQ_8

LED CQ_1 to CQ_8	Meaning
▫ Off	Process signal = 0
■ On	Process signal = 1

Channel status LEDs DIQ_n

LEDs Channel status/channel error	Meaning
▫ Off	Process value = 0
■ On	Process value = 1

PWR LED

Table 2-338 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.3.2.2 Interrupts

Interrupts

The IO-Link master CM 8x IO-Link + DIQ 6x24V, 8xM12 supports the following interrupts in multi-subslot mode:

- Diagnostic interrupts
- Pull/plug interrupt (at submodule port)

In case of an interrupt, the CPU of the IO controller automatically calls interrupt OBs. Information on the cause and type of the error is available, based on the OB number and start information.

Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).

Diagnostic interrupts

The I/O device generates a diagnostic interrupt on the following events:

- Wire break
- Internal module fault
- Parameter assignment error
- Short-circuit
- Low voltage 1L+

All IO-Link events of the type Error or Warning are mapped to the diagnostic interrupts of the assigned submodule. If you have parameterized the IO-Link master accordingly, it triggers a diagnostic interrupt for an incoming or outgoing event (alarm).
The coding of the events corresponds to the PROFINET standard of the extended channel diagnostics (USI=0x8002).

The CPU interrupts user program execution and processes the diagnostic interrupt OB (OB 82). You can determine the error events (channel diagnostics) with the "RALRM" instruction.

Pull/plug interrupts

If you remove an IO-Link device or the IO-Link communication is interrupted, a pull alarm is generated by the assigned submodule.
As soon as you plug the IO-Link device back in or the IO-Link communication is re-established, a plug alarm is generated.

When an insert/remove module interrupt occurs, the CPU interrupts execution of the user program and processes the insert/remove module interrupt OB (OB 83). The event that triggered the interrupt is set in the start information of the insert/remove OB.

5.3.2.3 Diagnostic messages

For each diagnostics event, a diagnostic message is issued and the LED DIAG flashes red on the communications module. You can read out the diagnostic messages for example, in the diagnostic buffer of the CPU. You can evaluate the error codes with the user program.

The IO-Link master can generate diagnostic alarms on behalf of the IO-Link device or the IO-Link port.

- Alarms of the "Diagnostics" type indicate a malfunction of the IO-Link device / port and should be corrected immediately.

IO-Link master error types

All IO-Link events of the type Error generated by the IO-Link device or port are mapped to the PROFINET diagnostic message of the type (severity) "Diagnosis" of the assigned submodule.

IO-Link device diagnostics

The IO-Link master generates PROFINET channel diagnostics (CET, ECET) from the IO-Link events of an IO-Link device according to the following mapping regulations:

In the "IO-Link Device Diagnostics - Page 1" (CET $0x9500_H$) the IO-Link event codes in the range 0x0000 - $0x7FFF_H$ are displayed directly:
$ECET_H$ = IO-Link Event $Code_H$

In the "IO-Link Device Diagnostics - Page 2" (CET $0x9501_H$) the IO-Link event codes in the range 0x8000 - $0xFFFF_H$ are displayed directly:
$ECET_H$ = (IO-Link Event $Code_H$ – $0x8000_H$)

Table 2-339 Overview of error types IO-Link device diagnostics

IO-Link event code	Error type (CET)	Extended error type (ECET)	Error text	Meaning
0x0000 - $0x7FFF_H$	$0x9500_H$ (38144_D)	0x0000 - $0x7FFF_H$ (0 - 32767_D)	Error / warning	See the manual of the IO-Link device or IODD file used.
0x8000 - $0xFFFF_H$	$0x9501_H$ (38145_D)	0x0000 - $0x7FFF_H$ (0 - 32767_D)	Error / warning	See the manual of the IO-Link device or IODD file used.

Example of displaying the IO-Link event codes:

An IO-Link device generates event code $0x4000_H$ (type "Error").
The channel diagnostics from the event code:

- PROFINET channel diagnostics type: Diagnosis, CET: $0x9500_H$, ECET: $0x4000_H$
  Diagnostic message "IO-Link Device Diagnostics - Page 1, Temperature fault - Overload", generated from the IO-Link event code $0x4000_H$.

IO-Link port diagnostics

The IO-Link master generates channel diagnostics for each port. The port-specific channel diagnostics are shown in the port diagnostics (CET $0x9502_H$).

The following table gives you an overview of the possible diagnostic events and their meaning.

Table 2-340 Overview of error types IO-Link port diagnostics

Error type (CET)	Extended error type (ECET)	Error text	Meaning
$0x9502_H$ (38146_D)	$0x17FF_H$ (6143_D)	Process data mismatch	Check submodule configuration
	$0x1800_H$ (6144_D)	Device does not exist	Communication cancelled
	$0x1801_H$ (6145_D)	Configuration error in start-up	Check parameter assignment
	$0x1802_H$ (6146_D)	Wrong device VendorID	Check device
	$0x1803_H$ (6147_D)	Wrong device DeviceID	Check device
	$0x1804_H$ (6148_D)	Short-circuit to C/Q	Check port connection
	$0x1805_H$ (6149_D)	IO-Link PHY overtemperature	Temperature on PCB too high
	$0x1806_H$ (6150_D)	Short-circuit to L+	Check port connection
	$0x1807_H$ (6151_D)	Undervoltage 1L+	Low supply voltage 1L+
	$0x1808_H$ (6152_D)	Event overflow on the device	More events present than can currently be processed
	$0x1809_H$ (6153_D)	Backup failed	Memory outside the range 2k
	$0x180A_H$ (6154_D)	Backup invalid	Mismatch when identifying data storage
	$0x180B_H$ (6155_D)	Backup invalid	Unspecified data storage error
	$0x180C_H$ (6156_D)	Backup invalid	Upload error
	$0x180D_H$ (6157_D)	Backup invalid	Download error
	$0x6000_H$ (24576_D)	Cycle time invalid	Check cycle time
	$0x6001_H$ (24577_D)	Revision error	Incompatible protocol version
	$0x6002_H$ (24578_D)	ISDU batch failed	Parameter inconsistency

Diagnostic messages input and output module DIQ 6x24V

A diagnostic message is output for each diagnostics event. The DIAG LED flashes red on the I/O device. You can read out the diagnostic messages for example, in the diagnostic buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-341 Diagnostic messages, their meanings and corrective measures

Diagnostic message	Error code	Meaning	Corrective measures
Wire break	6_H	Fault in the external circuitry	Check the external circuitry and correct the fault.
		Encoder faulty	Replace the encoder.
		Impedance of encoder circuitry is too high	Use a different encoder type or modify the wiring. For example, use cables with a larger cross-section.
		Interruption of cable between the I/O device and sensor.	Establish the connection.
		Channel not connected (open)	• Disable diagnostics • Connect a resistor of 25 kΩ to 45 kΩ to the encoder contacts.
Parameter assignment error	10_H	• I/O device cannot evaluate parameters for the channel • Incorrect parameter assignment	Correct the parameter assignment.
Short-circuit	105_H	Short circuit to L+	• Correct the process wiring. • Replace the defective encoder/actuator.
	106_H	Short circuit to ground	

5.3.3 Resetting to factory settings in multi-subslot mode

5.3.3.1 Effects of resetting to factory settings

Use the function "Reset to factory settings" to restore the parameter assignments of your CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module made with S7-PCT to the delivery state.

After a "Reset to factory settings" in single subslot mode, the parameters of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module are assigned as follows:

- The ports are in DI mode
- The I&M data 1 ... 3 is deleted

NOTE

The device parameters are deleted and the factory state is restored.
You should reset a removed CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module to the factory settings before you place it in storage.

5.3.3.2 Procedure

To perform a "Reset to factory settings", proceed as described in the S7-PCT online help.

Technical specifications

6

Technical specifications of the communications module CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12

The following table lists the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7147-5JJ00-0BA0/td?dl=en).

Article number	6ES7147-5JJ00-0BA0
General information	
Product type designation	CM 8x IO-Link
HW functional status	FS01
Firmware version	V2.0.0
Vendor identification (VendorID)	002AH
Product function	
• I&M data	Yes; I&M0 to I&M4
Engineering with	
• STEP 7 TIA Portal configurable/integrated from version	STEP 7 V19 or higher
• STEP 7 configurable/integrated from version	STEP 7 V5.7 or higher SP1 or higher
• PROFINET from GSD version/GSD revision	GSDML V2.4.x
Operating mode	
• IO-Link	Yes
• DI	Yes
• DQ	Yes; max. 100 mA
Supply voltage	
power supply according to NEC Class 2 required	No
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; actuator power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	45 mA; without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value

Article number	6ES7147-5JJ00-0BA0
Encoder supply	
Number of outputs	8
24 V encoder supply	
• Short-circuit protection	Yes; per channel, electronic
• Output current, max.	4 A; total current of all ports, max. 2 A per channel
Power loss	
Power loss, typ.	3.6 W
Address area	
Address space per module	
• Inputs	237 byte; including 8 byte for QI information
• Outputs	237 byte
Digital inputs	
Number of digital inputs	6; Parameterizable as DIQ
Digital inputs, parameterizable	Yes
Source/sink input	P-reading
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	8
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	2.5 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– parameterizable	No
Cable length	
• unshielded, max.	30 m
Digital outputs	
Number of digital outputs	6; Parameterizable as DIQ
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	1 A
Limitation of inductive shutdown voltage to	1L+ (-53 V)
Controlling a digital input	Yes
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 Ω
Output voltage	
• for signal "1", min.	1L+ (-0.8V)

Article number	6ES7147-5JJ00-0BA0
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per module, max.	4 A
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
IO-Link	
Number of ports	8
• of which simultaneously controllable	8
IO-Link protocol 1.0	Yes
IO-Link protocol 1.1	Yes
Transmission rate	4.8 kBaud (COM1); 38.4 kBaud (COM2), 230 kBaud (COM3)
Cycle time, min.	2 ms
Size of process data, input per port	33 byte
Size of process data, input per module	237 byte
Size of process data, output per port	32 byte
Size of process data, output per module	237 byte
Memory size for device parameter	2 kbyte
Master backup	possible with LIOLink_Master function block
Configuration without S7-PCT	Possible; autostart/manual function
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type A	via 3-core cable
• Port type B	Additional device supply: max. 2 A per port, max. 4 A per module
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Monitoring the supply voltage	Yes
• Wire-break	Yes
• Short-circuit	Yes
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED

Article number	6ES7147-5JJ00-0BA0
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and backplane bus	Yes
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	No
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pin, A-coded
Design of electrical connection for supply voltage	M8, 4-pole
ET-Connection	
• ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	184 g

PROFIenergy

7

7.1 Pause function

Introduction

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and in a coordinated manner during pause times regardless of the manufacturer or device type. This has the aim that the process is only provided with the energy that is absolutely required. In so doing, the majority of the energy savings come from the process itself; the PROFINET device contributes only a few watts to the possible savings. In PROFIenergy, this operating state is referred to as a "pause".

Start and end of a pause

You enable and disable the pause function of the system at the beginning and end of pauses, respectively; the IO controller then sends the PROFIenergy command "Start_Pause" or "End_Pause" to the modules.

Use the "Start_Pause" command to start a pause.

Use the "End_Pause" command to end a pause.

The following conditions will also cause a pause to be ended:

- Reconfiguration in RUN
- CPU stop
- CPU start
- Firmware update
- Station stop
- Restart of the interface module through:
  - POWER OFF/POWER ON of an interface module
  - POWER OFF/POWER ON of an I/O module
  - Termination of ET-Connection1 or ET-Connection2

The specific behavior of the communication module is explained in the following sections.

NOTICE
Reconfiguration/factory reset in the PROFIenergy pause Reconfiguration or factory reset with S7-PCT is not permitted during a PE pause.

Additional information

You can find additional information on working with PROFIenergy in the "PROFIenergy" section of the manual IM 157-1 PN interface module (http://support.automation.siemens.com/WW/view/en/89254863) and the "Saving energy with PROFIenergy" section of function manual PROFINET with STEP 7 V13 (http://support.automation.siemens.com/WW/view/en/49948856).

Application examples (http://support.automation.siemens.com/WW/view/en/41986454) are also available on the Internet.

7.2 DI operating mode

Display

If no external supply voltage is connected, switching off supply voltages $1U_S$ and $2U_A$ also leads to switching off the associated channel status LED Qn.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Load voltage 2L+" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-342 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: Configured pause substitute value • Value status "BAD"

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off during the pause, all supply voltages are switched off if no channel is assigned in PE_MODE_PROCEED.

7.3 DQ operating mode

Display

The channel status LEDs Qn show the output value.

Response to error detection

All channels that are in pause mode on "PE_MODE_PROCEED" report their diagnostic status as in productive mode.

The following applies for all channels which switch to a different pause mode:

- During the "pause", error detection of "Load voltage 2L+ missing" is not possible:
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-343 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off • Pause substitute value: 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last output value is maintained • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Pause substitute value: Configured pause substitute value is output • Value status "BAD"

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off in the pause, the supply voltages are switched off.

7.4 IO-Link operating mode

Display

Switching off the supply voltage $1U_S$ also switches off the associated port status LED Cn.

Response to error detection

All channels which are set to "PE_MODE_PROCEED" and "PE_MODE_LAST_VALUE" in pause mode report errors as in productive operation.

The following conditions apply to all channels (ports) which switch to a different pause mode ("PE_MODE_SHUTDOWN" and "PE_MODE_SUBST_VALUE"):

- Switching off the supply voltage U_{Sn} (port) upon starting the "pause" does not lead to generation of the alarms "Wire break" and "Short circuit".
- Error detection is not possible during the "pause" (no IO-Link device communication):
  - Alarms for errors already pending before the "pause" are retained.
  - After the "pause" is over, the error status is updated and incoming/outgoing errors are reported correspondingly.

Mode parameter

The following table shows the "Mode" parameter.

Table 2-344 Mode parameter

Element	Code	Explanation
Mode	0_D: PE_MODE_PROCEED	Proceed at "pause" • Value status "GOOD"
	1_D: PE_MODE_SHUTDOWN	Switch off at "pause" • Supply voltages $1U_S$ and $2U_A$ off[1] • Pause substitute value (input): 0_B • Value status "BAD"
	3_D: PE_MODE_LAST_VALUE	Last value at "pause" • Pause substitute value: Last input value • Value status "BAD"
	4_D: PE_MODE_SUBST_VALUE	Substitute value at "pause" • Supply voltages $1U_S$ and $2U_A$ off[1] • Pause substitute value (input): 0_B • Value status "BAD"

[1] Supply voltage $1U_S$ of the assigned port is switched off. Result: The IO-Link device is no longer supplied with voltage.

NOTE

Supply voltages $1U_S$ and $2U_A$

Supply voltages $1U_S$ and $2U_A$ can only be switched off separately for each module.
If all channels require switching off in the pause, the supply voltages are switched off.

Dimension drawing

The following figure shows the dimension drawing of the CM 8xIO-Link+DIQ 6x24VDC/0.5A 8xM12 communications module in front and side view.

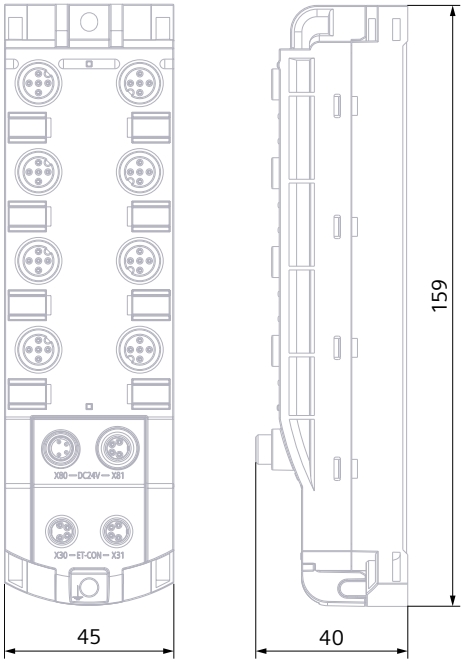


Figure 2-142 Dimension drawing

SIEMENS

SIMATIC

ET 200AL
IO-Link digital input module DI 8x24VDC 8xM8
(6ES7141-5BF00-0BL0)

Equipment Manual

ET 200AL IO-Link I/O modules Documentation Guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Interrupts/diagnostics alarms 5

Technical specifications 6

Dimension drawing A

08/2021
A5E47926568-AB

Preface

Preface IO-Link module AL

Purpose of the documentation

This manual supplements the system manual ET 200AL IO-Link (https://support.automation.siemens.com/WW/view/en/109773203). Functions that generally relate to the distributed I/O system ET 200AL IO-Link I/O modules are described there.

The information provided in this manual and in the system manual and function manuals supports you in commissioning the ET 200AL IO-Link I/O modules.

Changes compared to the previous version

This manual contains the following changes compared to the previous version:

- Supplements in the section Parameters (Page 13).

Conventions

Also observe notes labeled as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 ET 200AL IO-Link I/O modules Documentation Guide 5

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

3 Wiring 11

3.1 Terminal and block diagram 11

3.2 Pin assignment 12

4 Parameters/address space 13

4.1 Parameters 13

4.2 Explanation of the parameters 13

4.3 Address space 13

4.4 IODD parameters 14

5 Interrupts/diagnostics alarms 15

5.1 Status and error displays 15

5.2 Interrupts 16

5.3 Diagnostics alarms 17

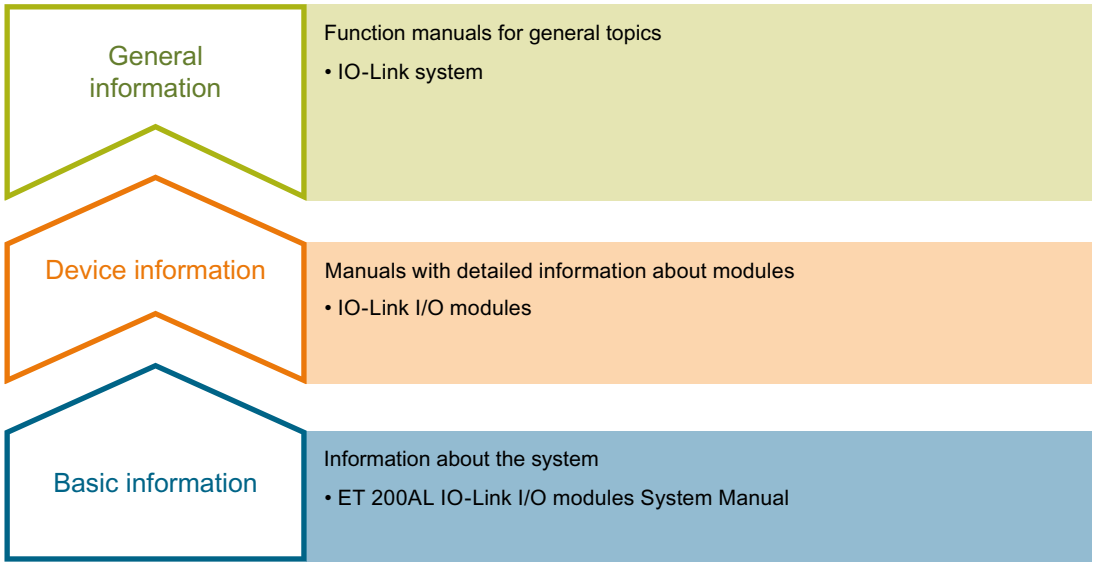
6 Technical specifications 18

A Dimension drawing 21

ET 200AL IO-Link I/O modules Documentation Guide

1

The documentation for the SIMATIC ET 200AL IO-Link I/O modules is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The system manual describes in detail the configuration, installation, wiring and commissioning of the distributed I/O system SIMATIC ET 200AL IO-Link I/O modules.

Device information
Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC IO-Link system.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

ET 200AL Manual Collection

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area of "mySupport", you can access the latest product data for your CAx or CAe system.

You configure your own download package with a few clicks.

You can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" CAx data on the Internet (https://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/ae).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109767888).

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning. PRONETA has two core functions:

- The topology overview automatically scans the PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SIMATIC S7-PCT

The Port Configuration Tool ("PCT") is PC-based software for the parameter assignment of Siemens IO-Link master-modules and IO-Link devices from any manufacturer.

The IO-Link devices are integrated using the standardized device description "IODD" that is available from the respective device manufacturer. S7-PCT supports the version 1.0 as well as V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link masters from STEP 7; however, it can also be started as "standalone" if the IO-Link master is not operated on a SIMATIC controller or when STEP 7 is not used.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Product overview

2

2.1 Properties

Article number

6ES7141-5BF00-0BL0

View of the module

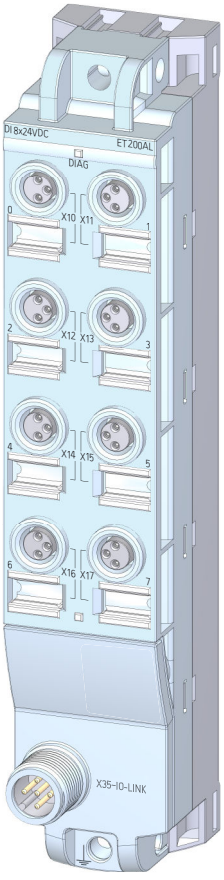


Figure 2-143 View of the DI 8x24VDC 8xM8 IO-Link digital input module

Properties

The module has the following technical properties:

- 8 digital inputs
- M8 sockets for connection of sensors
- 24 V DC supply voltage
- Configurable diagnostics can be set for each module
- Typical input delay of 3 ms
- Suitable for switches and proximity switches
- Dimensions 30 x 159 mm

Interface for IO-Link and power supply:

- M12 connector A-coded
- IO-Link Port Class A (Type A)
- Supply of module electronics and sensor supply

The module supports the following functions:

- Firmware update
- IO-Link profile: General profile

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

- Connectors
- Cables
- M8 sealing cap

See also

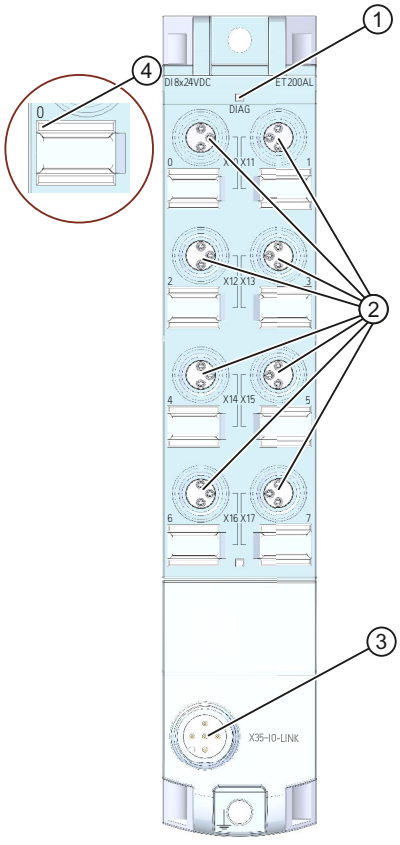
You can find more information on accessories in the system manual IO-Link IO modules Hotspot text ET 200AL distributed I/O system in the section Accessories/spare parts.

See also

ET 200AL system manual (https://support.automation.siemens.com/WW/view/en/109773203)

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DI 8x24VDC 8xM8 IO-Link digital input module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input signal
③ X35: IO-Link interface
④ LED displays 0 to 7 for the channel status

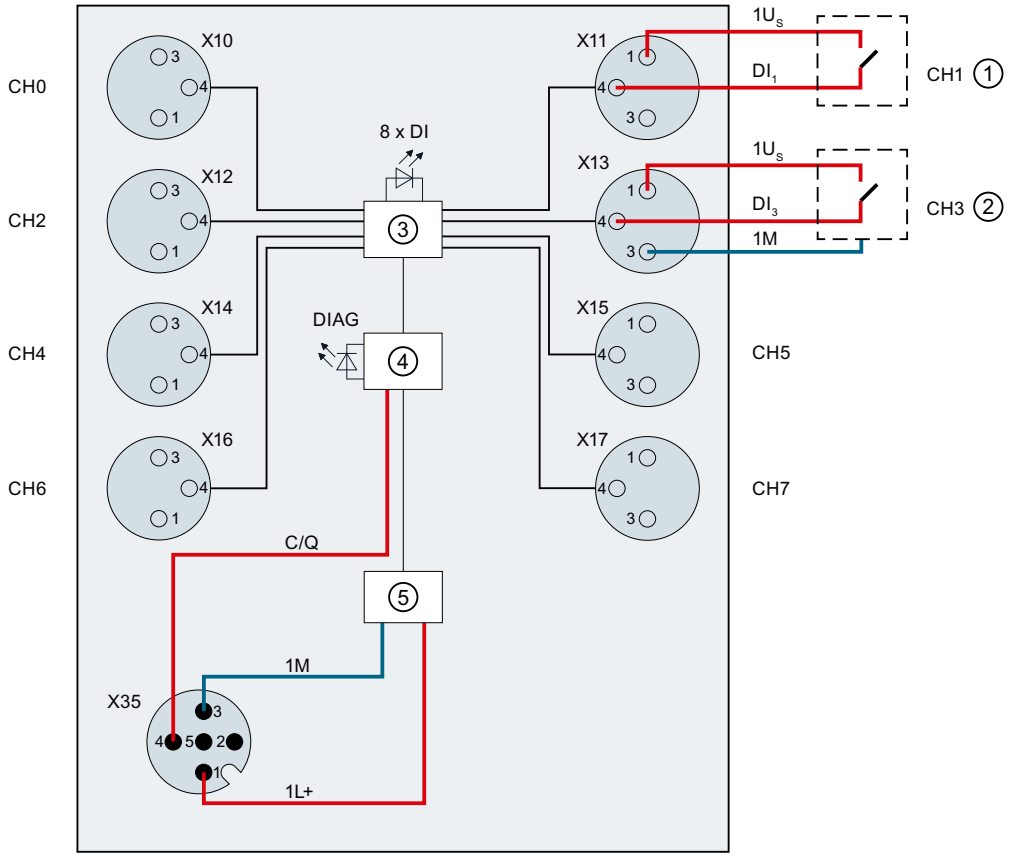
Figure 2-144 Operator controls and display elements

Wiring

3

3.1 Terminal and block diagram

The following figure shows an example of the pin assignment of signal outputs with 2- and 3-wire connection.



①	2-wire connection	1L+	Supply voltage 1L+ (non-switched)
②	3-wire connection	1M	Ground 1M (non-switched)
③	DI circuit	1U$_S$	24 V encoder supply
④	Microcontroller	DIn	Input signal
⑤	Internal supply voltage	DI	Channel status LEDs (0 to 7) (green)
X10 to X17	Channels 0 to 7	DIAG	LED diagnostic status (red/green)
X35	IO-Link interface		

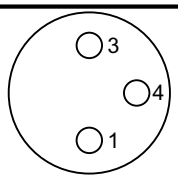
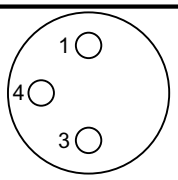
Figure 2-145 Terminal and block diagram

3.2 Pin assignment

Pin assignment of the sockets for digital inputs

The table below shows the pin assignment of the 8 sockets for the connection of digital inputs.

Table 2-345 Pin assignment for digital inputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 sockets for digital inputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
3	Encoder supply ground 1M		
4	Input signal DI_0: X10 Input signal DI_1: X11 Input signal DI_2: X12 Input signal DI_3: X13 Input signal DI_4: X14 Input signal DI_5: X15 Input signal DI_6: X16 Input signal DI_7: X17		

NOTICE

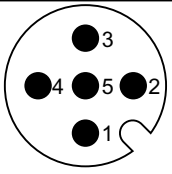
24 V encoder supply $1U_S$

Use only the 24 V encoder supply $1U_S$ provided by the digital input module to supply power to the encoder.

Pin assignment of the IO-Link connector

The following table shows the pin assignment of the connector for the IO-Link connection. The IO-Link interface corresponds to the specification according to port Class A.

Table 2-346 Pin assignment of the IO-Link interface

Pin	Assignment	Front view of the connector (Port Class A)
	X35	
1	1L+	
2	Unassigned	
3	Ground 1M	
4	Switching and communication cable (C/Q)	
5	Unassigned	

NOTE

Note that the module can only be supplied with a protective low voltage according to the standard SELV/PELV.

Parameters/address space

4

4.1 Parameters

The following table shows the parameters for the DI 8x24VDC 8xM8 IO-Link digital input module.

Table 2-347 Parameters

Parameters	Value range			Default	Scope	ISDU index (decimal)	ISDU subindex (decimal)
	Value	Dec.	Hex.				
Diagnostics: Short-circuit to ground	Disable	0	0	Disable	Module	131	1
	Enable	255	FF				

4.2 Explanation of the parameters

Diagnostics: Short-circuit to ground

Enabling of the diagnostics if a short-circuit of the encoder supply to ground occurs.

4.3 Address space

The figure below shows the assignment of the address space for the DI 8x24VDC 8xM8 IO-Link digital input module.

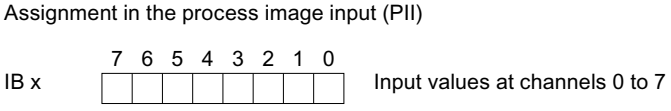


Figure 2-146 Address space IO-Link DI 8x24VDC 8xM8

4.4 IODD parameters

Device description IODD

An electronic device description is available for the DI 8x24VDC 8xM8 IO-Link digital input module, the IODD file (IO Device Description). The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the identical manner by the IO-Link Configuration Tool of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODDfinder is available on the Internet (https://ioddfinder.io-link.com).

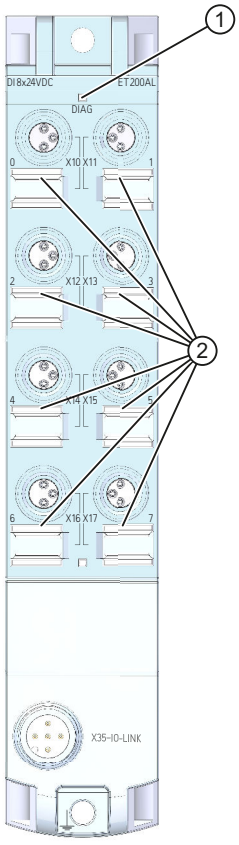
Interrupts/diagnostics alarms

5

5.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DI 8x24VDC 8xM8 IO-Link digital input module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 7) (green)

Figure 2-147 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 17).

DIAG LED

Table 2-348 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• No data exchange with the IO-Link Master, for example, due to wire break • Firmware is loading
On	Module is currently exchanging data with the IO-Link master and no module diagnostics
Flashes	Module is currently exchanging data with the IO-Link master and module diagnostics

LED channel status

Table 2-349 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

5.2 Interrupts

The DI 8x24VDC 8xM8 IO-Link digital input module supports diagnostic interrupts.

Diagnostic interrupt

The IO-Link digital input module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground

5.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input module. You can read out the diagnostics alarms, for example, in the diagnostics buffer of the CPU. You can evaluate the error codes with the user program.

Table 2-350 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Remedy
Short-circuit	0x7710	Short-circuit of an encoder supply to ground	• Eliminate the short-circuit

NOTE

Short-circuit at the sensor supply
A short-circuit at the sensor supply can cause wire break diagnostics of the IO-Link Master. The behavior depends on the technical specifications of the IO-Link Master used.

Technical specifications

6

Technical specifications of the DI 8x24VDC 8xM8 IO-Link digital input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/de/en/pv/6ES7141-5BF00-0BL0/td?dl=de).

Article number	6ES7141-5BF00-0BL0
General information	
Product type designation	DI 8x24VDC
HW functional status	FS01
Firmware version	V1.0.x
Vendor identification (VendorID)	42
Device identifier (DeviceID)	229379
Engineering with	
• IODD file	Yes
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V; Supply from 1Us+ of the IO-Link master
• permissible range, lower limit (DC)	18 V
• permissible range, upper limit (DC)	30 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	15 mA; without load
Encoder supply	
Number of outputs	8; Supply from 1Us+ of the IO-Link master
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders (depending on IO-Link master supply via 1Us+)
Power loss	
Power loss, typ.	1.5 W
Digital inputs	
Number of digital inputs	8
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	8
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-30 to +5 V

Article number	6ES7141-5BF00-0BL0
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
IO-Link	
IO-Link protocol 1.1	Yes
Transmission rate	38.4 kBd (COM2)
Cycle time, min.	2.1 ms
Size of process data, input per module	1 byte
Size of process data, output per module	0 byte
Supported IO-Link profiles	common profile
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type A	Yes
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Sensor supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
Potential separation channels	
• between the channels	No
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67

Article number	6ES7141-5BF00-0BL0
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	124 g

Dimension drawing

A

The figure below shows the dimension drawing of the DI 8x24VDC 8xM8 IO-Link digital input module in front and side view.

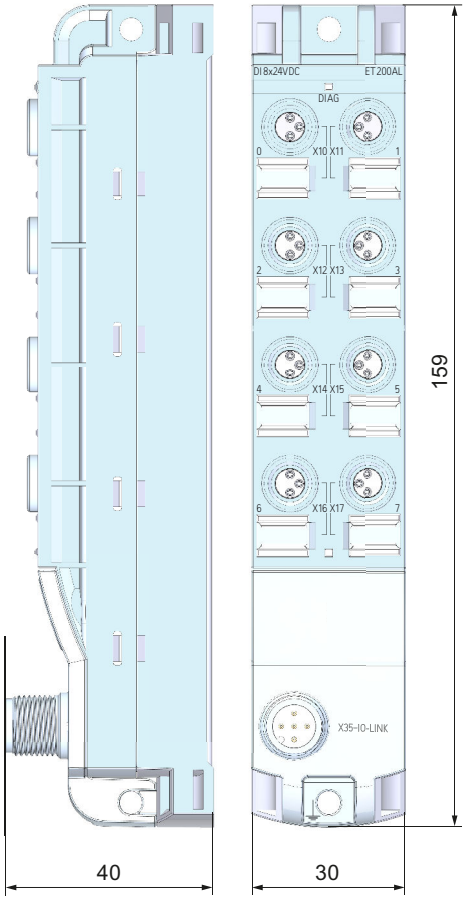


Figure 2-148 Dimension drawing

SIEMENS

SIMATIC

ET 200AL
IO-Link digital input module DI 16x24VDC 8xM12
(6ES7141-5AH00-0BL0)

Equipment Manual

ET 200AL IO-Link I/O modules Documentation Guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Interrupts/diagnostic alarms 5

Technical specifications 6

Dimension drawing A

08/2021
A5E47926661-AB

Preface

Preface IO-Link module AL

Purpose of the documentation

This manual supplements the system manual ET 200AL IO-Link (https://support.automation.siemens.com/WW/view/en/109773203). Functions that generally relate to the distributed I/O system ET 200AL IO-Link I/O modules are described in this manual.

The information provided in this manual and in the system manual and function manuals supports you in commissioning the ET 200AL IO-Link I/O modules.

Changes compared to the previous version

This manual contains the following changes compared to the previous version:

- Supplements in the section Parameters (Page 14)

Conventions

Also observe notes labeled as follows:

NOTE
Indicates important product information to which particular attention should be paid.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 ET 200AL IO-Link I/O modules Documentation Guide 5

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

3 Wiring 11

3.1 Terminal and block diagram 11

3.2 Pin assignment 12

4 Parameters/address space 14

4.1 Parameters 14

4.2 Explanation of the parameters 14

4.3 Address space 14

4.4 IODD parameters 15

5 Interrupts/diagnostic alarms 16

5.1 Status and error displays 16

5.2 Interrupts 17

5.3 Diagnostics alarms 18

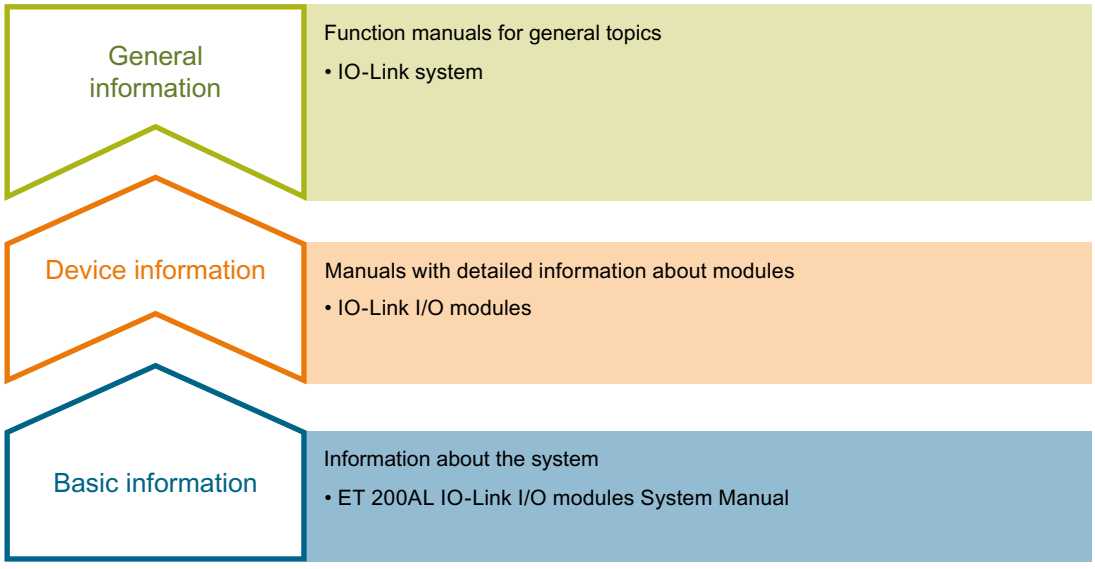
6 Technical specifications 19

A Dimension drawing 22

ET 200AL IO-Link I/O modules Documentation Guide

1

The documentation for the SIMATIC ET 200AL IO-Link I/O modules is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The system manual describes in detail the configuration, installation, wiring and commissioning of the distributed I/O system SIMATIC ET 200AL IO-Link I/O modules.

Device information
Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC IO-Link system.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

ET 200AL Manual Collection

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area of "mySupport", you can access the latest product data for your CAx or CAe system.

You configure your own download package with a few clicks.

You can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" CAx data on the Internet (https://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/ae).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109767888).

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning. PRONETA has two core functions:

- The topology overview automatically scans the PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SIMATIC S7-PCT

The Port Configuration Tool ("PCT") is PC-based software for the parameter assignment of Siemens IO-Link master-modules and IO-Link devices from any manufacturer.

The IO-Link devices are integrated using the standardized device description "IODD" that is available from the respective device manufacturer. S7-PCT supports the version 1.0 as well as V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link masters from STEP 7; however, it can also be started as "standalone" if the IO-Link master is not operated on a SIMATIC controller or when STEP 7 is not used.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Product overview

2

2.1 Properties

Article number

6ES7141-5AH00-0BL0

View of the module

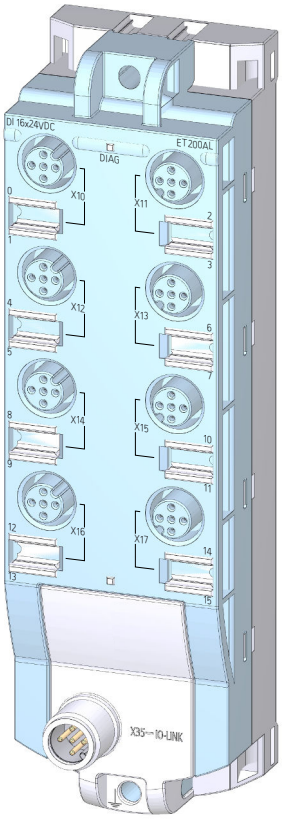


Figure 2-149 View of the DI 16x24VDC 8xM12 IO-Link digital input module

Properties

The module has the following technical properties:

- 16 digital inputs
- M12 sockets for connection of sensors
- 24 V DC supply voltage
- Configurable diagnostics can be set for each module
- Typical input delay of 3 ms
- Suitable for switches and proximity switches
- Dimensions 45 x 159 mm

Interface for IO-Link and power supply:

- M12 connector A-coded
- IO-Link Port Class A
- Supply of the module electronics
- Encoder supply

The module supports the following functions:

- Firmware update
- IO-Link profile: General profile

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

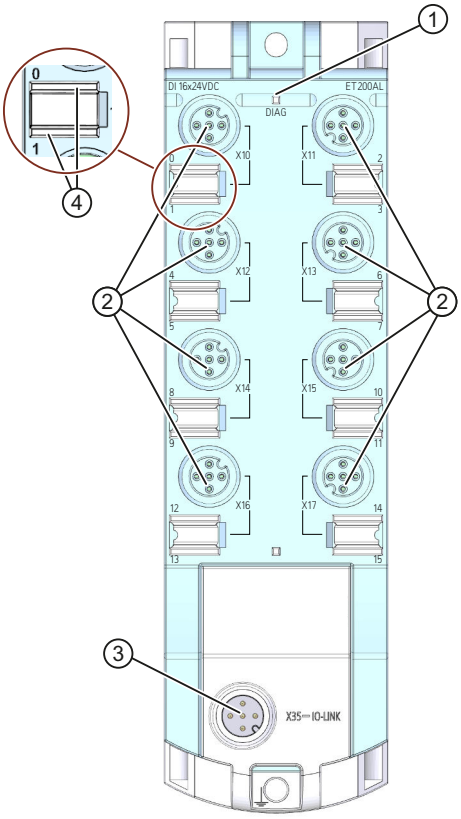
- Connectors
- Cables
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.automation.siemens.com/WW/view/en/109773203) IO-Link I/O modules system manual.

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DI 16x24VDC 8xM12 IO-Link digital input module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input signal
③ X35: IO-Link interface
④ LED displays 0 to 15 for the channel status

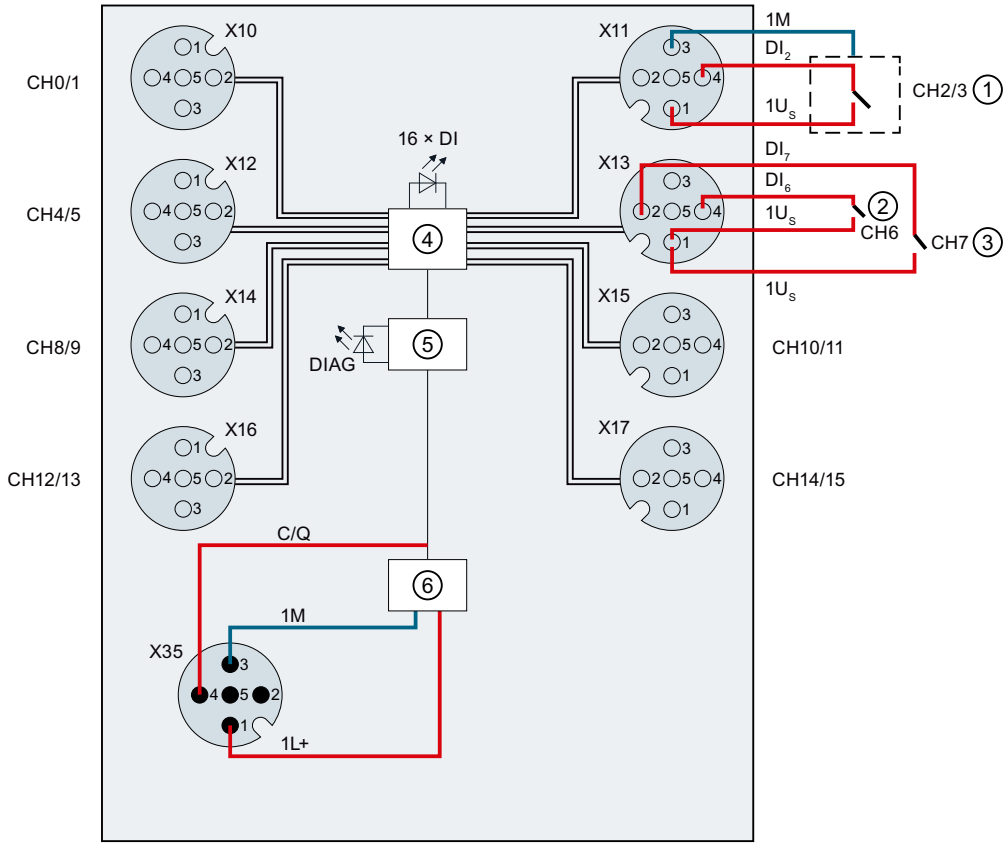
Figure 2-150 Operator controls and display elements

Wiring

3

3.1 Terminal and block diagram

The figure below shows an example of the pin assignment of signal inputs with 2-wire and 3-wire connection.



①	3-wire connection	1L+	Supply voltage 1L+ (non-switched)
②	2-wire connection	1M	Ground 1M (non-switched)
③	2-wire connection	$1U_S$	24 V encoder supply
④	DI circuit	DI_n	Input signal
⑤	Microcontroller	DI	Channel status LEDs (0 to 15) (green)
⑥	Internal supply voltage	DIAG	Diagnostic status LED (red/green)
X10 to X17	Channels 0 to 7		
X35	IO-Link interface		

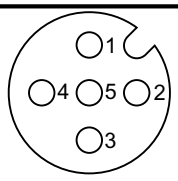
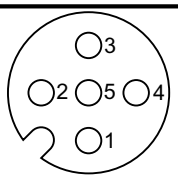
Figure 2-151 Terminal and block diagram

3.2 Pin assignment

Pin assignment of the sockets for digital inputs

The table below shows the pin assignment of the 8 sockets for the connection of digital inputs.

Table 2-351 Pin assignment for digital inputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 sockets for digital inputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	24 V encoder supply $1U_S$ (derived from 1L+ non-switched)		
2	Input signal DI_1: Connector X10 Input signal DI_3: Connector X11 Input signal DI_5: Connector X12 Input signal DI_7: Connector X13 Input signal DI_9: Connector X14 Input signal DI_{11}: Connector X15 Input signal DI_{13}: Connector X16 Input signal DI_{15}: Connector X17		
3	Encoder supply ground 1M		
4	Input signal DI_0: Connector X10 Input signal DI_2: Connector X11 Input signal DI_4: Connector X12 Input signal DI_6: Connector X13 Input signal DI_8: Connector X14 Input signal DI_{10}: Connector X15 Input signal DI_{12}: Connector X16 Input signal DI_{14}: Connector X17		
5	Functional earth FE		

NOTICE

24 V encoder supply $1U_S$

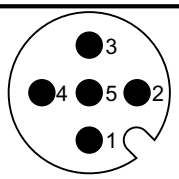
Use only the 24 V encoder supply $1U_S$ provided by the digital input module to supply power to the encoder.

Pin assignment of the IO-Link connector

The following table shows the pin assignment of the connector for the IO-Link connection. The IO-Link interface corresponds to the specification according to Port Class A.

Table 2-352 Pin assignment of the IO-Link interface

Pin	Assignment	Front view of the connector (Port Class A)
	X35	
1	1L+	
2	Unassigned	

Pin	Assignment	Front view of the connector (Port Class A)
	X35	
3	Ground 1M	
4	Switching and communication cable (C/Q)	
5	Unassigned	

NOTE

Note that the module can only be supplied with a protective low voltage according to the standard SELV/PELV.

Parameters/address space

4

4.1 Parameters

The following table shows the parameters for the DI 16x24VDC 8xM12 IO-Link digital input module.

Table 2-353 Parameters

Parameters	Value range			Default	Scope	ISDU index (hexa-decimal)	ISDU subindex (hexa-decimal)
	Value	Dec.	Hex.				
Diagnostics: Short-circuit to ground	Disable	0	0	Disable	Module	131	1
	Enable	255	FF				

4.2 Explanation of the parameters

Diagnostics: Short-circuit to ground

Enabling of the diagnostics if a short-circuit of the encoder supply to ground occurs.

4.3 Address space

The figure below shows the assignment of the address space for the DI 16x24VDC 8xM12 IO-Link digital input module.

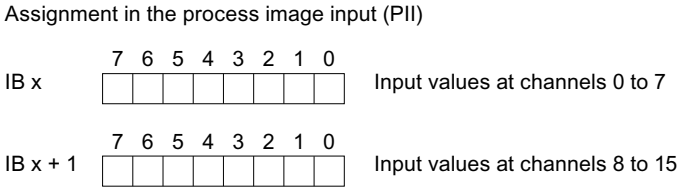


Figure 2-152 Address space IO-Link DI 16x24VDC 8xM12

4.4 IODD parameters

Device description IODD

An electronic device description is available for the DI 16x24VDC 8xM12 IO-Link digital input module, the IODD file (IO Device Description). The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the same manner by the IO-Link Configuration Tool of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODDfinder is available on the Internet (https://ioddfinder.io-link.com).

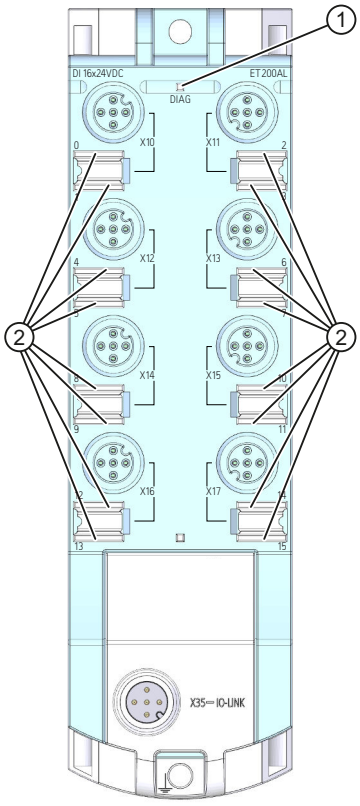
Interrupts/diagnostic alarms

5

5.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DI 16x24VDC 8xM12 IO-Link digital input module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 15) (green)

Figure 2-153 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in section Diagnostics alarms (Page 18).

DIAG LED

Table 2-354 Error display of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes	• No data exchange with the IO-Link master (e.g. wire break) • Firmware is loading
On	Module is currently exchanging data with the IO-Link master and no module diagnostics
Flashes	Module is currently exchanging data with the IO-Link master and module diagnostics

LED channel status

Table 2-355 LED channel status display

LED channel status	Meaning
Off	Process signal = 0
On	Process signal = 1

5.2 Interrupts

The DI 16x24VDC 8xM12 IO-Link digital input module supports diagnostic interrupts.

Diagnostic interrupt

The digital input module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground

5.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the LED DIAG flashes red on the digital input module. You can read out the diagnostics alarms, for example, from the status of the IO-Link master. You can evaluate the error codes with the user program.

Table 2-356 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Remedy
Short-circuit	0x7710	Short-circuit of an encoder supply to ground	Eliminate the short-circuit

NOTE

Short-circuit at the sensor supply

A short-circuit at the sensor supply can cause wire break diagnostics of the IO-Link Master. The behavior depends on the technical specifications of the IO-Link Master used.

Technical specifications

6

Technical specifications of the DI 16x24VDC 8xM12 IO-Link digital input module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/de/en/pv/6ES7141-5AH00-0BL0/td?dl=en).

Article number	6ES7141-5AH00-0BL0
General information	
Product type designation	DI 16x24VDC
HW functional status	FS01
Firmware version	V1.0.x
Vendor identification (VendorID)	42
Device identifier (DeviceID)	229380
Engineering with	
• IODD file	Yes
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V; Supply from 1Us+ of the IO-Link master
• permissible range, lower limit (DC)	18 V
• permissible range, upper limit (DC)	30 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity
Input current	
Current consumption (rated value)	20 mA; without load
Encoder supply	
Number of outputs	8; Supply from 1Us+ of the IO-Link master
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders (depending on IO-Link master supply via 1Us+)
Power loss	
Power loss, typ.	2.4 W
Digital inputs	
Number of digital inputs	16
Input characteristic curve in accordance with IEC 61131, type 3	Yes
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	16
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-30 to +5 V

Article number	6ES7141-5AH00-0BL0
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
IO-Link	
IO-Link protocol 1.1	Yes
Transmission rate	38.4 kBd (COM2)
Cycle time, min.	2.5 ms
Size of process data, input per module	2 byte
Size of process data, output per module	0 byte
Supported IO-Link profiles	common profile
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type A	Yes
Interrupts/diagnostics/status information	
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Sensor supply to M; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
Potential separation	
Potential separation channels	
• between the channels	No
• between the channels and the power supply of the electronics	No
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67

Article number	**6ES7141-5AH00-0BL0**
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	155 g

Dimension drawing

A

The figure below shows the dimension drawing of the DI 16x24VDC 8xM12 IO-Link digital input module in front and side view.

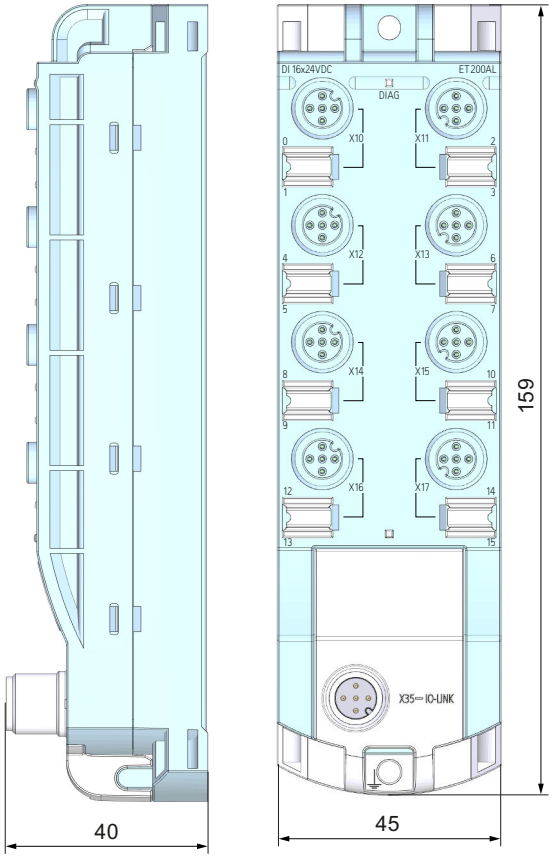


Figure 2-154 Dimension drawing

SIEMENS

SIMATIC

ET 200AL IO-Link digital output module DQ 8x24VDC/2A 8xM12 (6ES7142-5AF00-0BL0)

Equipment Manual

ET 200AL IO-Link I/O modules Documentation Guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Interrupts/diagnostic alarms 5

Technical specifications 6

Dimension drawing A

08/2021
A5E47926730-AB

Preface

Preface IO-Link module AL

Purpose of the documentation

This manual supplements the system manual ET 200AL IO-Link (https://support.automation.siemens.com/WW/view/en/109773203). Functions that generally relate to the distributed I/O system ET 200AL IO-Link I/O modules are described there.

The information provided in this manual and in the system manual and function manuals supports you in commissioning the ET 200AL IO-Link I/O modules.

Changes compared to the previous version

This manual contains the following changes compared to the previous version:

- Supplements in the section Parameters (Page 14).
- Update of the section Technical specifications (Page 19)

Conventions

Also observe notes labeled as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 ET 200AL IO-Link I/O modules Documentation Guide 5

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

3 Wiring 11

3.1 Terminal and block diagram 11

3.2 Pin assignment 12

4 Parameters/address space 14

4.1 Parameters 14

4.2 Explanation of the parameters 14

4.3 Address space 15

4.4 IODD parameters 15

5 Interrupts/diagnostic alarms 16

5.1 Status and error displays 16

5.2 Interrupts 17

5.3 Diagnostics alarms 18

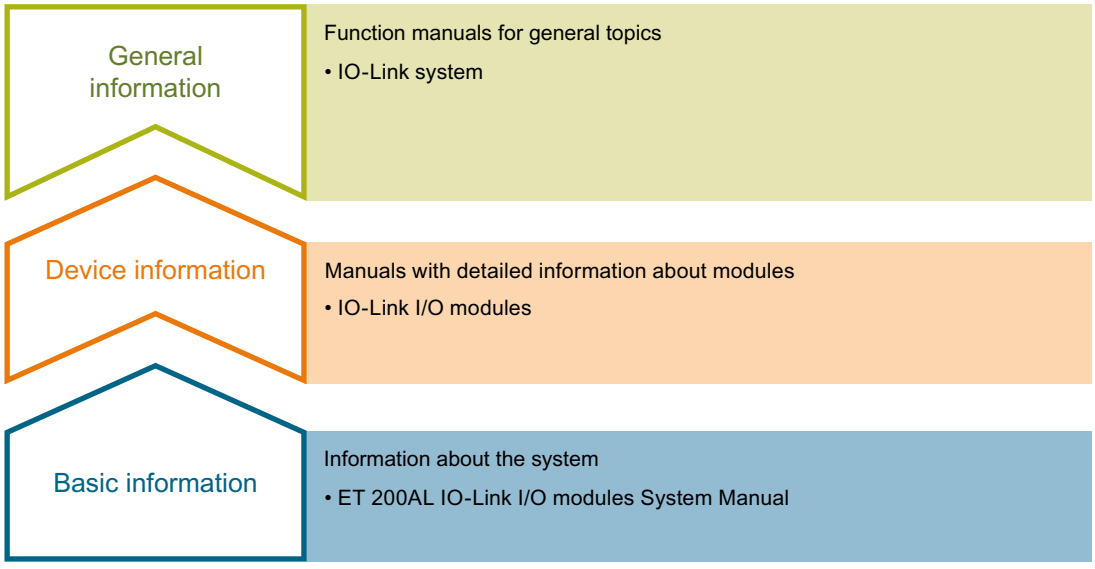
6 Technical specifications 19

A Dimension drawing 22

ET 200AL IO-Link I/O modules Documentation Guide

1

The documentation for the SIMATIC ET 200AL IO-Link I/O modules is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The system manual describes in detail the configuration, installation, wiring and commissioning of the distributed I/O system SIMATIC ET 200AL IO-Link I/O modules.

Device information
Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC IO-Link system.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

ET 200AL Manual Collection

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area of "mySupport", you can access the latest product data for your CAx or CAe system.

You configure your own download package with a few clicks.

You can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" CAx data on the Internet (https://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/ae).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109767888).

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning. PRONETA has two core functions:

- The topology overview automatically scans the PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SIMATIC S7-PCT

The Port Configuration Tool ("PCT") is PC-based software for the parameter assignment of Siemens IO-Link master-modules and IO-Link devices from any manufacturer.

The IO-Link devices are integrated using the standardized device description "IODD" that is available from the respective device manufacturer. S7-PCT supports the version 1.0 as well as V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link masters from STEP 7; however, it can also be started as "standalone" if the IO-Link master is not operated on a SIMATIC controller or when STEP 7 is not used.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Product overview

2

2.1 Properties

Article number

6ES7142-5AF00-0BL0

View of the module

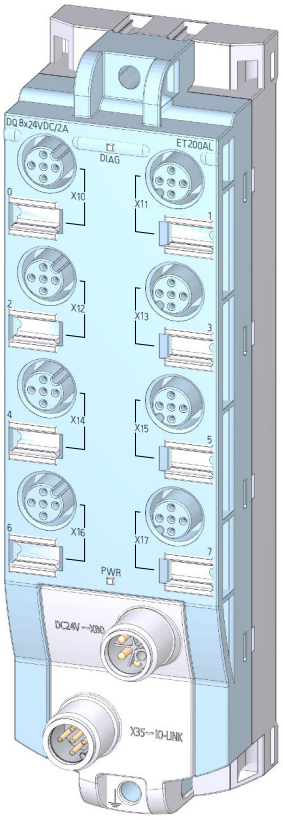


Figure 2-155 View of the DQ 8x24VDC/2A 8xM12 IO-Link digital output module

Properties

The module has the following technical properties:

- 8 digital outputs
  - Channels 0 to 7 connected to 2L+ (switched)
- M12 sockets for connection of actuators

- Rated load voltage 24 V DC
- Suitable for solenoid valves, DC contactors, and indicator lights
- Output current per output 2 A
- Configurable diagnostics can be set for each module
- Dimensions 45 x 159 mm
- Interface for supply 2L+

Interface for IO-Link and power supply:

- M12 connector A-coded
- IO-Link Port Class A
- Supply of module electronics

Load voltage supply of output

- M12 connector L-coded

The module supports the following functions:

- Firmware update
- IO-Link profile: General profile

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

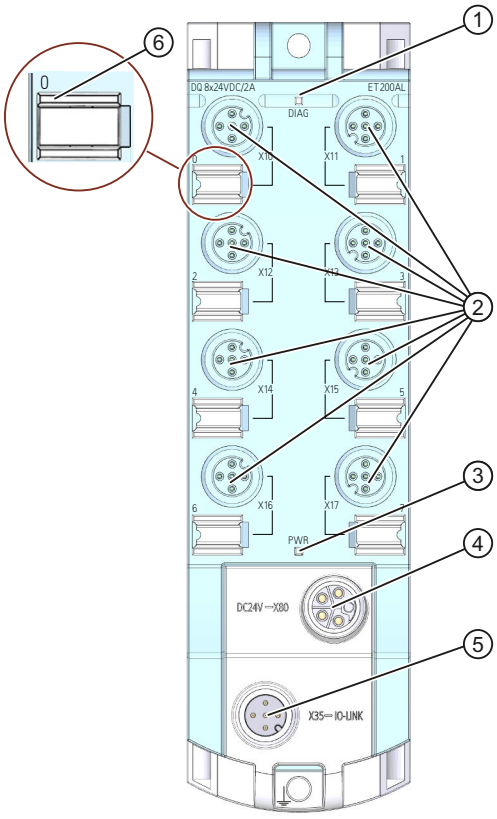
- Connectors
- Cables
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.automation.siemens.com/WW/view/en/109773203) IO-Link I/O modules system manual.

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the IO-Link DQ 8x24VDC/2A 8xM12 digital output module.

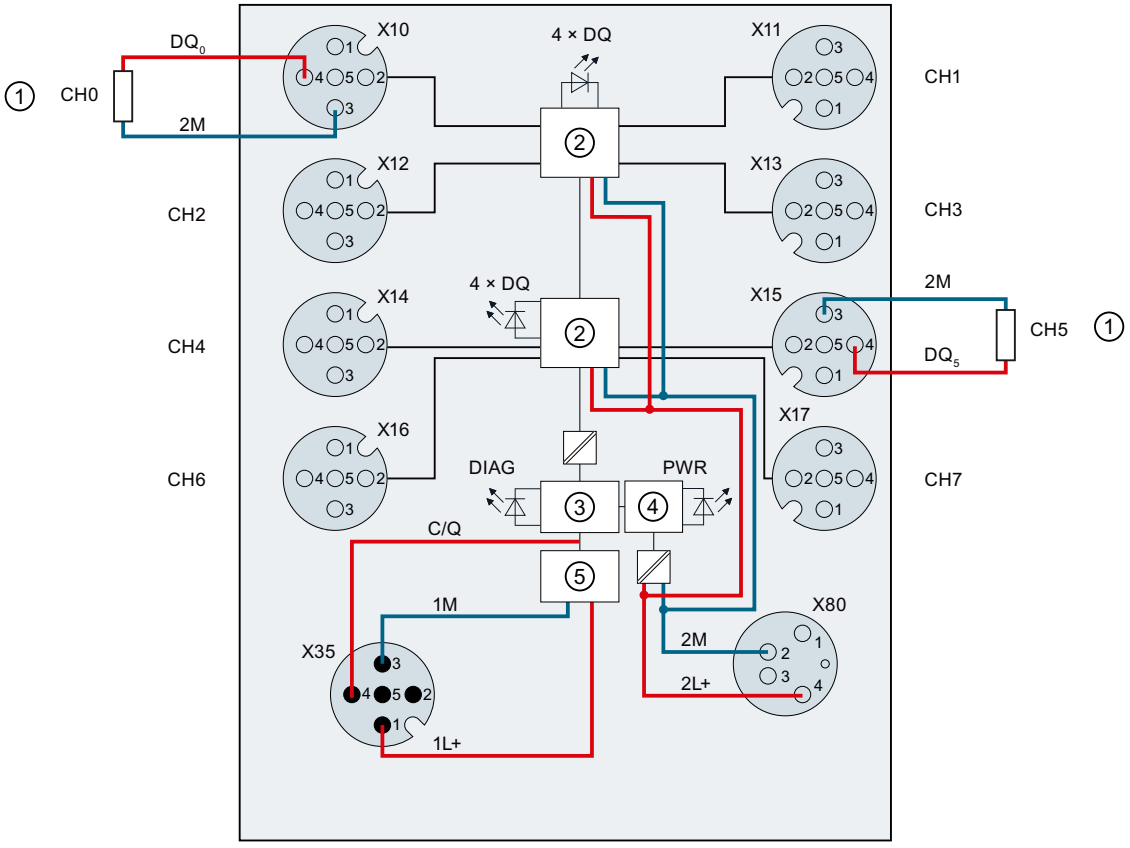


① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the output signal
③ PWR: LED display for load voltage 2L+
④ X80: Connector for infeed of the supply voltage (POWER input)
⑤ X35: IO-Link interface
⑥ LED displays 0 to 7 for the channel status

Figure 2-156 Operator controls and display elements

3.1 Terminal and block diagram

The example in the figure below shows the pin assignment of signal outputs.



①	Output to 2L+	1L+	Supply voltage 1L+ (non-switched)
②	DQ circuit	1M	Ground 1M (non-switched)
③	Microcontroller	2L+	Load voltage 2L+ (switched)
④	Monitoring	2M	Ground 2M (switched)
⑤	Internal supply voltage	DQ_n	Output signal
X10 to X17	Channels 0 to 7	DQ	Channel status LEDs (0 to 7) (green)
X35	IO-Link interface	DIAG	Diagnostic status LED (red/green)
X80	Connector for infeed of supply voltage 2L+	PWR	Supply voltage LED 2L+ (green)

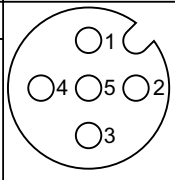
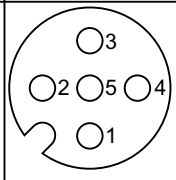
Figure 2-157 Terminal and block diagram

3.2 Pin assignment

Pin assignment of the sockets for digital outputs

The table below shows the pin assignment of the 8 sockets for the connection of the digital outputs.

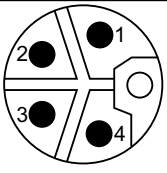
Table 2-357 Pin assignment for digital outputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 sockets for digital outputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	Unassigned		
2	Unassigned		
3	Ground 2M		
4	Output signal DQ_0: Connector X10 Output signal DQ_1: Connector X11 Output signal DQ_2: Connector X12 Output signal DQ_3: Connector X13 Output signal DQ_4: Connector X14 Output signal DQ_5: Connector X15 Output signal DQ_6: Connector X16 Output signal DQ_7: Connector X17		
5	Functional earth FE		

Pin assignment of the connector for infeed of the supply voltage 2L+

The table below shows the pin assignment of the connector for infeed of the supply voltage 2L+.

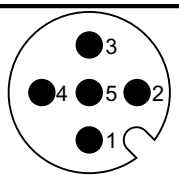
Table 2-358 Pin assignment of the supply voltage connector

Pin	Assignment	Front view of the connector
	X80	
1	Unassigned	
2	Ground 2M	
3	Unassigned	
4	2L+	

Pin assignment of the connector for IO-Link

The following table shows the pin assignment of the connector for IO-Link. The IO-Link interface corresponds to the specification according to port Class A.

Table 2-359 Pin assignment of the IO-Link interface

Pin	Assignment	Front view of the connector (Port Class A)
	X35	
1	1L+	
2	Unassigned	
3	Ground 1M	
4	Switching and communication cable (C/Q)	
5	Unassigned	

NOTE

Note that the module can only be supplied with a protective low voltage according to the standard SELV/PELV.

Parameters/address space

4

4.1 Parameters

The following table shows the parameters for the DQ 8x24VDC/2A 8xM12 IO-Link digital output module.

Table 2-360 Parameters

Parameters	Value range			Default	Scope	ISDU index (decimal)	ISDU subindex (decimal)
	Value	Dec.	Hex.				
Diagnostics: Missing load voltage 2L+	Disable	0	0	Disable	Module	131	1
	Enable	255	FF				
Diagnostics: Short-circuit to ground	Disable	0	0	Disable	Module (Short-circuit of an output to ground)	131	2
	Enable	255	FF				
Reaction to CPU/master STOP	Shutdown	0	0	Shutdown	Module	131	3
	Keep last value	2	2				
	Output substitute value	3	3				
Substitute value channel	0	0	0	0	Channel	131	4 ... 11
	1	255	FF				

4.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics for short-circuit of the output to ground.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the digital outputs of the module after a CPU/master STOP:

- Shut down: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel

With this parameter, you set substitute values for the digital outputs.

4.3 Address space

The figure below shows the assignment of the address space for the DQ 8x24VDC/2A 8xM12 IO-Link digital output module.

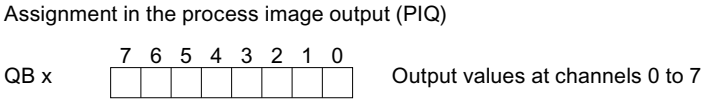


Figure 2-158 Address space IO-Link DQ 8x24VDC/2A 8xM12

4.4 IODD parameters

Device description IODD

An electronic device description is available for the DQ 8x24VDC/2A 8xM12 IO-Link digital output module, the IODD file (IO Device Description). The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the same manner by the IO-Link Configuration Tool of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODDfinder is available on the Internet (https://ioddfinder.io-link.com).

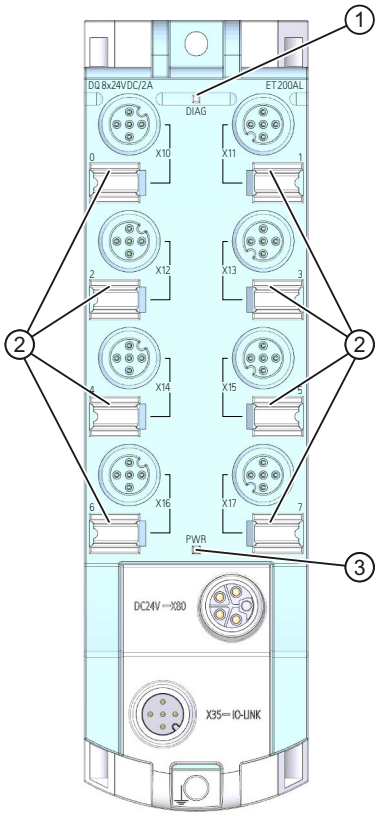
Interrupts/diagnostic alarms

5

5.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DQ 8x24VDC/2A 8xM12 IO-Link digital output module.



①	Diagnostic status (DIAG)	(red/green)
②	Channel status (0 to 7)	(green)
③	Load voltage 2L+ (PWR)	(green)

Figure 2-159 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic alarms can be found in the section Diagnostics alarms (Page 18).

DIAG LED

Table 2-361 Error display of the DIAG LED

DIAG LED	Meaning
□ Off	No supply voltage 1L+
☼ Flashes	• No data exchange with the IO-Link Master (e.g. wire break) • Firmware is loading
■ On	Module is currently exchanging data with the IO-Link master and no module diagnostics
☼ Flashes	Module is currently exchanging data with the IO-Link master and module diagnostics

LED channel status

Table 2-362 LED channel status display

LED channel status	Meaning
□ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-363 Status display of the PWR LED

PWR LED	Meaning
□ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.2 Interrupts

The DQ 8x24VDC/2A 8xM12 IO-Link digital output module supports diagnostic interrupts.

Diagnostic interrupt

The digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of outputs to ground
- Load voltage 2L+ missing or too low

5.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the LED DIAG flashes red on the digital output module. You can read out the diagnostics alarms, for example, from the status of the IO-Link master. You can evaluate the error codes with the user program.

Table 2-364 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Remedy
Short-circuit	0x7711	Short-circuit of an output to ground	Eliminate the short-circuit
Load voltage 2L+ missing	0x5112	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module

Technical specifications

6

Technical specifications of the DQ 8x24VDC/2A 8xM12 IO-Link digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/de/en/pv/6ES7142-5AF00-0BL0/td?dl=en).

Article number	6ES7142-5AF00-0BL0
General information	
Product type designation	IO-Link DQ 8x24VDC/2A
HW functional status	FS01
Firmware version	V1.0.x
Engineering with	
• IODD file	Yes
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V; Supply from 1Us+ of the IO-Link master
• permissible range, lower limit (DC)	18 V
• permissible range, upper limit (DC)	30 V
• Reverse polarity protection	Yes; against destruction
Load voltage 2L+	
• Rated value (DC)	24 V; Supply via M12 connector L-coded
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; against destruction; load increasing
Input current	
Current consumption (rated value)	12 mA; without load
from load voltage 2L+, max.	8 A; Maximum value
Power loss	
Power loss, typ.	3.6 W
Digital outputs	
Number of digital outputs	8
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	2.8 A
Switching capacity of the outputs	
• on lamp load, max.	10 W
Load resistance range	
• lower limit	12 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	2 A (45 °C); 1 A (55 °C)

Article number	6ES7142-5AF00-0BL0
• for signal "1" permissible range, max.	2 A; with inductive load to IEC 60947-5-1, DC-13 / AC-15
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.1 Hz; 0.25 Hz at 25 °C
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per module, max.	8 A
Cable length	
• unshielded, max.	30 m
IO-Link	
IO-Link protocol 1.1	Yes
Transmission rate	38.4 kBd (COM2)
Cycle time, min.	2.1 ms
Size of process data, input per module	0 byte
Size of process data, output per module	1 byte
Supported IO-Link profiles	common profile
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type A	Yes
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; Outputs to ground; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and the power supply of the electronics	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01

Article number	6ES7142-5AF00-0BL0
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SILCL according to IEC 62061	SILCL 2
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pin, A-coded
Type of electrical connection for IO-Link	M12, 5-pin, A-coded
Design of electrical connection for supply voltage	M12, 4-pin, L-coded
Dimensions	
Width	45 mm
Height	159 mm
Depth	45 mm
Weights	
Weight, approx.	168 g

Derating curve

The following figure show the load current derating with mounting clearance observed, depending on the ambient temperature.

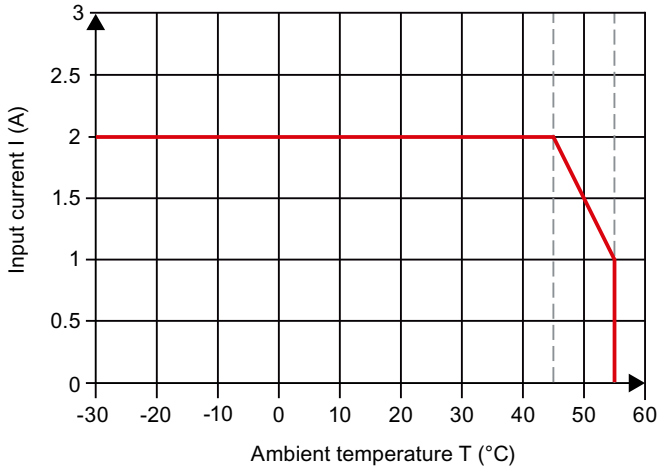


Figure 2-160 Derating curve IO-Link digital output module DQ 8x24VDC/2A 8xM12

Dimension drawing

A

The figure below shows the dimension drawing of the DQ 8x24VDC/2A 8xM12 IO-Link digital output module in front and side views.

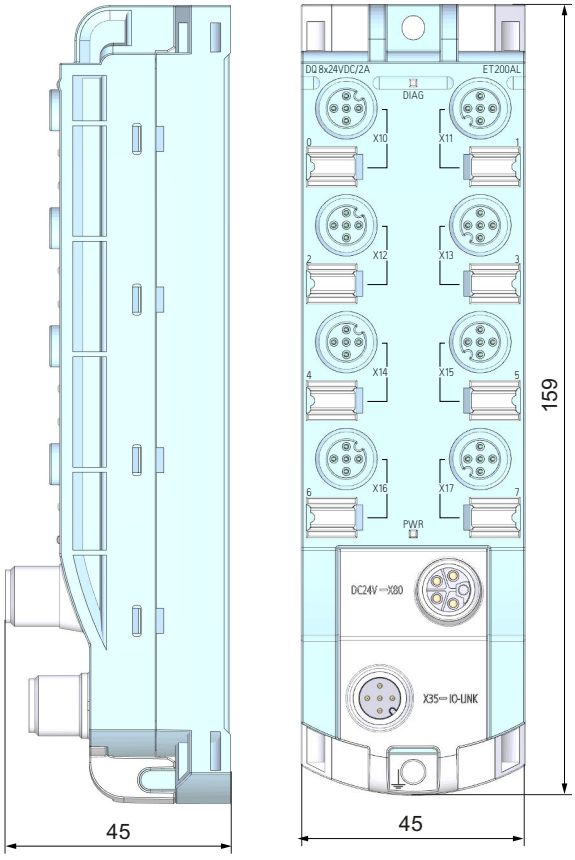


Figure 2-161 Dimension drawing

SIEMENS

SIMATIC

ET 200AL IO-Link digital input/digital output module DIQ 4+DQ 4x24VDC/0,5A 8xM8 (6ES7143-5BF00-0BL0)

Equipment Manual

ET 200AL IO-Link I/O modules Documentation Guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Interrupts/diagnostics alarms 5

Technical specifications 6

Dimension drawing A

08/2021
A5E47925743-AB

Preface

Purpose of the documentation

This manual supplements the system manual ET 200AL IO-Link (https://support.automation.siemens.com/WW/view/en/109773203). Functions that generally relate to the distributed I/O system ET 200AL IO-Link I/O modules are described there.

The information provided in this manual and in the system manual and function manuals supports you in commissioning the ET 200AL IO-Link I/O modules.

Changes compared to the previous version

This manual contains the following changes compared to the previous version:

- Supplements in the section Parameters (Page 14).
- Update of the section Technical specifications (Page 20)

Conventions

Also observe notes labeled as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are

available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 ET 200AL IO-Link I/O modules Documentation Guide 5

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

3 Wiring 11

3.1 Terminal and block diagram 11

3.2 Pin assignment 12

4 Parameters/address space 14

4.1 Parameters 14

4.2 Explanation of the parameters 14

4.3 Address space 15

4.4 IODD parameters 16

5 Interrupts/diagnostics alarms 17

5.1 Status and error displays 17

5.2 Interrupts 18

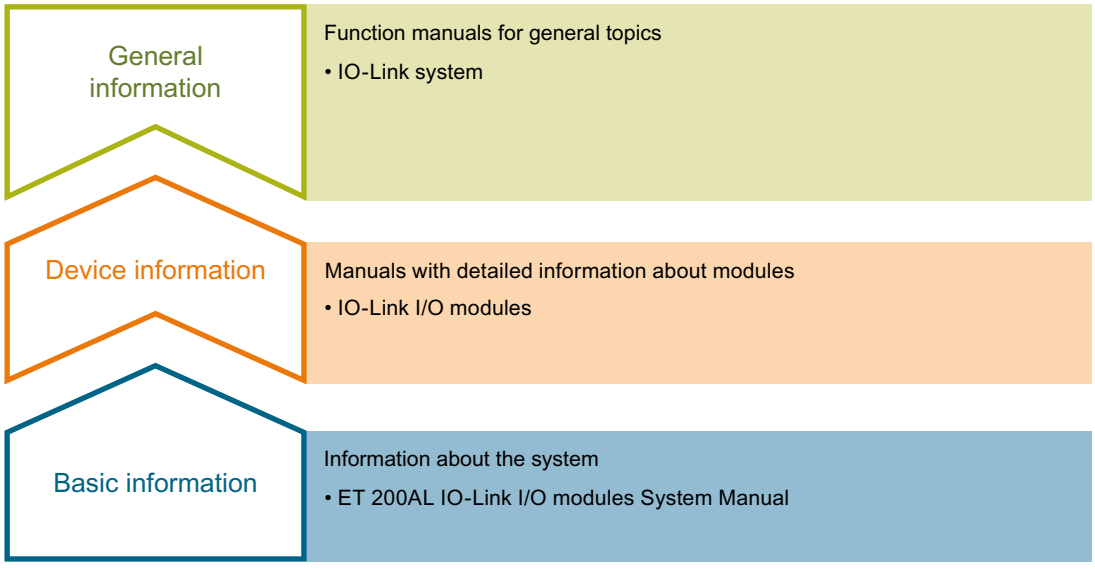
5.3 Diagnostics alarms 19

6 Technical specifications 20

A Dimension drawing 24

ET 200AL IO-Link I/O modules Documentation Guide 1

The documentation for the SIMATIC ET 200AL IO-Link I/O modules is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The system manual describes in detail the configuration, installation, wiring and commissioning of the distributed I/O system SIMATIC ET 200AL IO-Link I/O modules.

Device information
Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC IO-Link system.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

ET 200AL Manual Collection

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area of "mySupport", you can access the latest product data for your CAx or CAe system.

You configure your own download package with a few clicks.

You can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" CAx data on the Internet (https://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/ae).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109767888).

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning. PRONETA has two core functions:

- The topology overview automatically scans the PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SIMATIC S7-PCT

The Port Configuration Tool ("PCT") is PC-based software for the parameter assignment of Siemens IO-Link master-modules and IO-Link devices from any manufacturer.

The IO-Link devices are integrated using the standardized device description "IODD" that is available from the respective device manufacturer. S7-PCT supports the version 1.0 as well as V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link masters from STEP 7; however, it can also be started as "standalone" if the IO-Link master is not operated on a SIMATIC controller or when STEP 7 is not used.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Product overview

2

2.1 Properties

Article number

6ES7143-5BF00-0BL0

View of the module

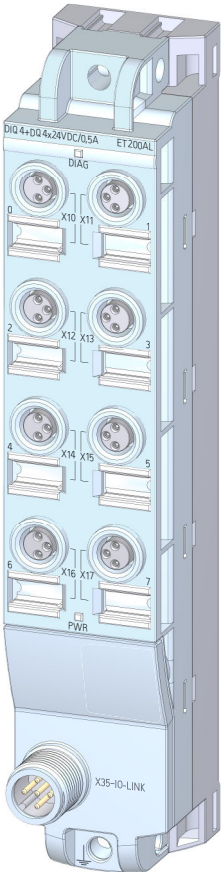


Figure 2-162 View of the DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input/digital output module

Properties

The module has the following technical properties:

- 4 digital inputs or digital outputs and 4 digital outputs, depending on parameter assignment
  - DIQ signals connected to 2L+ (switched)
  - DQ signals connected to 2L+ (switched)
- M8 sockets for connection of sensors and actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Configurable diagnostics can be set for each module
  - Typical input delay of 3 ms
  - Suitable for switches and proximity switches
- Digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current 0.5 A per output
  - Configurable diagnostics can be set for each module
- Dimensions 30 x 159 mm
- Interface for IO-Link and power supply:
  - M12 connector A-coded
  - IO-Link Port Class B
  - Supply of the module electronics
  - Encoder supply and load voltage supply of output

The module supports the following functions:

- Firmware update
- IO-Link profile: General profile

Accessories

The following components are included in the module package:

- Identification labels
- Spacers

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

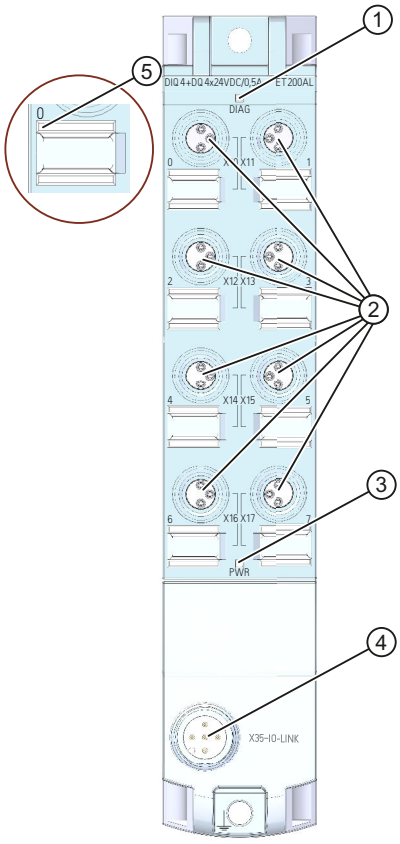
- Connectors
- Cables
- M8 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.automation.siemens.com/WW/view/en/109773203) IO-Link I/O modules system manual.

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input/digital output module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input/output signal
③ PWR: LED display for load voltage 2L+
④ X35: IO-Link interface
⑤ LED displays 0 to 7 for the channel status

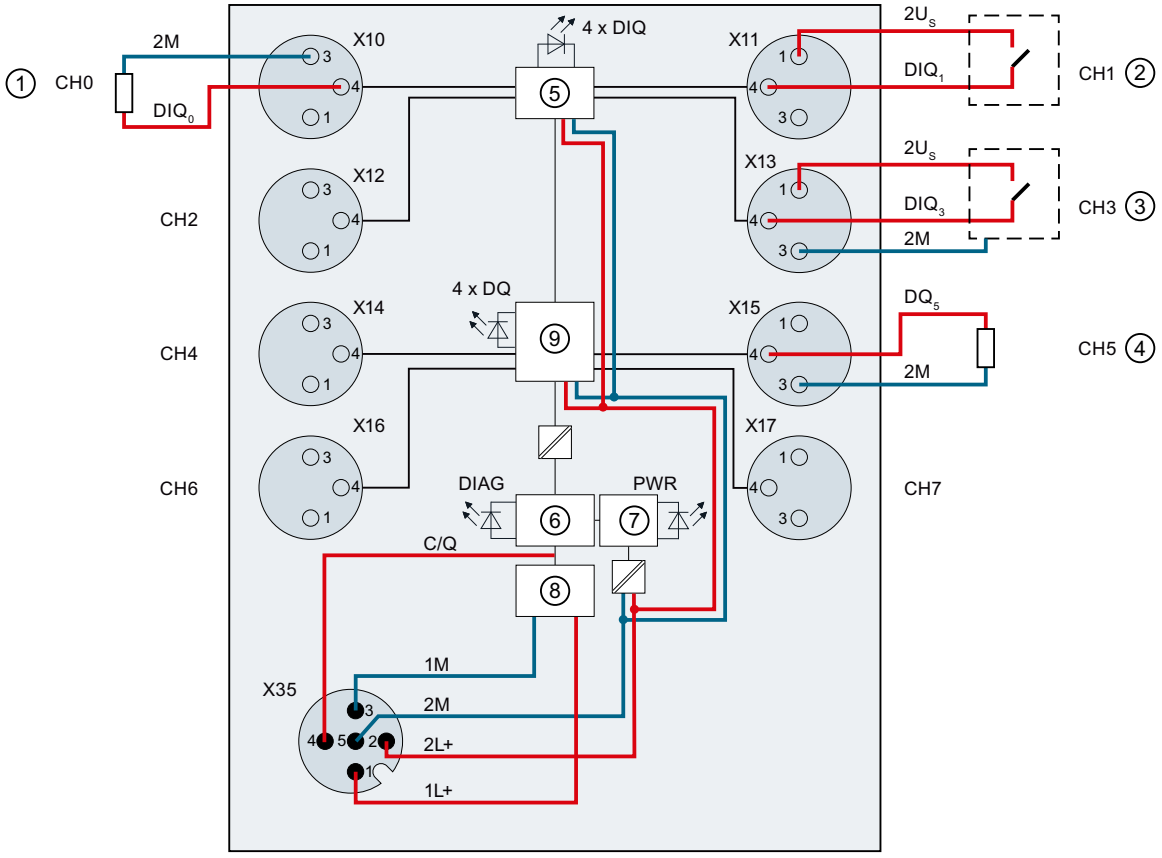
Figure 2-163 Operator controls and display elements

Wiring

3

3.1 Terminal and block diagram

The following figure shows an example of the pin assignment of signal inputs with 2- and 3-wire connection as well as signal outputs.



①	Configured as output	1L+	Supply voltage 1L+ (non-switched)
②	Configured as input: 2-wire connection	1M	Ground 1M (non-switched)
③	Configured as input: 3-wire connection	2L+	Load voltage 2L+ (switched)
④	Output	2M	Ground 2M (switched)
⑤	DI/DQ circuit (2L+ switched)	$2U_S$	24 V encoder supply
⑥	Microcontroller	DIQ_n	Input/output signal
⑦	Monitoring	DQn	Output signal
⑧	Internal supply voltage	DIQ	LEDs channel status (0, 1, 2 and 3) (green)
⑨	DQ circuit (2L+ switched)	DQ	LEDs channel status (4, 5, 6 and 7) (green)
X10 to X17	Channels 0 to 7	DIAG	LED diagnostic status (red/green)
X35	IO-Link interface	PWR	LED supply voltage 2L+ (green)

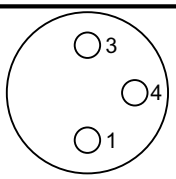
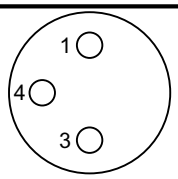
Figure 2-164 Terminal and block diagram

3.2 Pin assignment

Pin assignment of the sockets for digital inputs/digital outputs

The tables below show the pin assignments of the 8 sockets for connection of the digital inputs/digital outputs.

Table 2-365 Pin assignment for digital inputs/digital outputs

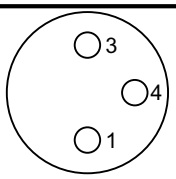
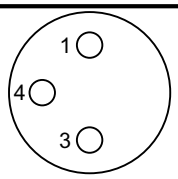
Pin	Assignment	Front view of the sockets	
	X10 to X13 - sockets for digital inputs / outputs	**X10, X12**	**X11, X13**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
3	Ground 2M		
4	Input/output signal DIQ_0: X10 Input/output signal DIQ_1: X11 Input/output signal DIQ_2: X12 Input/output signal DIQ_3: X13		

NOTICE

24 V encoder supply $2U_S$

Use only the 24 V encoder supply $2U_S$ provided by the digital input/digital output module to supply power to the encoder.

Table 2-366 Pin assignment for digital outputs

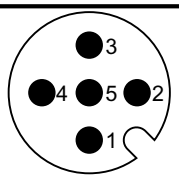
Pin	Assignment	Front view of the sockets	
	X14 to X17- sockets for digital inputs / outputs	**X14, X16**	**X15, X17**
1	n.c.		
3	Ground 2M		
4	Output signal DQ_4: X14 Output signal DQ_5: X15 Output signal DQ_6: X16 Output signal DQ_7: X17		

Pin assignment of the IO-Link connector

The following table shows the pin assignment of the connector for the IO-Link connection. The IO-Link interface corresponds to the specification according to Port Class B.

Table 2-367 Pin assignment of the IO-Link interface

Pin	Assignment	Front view of the connector (Port Class B)
	X35	
1	1L+	
2	2L+	

Pin	Assignment	Front view of the connector (Port Class B)
	X35	
3	Ground 1M	
4	Switching and communication cable (C/Q)	
5	Ground 2M	

NOTE

Note that the module can only be supplied with a protective low voltage according to the standard SELV/PELV.

Parameters/address space

4

4.1 Parameters

The following table shows the parameters for the DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input / digital output module.

Table 2-368 Parameters

Parameters	Value range			Default	Scope	ISDU index (decimal)	ISDU subindex (decimal)
	Value	Dec.	Hex.				
Diagnostics: Missing load voltage 2L+	Disable	0	0	Disable	Module	131	1
	Enable	255	FF				
Diagnostics: Short-circuit to ground	Disable	0	0	Disable	Module (Short-circuit of encoder supply or of the output to ground)	131	2
	Enable	255	FF				
Freely assignable channel 0 ... 3	DI	0	0	DI	Channel	131	3 ... 6
	DQ	255	FF				
Reaction to CPU/master STOP	Shutdown	0	0	Shutdown	Module (digital outputs)	131	7
	Keep last value	2	2				
	Output substitute value	3	3				
Substitute value channel	0	0	0	0	Channel (digital outputs)	131	8 ... 15
	1	255	FF				

4.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics for short-circuit of the encoder supply or output to ground.

Freely assignable channel n

With this parameter, you set whether the channel is to be operated as an input or output.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the digital outputs of the digital input/ digital output module after a CPU/master STOP:

- Shut down: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel

With this parameter, you set substitute values for the digital outputs.

4.3 Address space

The figure below shows the assignment of the address space for the IO-Link DIQ 4+DQ 4x24VDC/0,5A 8xM8.

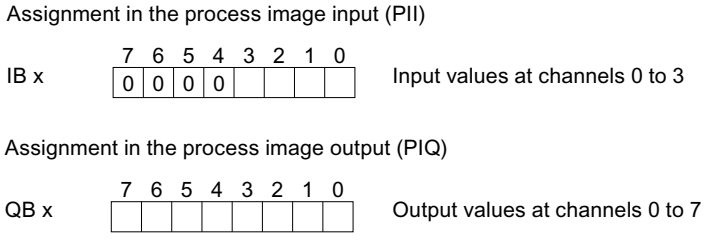


Figure 2-165 Address space IO-Link DIQ 4+DQ 4x24VDC/0,5A 8x8M

NOTE

Parameter assignment of the channels

Parameters for the first four channels can be freely assigned.

For the channels 0 ... 3 that are configured as input, the corresponding values in the output data do not trigger any reaction.

For the channels 0 ... 3 that are configured as output, the input value in the process image is 0.

4.4 IODD parameters

Device description IODD

An electronic device description is available for the DIQ 4+DQ 4x24VDC/0.5A 8xM8 IO-Link digital input / digital output module, the IODD file (IO Device Description). The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the same manner by the IO-Link Configuration Tool of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODDfinder is available on the Internet (https://ioddfinder.io-link.com).

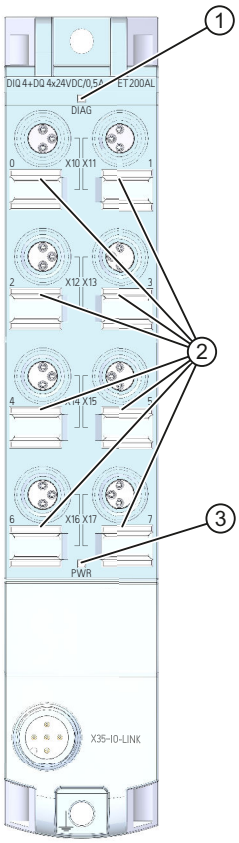
Interrupts/diagnostics alarms

5

5.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input / digital output module.



①	Diagnostic status (DIAG)	(red/green)
②	Channel status (0 to 7)	(green)
③	Load voltage 2L+ (PWR)	(green)

Figure 2-166 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Corrective measures for diagnostics alarms can be found in the section Diagnostics alarms (Page 19).

DIAG LED

Table 2-369 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• No data exchange with the IO-Link Master, for example, due to wire break • Firmware is loading
■ On	Module is currently exchanging data with the IO-Link master and no module diagnostics
☼ Flashes	Module is currently exchanging data with the IO-Link master and module diagnostics

LED channel status

Table 2-370 LED channel status display

LED channel status	Meaning
☐ Off	Process signal = 0 or deactivated
■ On	Process signal = 1

PWR LED

Table 2-371 Status display of the PWR LED

PWR LED	Meaning
☐ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.2 Interrupts

The DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input / digital output module supports diagnostic interrupts.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of encoder supply to ground
- Short-circuit of outputs to ground
- Load voltage 2L+ missing or too low

5.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the DIAG LED flashes red on the digital input/output module.
You can read out the diagnostics alarms, for example, from the port status of the IO-Link master. You can evaluate the error codes with the user program.

Table 2-372 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Remedy
Short-circuit[1]	0x7710	Short-circuit of an encoder supply to ground	• Eliminate the short-circuit
	0x7711	Short-circuit of an output to ground	
Load voltage 2L+ missing	0x5112	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module
[1] = If a short-circuit of the encoder supply to ground is detected, the diagnostic alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.			

Technical specifications

6

Technical specifications of the DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input / digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/de/en/pv/6ES7143-5BF00-0BL0/td?dl=de).

Article number	6ES7143-5BF00-0BL0
General information	
Product type designation	DIQ 4+DQ 4X24VDC/0.5A, 8xM8
HW functional status	FS01
Firmware version	V1.0.x
Engineering with	
• IODD file	Yes
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V; Supply from 1Us+ of the IO-Link master
• permissible range, lower limit (DC)	18 V
• permissible range, upper limit (DC)	30 V
• Reverse polarity protection	Yes; against destruction
Load voltage 2L+	
• Rated value (DC)	24 V; Supply from 2UA+ of the IO-Link master
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up
Input current	
Current consumption (rated value)	15 mA; without load
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	8; Supply from 2UA+ of the IO-Link master
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders (depending on IO-Link master supply via 2UA+)
Power loss	
Power loss, typ.	2.3 W
Digital inputs	
Number of digital inputs	4; Parameterizable as DIQ
Input characteristic curve in accordance with IEC 61131, type 3	Yes

Article number	**6ES7143-5BF00-0BL0**
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	4
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Digital outputs	
Number of digital outputs	8; 4 DQ fixed, 4 DIQ parameterizable
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	0.7 A
Limitation of inductive shutdown voltage to	2L+ (-50 V)
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per module, max.	4 A
Cable length	
• unshielded, max.	30 m

Article number	6ES7143-5BF00-0BL0
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
IO-Link	
IO-Link protocol 1.1	Yes
Transmission rate	38.4 kBd (COM2)
Cycle time, min.	2.4 ms
Size of process data, input per module	1 byte
Size of process data, output per module	1 byte
Supported IO-Link profiles	common profile
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type B	Yes
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; outputs to ground; encoder supply to ground; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and the power supply of the electronics	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SILCL according to IEC 62061	SILCL 2
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C

Article number	6ES7143-5BF00-0BL0
Connection method	
Design of electrical connection for the inputs and outputs	M8, 3-pole
Type of electrical connection for IO-Link	M12, 5-pin, A-coded
Dimensions	
Width	30 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	125 g

Dimension drawing

A

The figure below shows the dimension drawing of the DIQ 4+DQ 4x24VDC/0,5A 8xM8 IO-Link digital input / digital output module in front and side view.

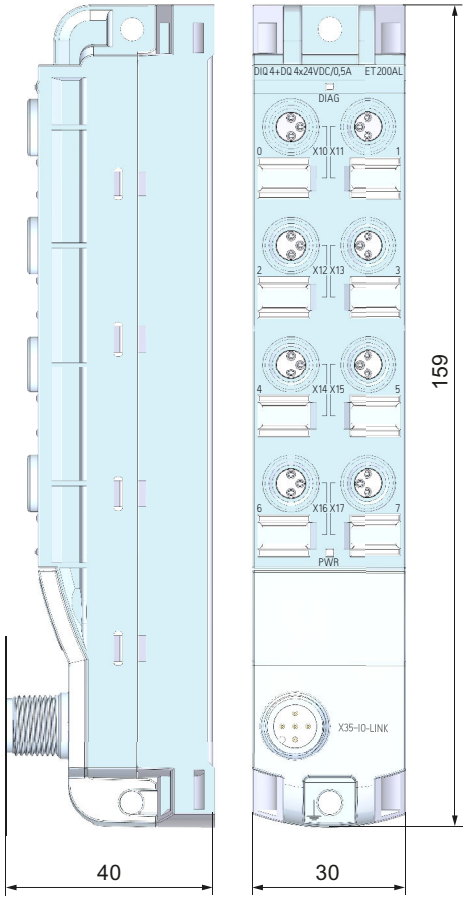


Figure 2-167 Dimension drawing

SIEMENS

SIMATIC

ET 200AL IO-Link digital input/digital output module DIQ 16x24VDC/0,5A 8xM12 (6ES7143-5AH00-0BL0)

Equipment Manual

ET 200AL IO-Link I/O modules Documentation Guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Interrupts/diagnostic alarms 5

Technical specifications 6

Dimension drawing A

08/2021
A5E47926885-AB

Preface

Preface IO-Link module AL

Purpose of the documentation

This manual supplements the system manual ET 200AL IO-Link (https://support.automation.siemens.com/WW/view/en/109773203). Functions that generally relate to the distributed I/O system ET 200AL IO-Link I/O modules are described there.

The information provided in this manual and in the system manual and function manuals supports you in commissioning the ET 200AL IO-Link I/O modules.

Changes compared to the previous version

This manual contains the following changes compared to the previous version:

- Supplements in the section Parameters (Page 13).
- Update of the section Technical specifications (Page 19)

Conventions

Also observe notes labeled as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 ET 200AL IO-Link I/O modules Documentation Guide 5

2 Product overview 8

2.1 Properties 8

2.2 Operator controls and display elements 10

3 Wiring 11

3.1 Terminal and block diagram 11

3.2 Pin assignment 12

4 Parameters/address space 13

4.1 Parameters 13

4.2 Explanation of the parameters 13

4.3 Address space 14

4.4 IODD parameters 14

5 Interrupts/diagnostic alarms 16

5.1 Status and error displays 16

5.2 Interrupts 17

5.3 Diagnostics alarms 18

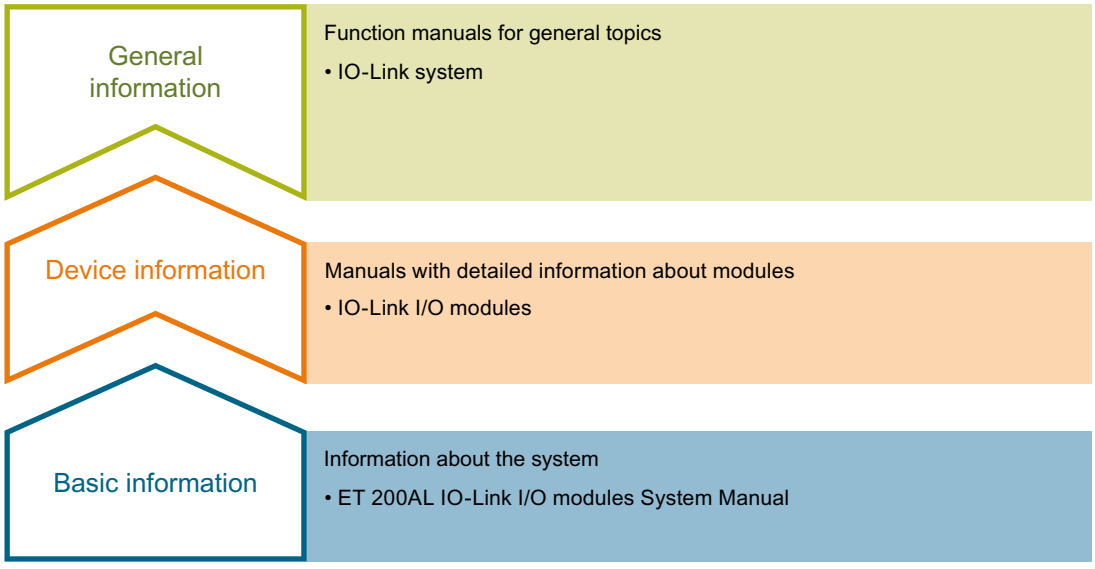
6 Technical specifications 19

A Dimension drawing 23

ET 200AL IO-Link I/O modules Documentation Guide

1

The documentation for the SIMATIC ET 200AL IO-Link I/O modules is arranged into three areas.
This arrangement enables you to access the specific content you require.



Basic information
The system manual describes in detail the configuration, installation, wiring and commissioning of the distributed I/O system SIMATIC ET 200AL IO-Link I/O modules.

Device information
Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics regarding the SIMATIC IO-Link system.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

ET 200AL Manual Collection

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.automation.siemens.com/WW/view/en/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en).

"mySupport" - Documentation

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/My/ww/en/documentation).

"mySupport" - CAx data

In the CAx data area of "mySupport", you can access the latest product data for your CAx or CAe system.

You configure your own download package with a few clicks.

You can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find "mySupport" CAx data on the Internet (https://support.industry.siemens.com/my/ww/en/CAxOnline).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/ae).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109767888).

PRONETA

SIEMENS PRONETA (PROFINET network analysis) allows you to analyze the plant network during commissioning. PRONETA has two core functions:

- The topology overview automatically scans the PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

You can find SIEMENS PRONETA on the Internet (https://support.industry.siemens.com/cs/ww/en/view/67460624).

SIMATIC S7-PCT

The Port Configuration Tool ("PCT") is PC-based software for the parameter assignment of Siemens IO-Link master-modules and IO-Link devices from any manufacturer.

The IO-Link devices are integrated using the standardized device description "IODD" that is available from the respective device manufacturer. S7-PCT supports the version 1.0 as well as V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link masters from STEP 7; however, it can also be started as "standalone" if the IO-Link master is not operated on a SIMATIC controller or when STEP 7 is not used.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

Product overview

2

2.1 Properties

Article number

6ES7143-5AH00-0BL0

View of the module

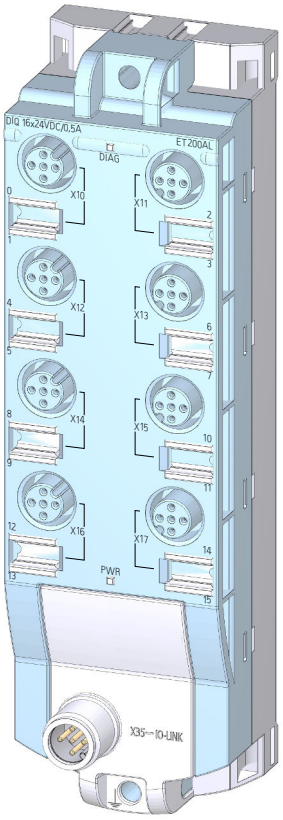


Figure 2-168 View of the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module

Properties

The module has the following technical properties:

- 16 digital inputs or digital outputs, depending on configuration and parameter assignment
  - 16 DIQ signals connected to 2L+ (switched)
- M12 sockets for connection of sensors and actuators
- Digital inputs:
  - 24 V DC supply voltage
  - Suitable for switches and proximity switches
  - Typical input delay of 3 ms
  - Configurable diagnostics can be set for each module
- Digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current per output 0.5 A
  - Configurable diagnostics can be set for each module
- Dimensions 45 x 159 mm
- Interface for IO-Link and power supply:
  - M12 connector A-coded
  - Supply of the module electronics
  - IO-Link Port Class B
  - Encoder supply and load voltage supply of output

The module supports the following functions:

- Firmware update
- IO-Link profile: General profile

Accessories

The following components are included in the module package:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

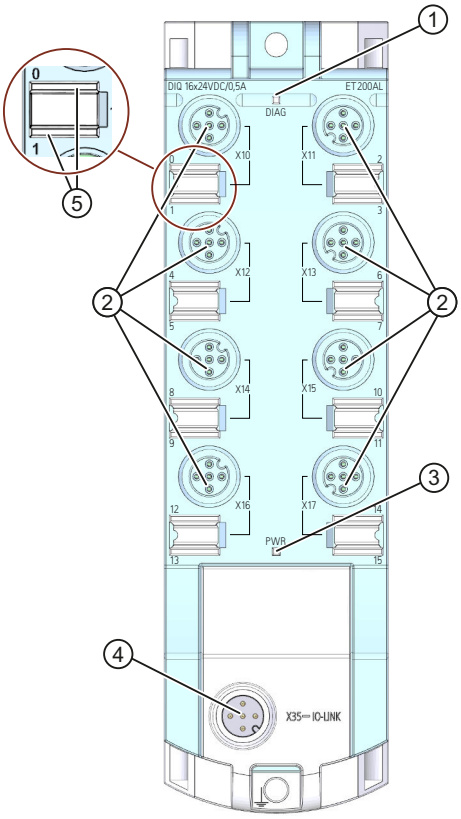
- Connectors
- Cables
- M12 sealing cap

See also

You can find more information on accessories in the Accessories/spare parts section of the ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965) IO-Link I/O modules system manual.

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module.



① DIAG: LED display for the diagnostic status
② X10 to X17: Sockets for the input/output signal
③ PWR: LED display for load voltage 2L+
④ X35: IO-Link interface
⑤ LED displays 0 to 15 for the channel status

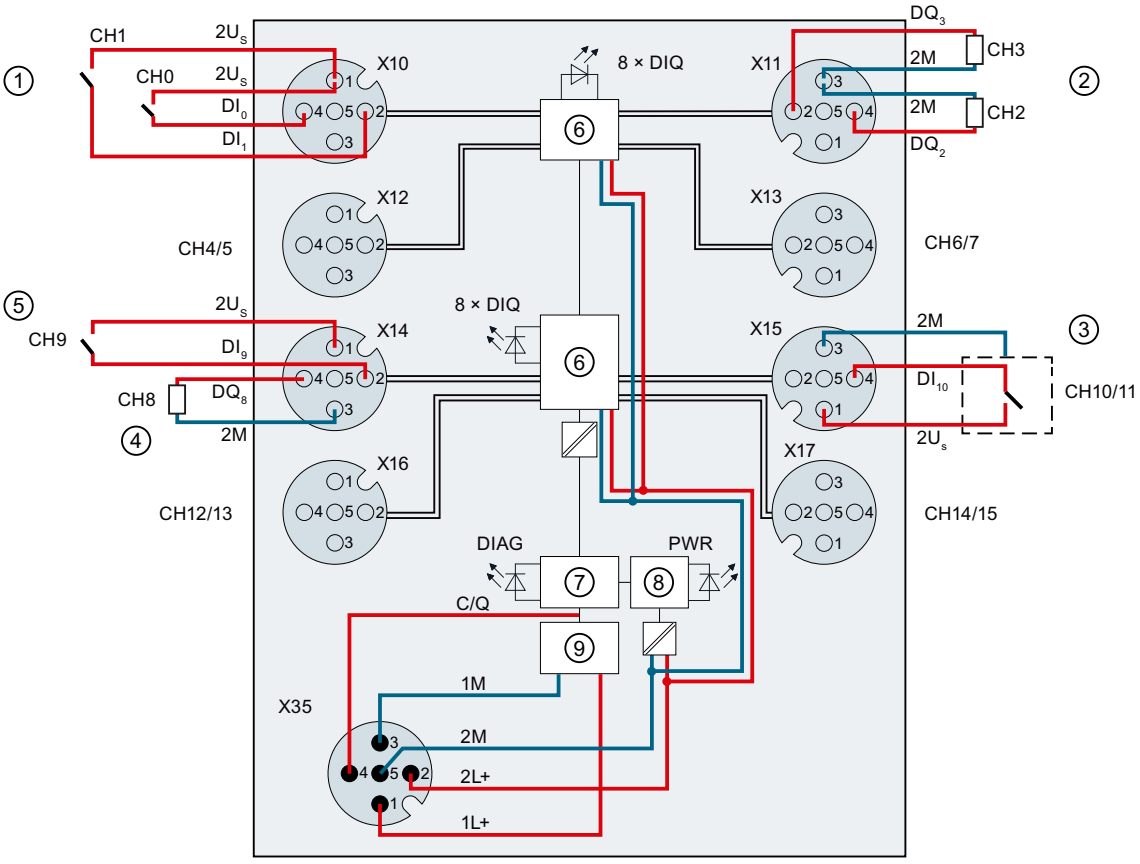
Figure 2-169 Operator controls and display elements

Wiring

3

3.1 Terminal and block diagram

The figure below shows an example of the pin assignment of signal inputs with 2-wire and 3-wire connection and of signal outputs in the configuration modes for digital inputs and outputs.



①	Configured as inputs: 2-wire connection	1L+	Supply voltage 1L+ (non-switched)
②	Configured as outputs	1M	Ground 1M (non-switched)
③	Configured as input: 3-wire connection	2L+	Load voltage 2L+ (switched)
④	Configured as output	2M	Ground 2M (switched)
⑤	Configured as input: 2-wire connection	$2U_S$	24 V encoder supply
⑥	DI/DQ circuit (2L+ switched)	DIQ_n	Input/output signal
⑦	Microcontroller	DIQ	LEDs channel status (0..15) (green)
⑧	Monitoring	DIAG	Diagnostic status LED (red/green)
⑨	Internal supply voltage	PWR	LED supply voltage 2L+ (green)
X10 to X17	Channels 0 to 15		
X35	IO-Link interface		

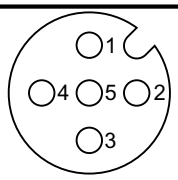
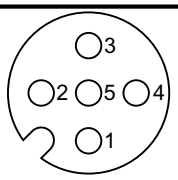
Figure 2-170 Wiring and block diagram of configuration modes for digital inputs and outputs

3.2 Pin assignment

Pin assignment of the sockets for digital inputs/digital outputs

The table below shows the pin assignments of the 8 sockets for the connection of the digital inputs/digital outputs.

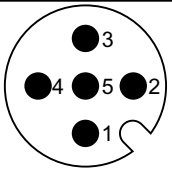
Table 2-373 Pin assignment for digital inputs/digital outputs

Pin	Assignment	Front view of the sockets	
	X10 to X17 - sockets for digital inputs/outputs	**X10, X12, X14, X16**	**X11, X13, X15, X17**
1	24 V encoder supply $2U_S$ (derived from 2L+ switched)		
2	Input/output signal DIQ_1: Connector X10 Input/output signal DIQ_3: Connector X11 Input/output signal DIQ_5: Connector X12 Input/output signal DIQ_7: Connector X13 Input/output signal DIQ_9: Connector X14 Input/output signal DIQ_{11}: Connector X15 Input/output signal DIQ_{13}: Connector X16 Input/output signal DIQ_{15}: Connector X17		
3	Ground 2M		
4	Input/output signal DIQ_0: Connector X10 Input/output signal DIQ_2: Connector X11 Input/output signal DIQ_4: Connector X12 Input/output signal DIQ_6: Connector X13 Input/output signal DIQ_8: Connector X14 Input/output signal DIQ_{10}: Connector X15 Input/output signal DIQ_{12}: Connector X16 Input/output signal DIQ_{14}: Connector X17		
5	Functional earth FE		

Pin assignment of the connector for IO-Link

The following table shows the pin assignment of the connector for the IO-Link.

Table 2-374 Pin assignment of the IO-Link interface

Pin	Assignment	Front view of the connector (Port Class B)
	X35	
1	1L+	
2	2L+	
3	Ground 1M	
4	Switching and communication cable (C/Q)	
5	Ground 2M	

NOTE

Note that the module can only be supplied with a protective low voltage according to the standard SELV/PELV.

Parameters/address space

4

4.1 Parameters

The table below shows the parameters for the IO-Link digital input/digital output module DIQ 16x24VDC/0,5A 8xM12.

Table 2-375 Parameters

Parameters	Value range			Default	Scope	ISDU index (decimal)	ISDU subindex (decimal)
	Value	Dec.	Hex.				
Diagnostics: Missing load voltage 2L+	Disable	0	0	Disable	Module	131	1
	Enable	255	FF				
Diagnostics: Short-circuit to ground	Disable	0	0	Disable	Module (Short-circuit of encoder supply or of the output to ground)	131	2
	Enable	255	FF				
Freely assignable channel 0 ... 7	DI	0	0	DI	Channel	131	3 ... 10
	DQ	255	FF				
Freely assignable channel 8 ... 15	DI	0	0	DQ	Channel	131	11 ... 18
	DQ	255	FF				
Reaction to CPU/master STOP	Shutdown	0	0	Shutdown	Module (digital outputs)	131	19
	Keep last value	2	2				
	Output substitute value	3	3				
Substitute value channel	0	0	0	0	Channel (digital outputs)	131	20 ... 35
	1	255	FF				

4.2 Explanation of the parameters

Diagnostics: Missing load voltage 2L+

Enabling of the diagnostics for missing or insufficient load voltage 2L+.

Diagnostics: Short-circuit to ground

Enabling of the diagnostics, at short-circuit of an encoder supply or of an output to ground.

Freely assignable channel

With this parameter, you set whether the channel is to be operated as an input or output.

Reaction to CPU/master STOP

With this parameter, you set the reaction of the channels configured as output of the digital input/output module after a CPU/master STOP:

- Deactivate: The digital output is de-energized.
- Keep last value: The last value of the digital output remains activated.
- Output substitute value: The module outputs a configured substitute value.

Substitute value channel

With this parameter, you set substitute values for the digital outputs.

4.3 Address space

The figure below shows the assignment of the address space for the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module.

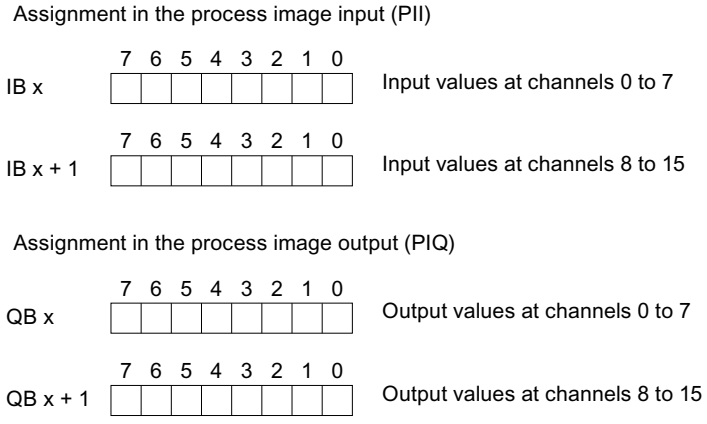


Figure 2-171 Address space IO-Link DIQ 16x24VDC/0,5A 8xM12

4.4 IODD parameters

Device description IODD

An electronic device description is available for the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module, the IODD file (IO Device Description). The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the same manner by the IO-Link Configuration Tool of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODDfinder is available on the Internet (https://ioddfinder.io-link.com).

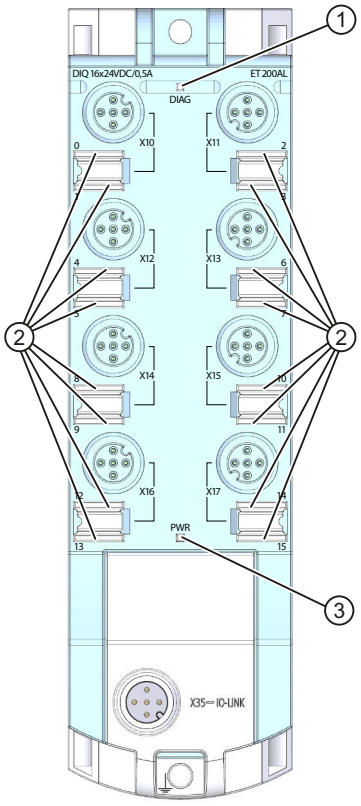
Interrupts/diagnostic alarms

5

5.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module.



① Diagnostic status (DIAG) (red/green)
② Channel status (0 to 15) (green)
③ Load voltage 2L+ (PWR) (green)

Figure 2-172 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic reports can be found in chapter Diagnostics alarms (Page 18).

DIAG LED

Table 2-376 Error display of the DIAG LED

DIAG LED	Meaning
☐ Off	No supply voltage 1L+
☼ Flashes	• No data exchange with the IO-Link Master (e.g. wire break) • Firmware is loading
■ On	Module is currently exchanging data with the IO-Link master and no module diagnostics
☼ Flashes	Module is currently exchanging data with the IO-Link master and module diagnostics

LED channel status

Table 2-377 LED channel status display

LED channel status	Meaning
☐ Off	Process signal = 0
■ On	Process signal = 1

PWR LED

Table 2-378 Status display of the PWR LED

PWR LED	Meaning
☐ Off	Load voltage 2L+ is missing or too low
■ On	Load voltage 2L+ present

5.2 Interrupts

Diagnostic interrupts of the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module.

Diagnostic interrupt

The digital input/digital output module generates a diagnostic interrupt at the following events:

- Short-circuit of an encoder supply to ground, or
- Short-circuit of an output to ground
- Load voltage 2L+ missing or too low

5.3 Diagnostics alarms

For each diagnostic event, a diagnostics alarm is issued and the LED DIAG flashes red on the digital input/digital output module.
You can read out the diagnostics alarms, for example, from the status of the IO-Link master.
You can evaluate the error codes with the user program.

Table 2-379 Diagnostics alarms, their meanings and corrective measures

Diagnostics alarm	Error code	Meaning	Solution
Short circuit[1]	0x7710	Short-circuit of an encoder supply to ground	• Eliminate the short-circuit
	0x7711	Short-circuit of an output to ground	
Load voltage 2L+ missing[2]	0x5112	Load voltage 2L+ missing or too low	• Check the supply voltage • Check the module

[1] = If a short-circuit of an encoder supply to ground is detected, the diagnostic alarm "Short-circuit" is always output. This alarm is output even if all channels are configured as outputs.
[2] = If you are using ET 200AL modules in connection with the ET 200SP distributed I/O system, the diagnostic alarm "Load voltage missing" is displayed.

Technical specifications

6

Technical specifications of the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module

The following table shows the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/de/en/pv/6ES7143-5AH00-0BL0/td?dl=en).

Article number	6ES7143-5AH00-0BL0
General information	
Product type designation	DIQ 16X24VDC/0.5A, 8XM12
HW functional status	FS01
Firmware version	V1.0.x
Engineering with	
• IODD file	Yes
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V; Supply from 1Us+ of the IO-Link master
• permissible range, lower limit (DC)	18 V
• permissible range, upper limit (DC)	30 V
• Reverse polarity protection	Yes; against destruction
Load voltage 2L+	
• Rated value (DC)	24 V; Supply from 2UA+ of the IO-Link master
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes; Against destruction; encoder power supply outputs applied with reversed polarity, loads pick up
Input current	
Current consumption (rated value)	20 mA; without load
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	8; Supply from 2UA+ of the IO-Link master
24 V encoder supply	
• Short-circuit protection	Yes; per module, electronic
• Output current, max.	0.7 A; Total current of all encoders (depending on IO-Link master supply via 2UA+)
Power loss	
Power loss, typ.	4 W
Digital inputs	
Number of digital inputs	16; Parameterizable as DIQ
Input characteristic curve in accordance with IEC 61131, type 3	Yes

Article number	6ES7143-5AH00-0BL0
Number of simultaneously controllable inputs	
all mounting positions	
– up to 55 °C, max.	16
Input voltage	
• Rated value (DC)	24 V
• for signal "0"	-3 to +5V
• for signal "1"	+11 to +30V
Input current	
• for signal "1", typ.	3 mA
Input delay (for rated value of input voltage)	
for standard inputs	
– at "0" to "1", min.	1.2 ms
– at "0" to "1", max.	4.8 ms
– at "1" to "0", min.	1.2 ms
– at "1" to "0", max.	4.8 ms
Cable length	
• unshielded, max.	30 m
Digital outputs	
Number of digital outputs	16; Parameterizable as DIQ
Short-circuit protection	Yes; per channel, electronic
• Response threshold, typ.	0.7 A
Limitation of inductive shutdown voltage to	2L+ (-50 V)
Switching capacity of the outputs	
• on lamp load, max.	5 W
Load resistance range	
• lower limit	48 Ω
• upper limit	4 kΩ
Output voltage	
• for signal "1", min.	L+ (-0.8 V)
Output current	
• for signal "1" rated value	0.5 A
• for signal "0" residual current, max.	0.5 mA
Switching frequency	
• with resistive load, max.	100 Hz
• with inductive load, max.	0.5 Hz
• on lamp load, max.	1 Hz
Total current of the outputs	
• Current per module, max.	4 A
Cable length	
• unshielded, max.	30 m

Article number	6ES7143-5AH00-0BL0
Encoder	
Connectable encoders	
• 2-wire sensor	Yes
– permissible quiescent current (2-wire sensor), max.	1.5 mA
IO-Link	
IO-Link protocol 1.1	Yes
Transmission rate	38.4 kBd (COM2)
Cycle time, min.	3 ms
Size of process data, input per module	2 byte
Size of process data, output per module	2 byte
Supported IO-Link profiles	common profile
Cable length unshielded, max.	20 m
Connection of IO-Link devices	
• Port type B	Yes
Interrupts/diagnostics/status information	
Substitute values connectable	Yes; channel by channel, parameterizable
Alarms	
• Diagnostic alarm	Yes; Parameterizable
Diagnoses	
• Short-circuit	Yes; outputs to ground; encoder supply to ground; module by module
Diagnostics indication LED	
• Channel status display	Yes; green LED
• for module diagnostics	Yes; green/red LED
• For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
• between the channels	No
• between the channels and the power supply of the electronics	Yes
Isolation	
Isolation tested with	707 V DC (type test)
Standards, approvals, certificates	
Suitable for safety-related tripping of standard modules	Yes; From FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SILCL according to IEC 62061	SILCL 2
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C

Article number	6ES7143-5AH00-0BL0
Connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pin, A-coded
Type of electrical connection for IO-Link	M12, 5-pin, A-coded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	157 g

Dimension drawing

The figure below shows the dimension drawing of the DIQ 16x24VDC/0,5A 8xM12 IO-Link digital input/digital output module in front and side view.

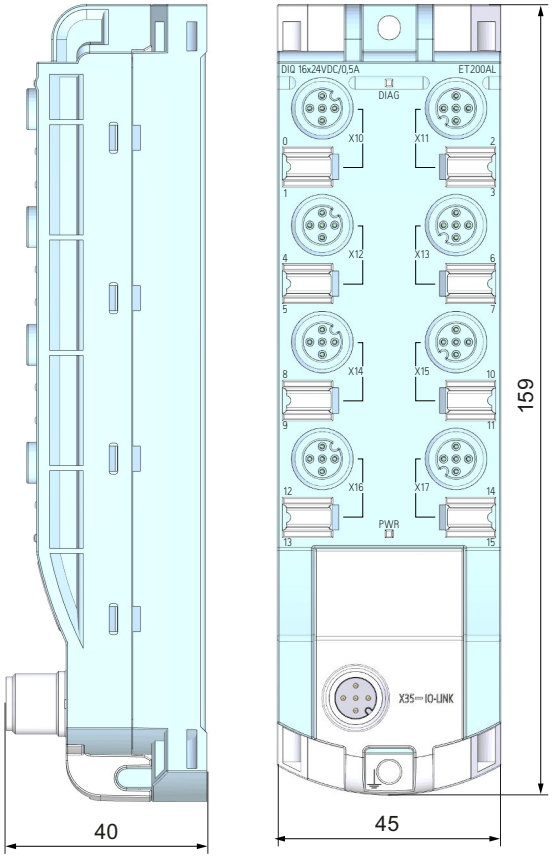


Figure 2-173 Dimension drawing

SIEMENS

SIMATIC

ET 200AL
Digital I/O module F-DI 4+F-DQ 2x24VDC/2A, 4xM12 (6ES7146-5FF00-0BA0)

Equipment Manual

Documentation guide 1

Product overview 2

Wiring 3

Parameters/address space 4

Applications of the F-I/O module 5

Interrupts/diagnostic messages/diagnostics 6

Technical specifications 7

Dimension drawing A

Response times B

Switching of loads C

V1.0, 03/2022
A5E51082342-AB

Preface

Purpose of the documentation

This manual supplements the *ET 200AL distributed I/O system system manual* (https://support.industry.siemens.com/cs/ww/en/view/89254965). Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present manual, the system manual and the function manuals enables you to commission the ET 200AL distributed I/O system.

⚠ WARNING

The *SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* in the current version is the authoritative source for functional safety-related information concerning configuring and programming.

Siemens identifies the *SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* as the authoritative and/or original source in the case of discrepancies between the manuals.

All warnings in the *SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* have to be observed. You can find the current version of the manual on the Internet (https://support.industry.siemens.com/cs/ww/en/view/54110126).

Conventions

Please observe notes marked as follows:

NOTE

Indicates important product information to which particular attention should be paid.

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are

available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/cert).

Table of contents

1 Documentation guide 6

2 Product overview 9

2.1 Properties 9

2.2 Operator controls and display elements 12

2.3 Fail-safe digital inputs 13

2.4 Fail-safe digital outputs 14

3 Wiring 15

3.1 Terminal and block diagram 15

3.2 Pin assignment 16

3.3 Connecting the M12 eCoding plug 18

4 Parameters/address space 20

4.1 Configuring module I/O properties 20

4.2 Parameters 21

4.3 Explanation of parameters 23

4.3.1 F-parameters 23

4.3.2 DI parameters 23

4.3.3 DQ parameters 28

4.4 Address space 32

5 Applications of the F-I/O module 34

5.1 Digital input applications 35

5.1.1 Applications 1 and 2: 1oo1 evaluation of single-channel sensors 37

5.1.2 Applications 3 and 4: 1oo2 evaluation of equivalent sensors 40

5.1.3 Applications 5 and 6: 1oo2 evaluation of a 3-wire, nonequivalent sensor circuit 42

5.1.4 Applications 7 and 8: 1oo2 evaluation of a 4-wire, nonequivalent sensor circuit 45

5.2 Digital output applications 48

5.2.1 Application 1: Wiring a directly-connected SIL-rated actuator 49

5.2.2 Application 2: Wiring external contactors: Separate P and M controlled contactors 49

5.2.3 Application 3: Wiring external contactors: Parallel-connected contactors between P and M 50

5.2.4 Application 4: Wiring external contactors: Separate output channels for each contactor 51

5.3 Examples of application modes for the F-DI 4/F-DQ 2 Fail-Safe module 52

6 Interrupts/diagnostic messages/diagnostics 57
6.1 Reactions to faults 57
6.2 Fault diagnostics overview 60
6.3 Diagnostics performed at startup 61
6.4 Diagnostics by LED display 62
6.4.1 Status and error displays 62
6.5 Fault types, causes, and corrective measures 65

7 Technical specifications 71
7.1 Specifications 71

A Dimension drawing 75
A.1 Dimension drawing 75

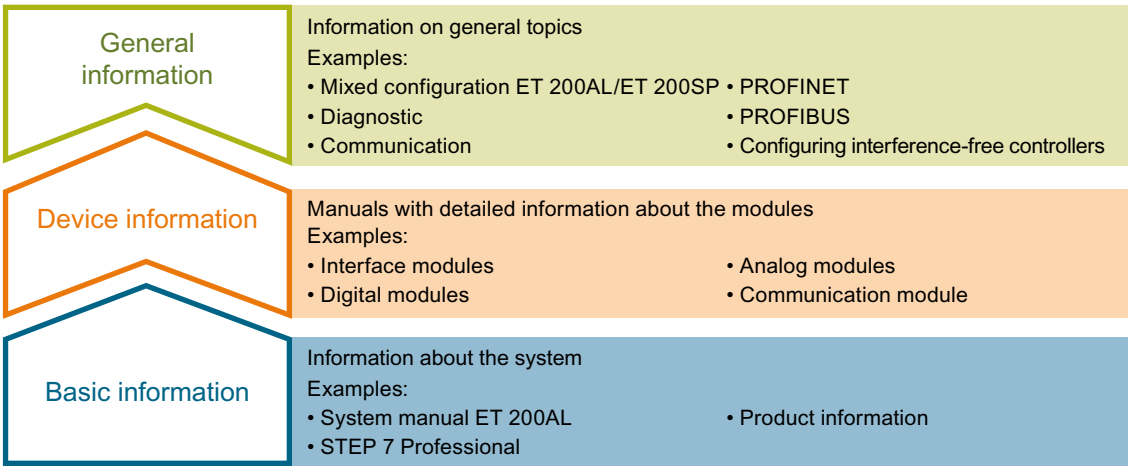
B Response times 76
B.1 Maximum response time 76
B.2 Response time parameters for the F-DI 4/F-DQ 2 digital inputs 77
B.3 Response time parameters for the F-DI 4/F-DQ 2 digital outputs 78

C Switching of loads 79
C.1 Connecting capacitive loads 79
C.2 Switching of inductive loads 80

Documentation guide

1

The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.



Basic information

The *System Manual* and *Getting Started* describe in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system. The STEP 7 online help supports you in the configuration and programming.

Device information

Product manuals contain a compact description of the module-specific information, such as properties, terminal diagrams, characteristics and technical specifications.

General information

The function manuals contain detailed descriptions on general topics regarding the SIMATIC ET 200AL distributed I/O system, e.g. diagnostics, communication, Motion Control, Web server.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742667).

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet (https://support.industry.siemens.com/cs/ww/en/view/95242965).

"mySupport"

With "mySupport", your personal workspace, you make the best out of your Industry Online Support.

In "mySupport", you can save filters, favorites and tags, request CAx data and compile your personal library in the Documentation area. In addition, your data is already filled out in support requests and you can get an overview of your current requests at any time.

You must register once to use the full functionality of "mySupport".

You can find "mySupport" on the Internet (https://support.industry.siemens.com/cs/ww/en/my).

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You will find the application examples on the Internet (https://support.industry.siemens.com/sc/ww/en/sc/2054).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).

This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.

With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (https://support.industry.siemens.com/cs/us/en/view/109767888).

Safety technology support

Siemens provides the following online comprehensive support for your use of safety technology:

- Safety Evaluation Tool - assists you in determining required safety levels
- Functional Examples - guides you in your safety applications
- Siemens training (SITRAIN) classes - offers training in safety standards and products
- SIMATIC STEP 7 Safety Advance F-Execution Times, F-Runtimes, F-Monitoring and Reaction Times Excel file (RT_calculator) - assists you in calculating your maximum system response time

You can find the Safety Evaluation Tool on the Internet (http://www.siemens.com/safety-evaluation-tool).

You can find Functional Examples on the Internet (http://www.siemens.com/safety-functional-examples).

You can find SITRAIN classes on the Internet (http://www.siemens.com/sitrain-safetyintegrated).

You can find the RT_calculator on the Internet (http://support.automation.siemens.com/WW/view/en/49368678/133100).

Product overview

2

2.1 Properties

Article Number

6ES7146-5FF00-0BA0

View of the Module

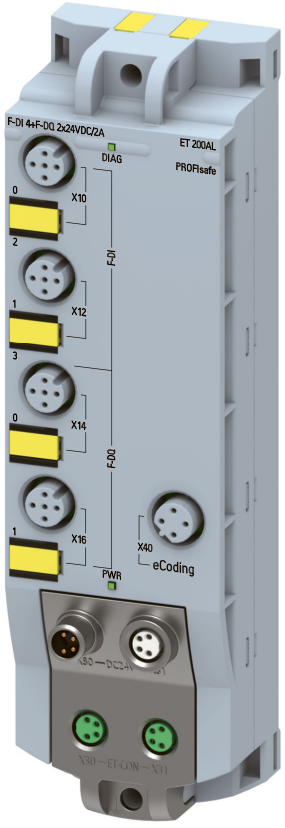


Figure 2-174 View of the F-DI 4+F-DQ 2x24VDC/2A, 4xM12 Fail-Safe I/O module

Properties

The module has the following technical properties:

- Four fail-safe digital inputs and two fail-safe digital outputs (M12 sockets for connection of sensors and actuators)
- One eCoding connection (M12 socket for eCoding plug)
- Two power ports, infeed and loop-through, which contain both logic and input power (1L+) and output power (2L+) (M8 module supply voltage ports)
- Two ET-Connection communication ports (M8 sockets)
- Fail-safe digital inputs:
  - 24 V DC rated
  - Two short-circuit proof sensor supplies
  - External sensor supply possible
  - Configurable diagnostics can be set for each channel
  - Configurable input delay
  - Suitable for switches and 3/4-wire proximity switches
- Fail-safe digital outputs:
  - Rated load voltage 24 V DC
  - Suitable for solenoid valves, DC contactors, and indicator lights
  - Output current per output 2.0 A
  - Configurable diagnostics can be set for each channel
- Dimensions 45 x 159 mm

The module supports the following functions:

- Firmware update
- Identification and maintenance data I&M0 to I&M3
- Value status (Quality Information)

The module has the following maximum achievable safety class in safety mode:

Maximum achievable safety class in safety mode	**1-channel input**	**2-channel input**	**Output channel**
Performance level according to EN ISO 13849-1	Cat. 3, PL d	Cat. 4, PL e	Cat. 4, PL e
SIL according to IEC 61508	SIL 2	SIL 3	SIL 3

Accessories

The following components are included in the module package:

- Identification labels (Yellow)
- eCoding plug (Used to store the application's PROFIsafe addresses)

Other components

The following components can be ordered as a spare part:

- Identification labels (Yellow)
- eCoding plug

The following components can be ordered as accessories:

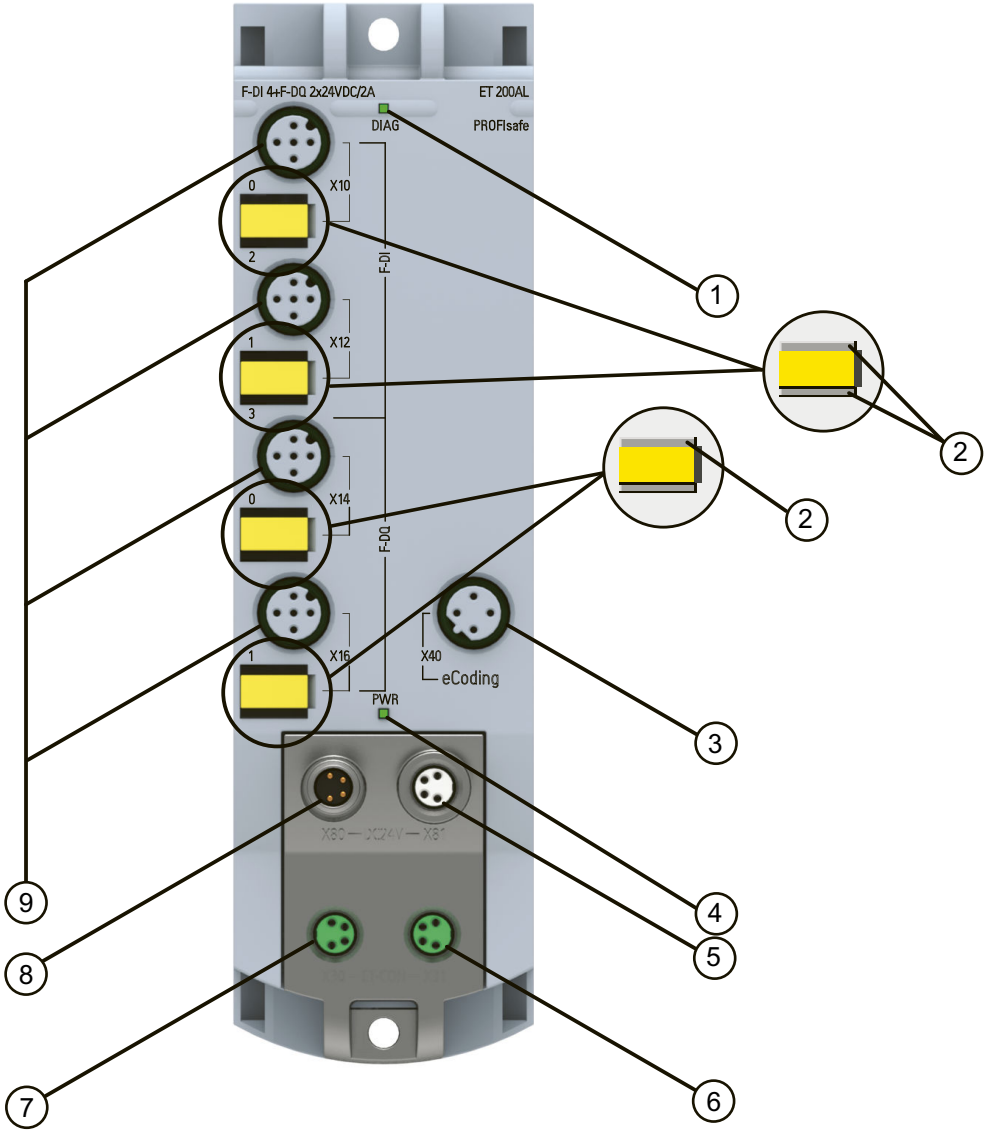
- Connectors
- Cables
- Stripping Tool for ET-Connection
- M8 sealing cap
- M12 sealing cap

See also

You can find more information on accessories in "Accessories/spare parts" in the *ET 200AL distributed I/O system system manual* (https://support.industry.siemens.com/cs/ww/en/view/89254965).

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the F-DI 4/F-DQ 2 Fail-Safe module:



① DIAG: LED display for the diagnostic status
② LED displays for the channel status
③ X40: eCoding plug connection
④ PWR: LED display for load voltage 2L+
⑤ X81: Socket for loop-through of the supply voltage (POWER output)
⑥ X31: Socket for ET-Connection OUT
⑦ X30: Socket for ET-Connection IN
⑧ X80: Connector for infeed of the supply voltage (POWER input)
⑨ X10 to X16: Sockets for the input/output signals

Figure 2-175 Operator controls and display elements

2.3 Fail-safe digital inputs

The digital inputs of the F-DI 4/F-DQ 2 Fail-Safe module are rated for connection to 24 V DC sensors/switches and 3/4-wire proximity switches (for example, BEROs: Siemens line of no-touch sensors) and have an EN 61131-2 type 1 input rating.

The fail-safe module has two 0.5 A sensor supply outputs that can power external sensors (inputs). All 1oo1 and 1oo2 application modes, except the "1oo2, 2 channel 3-wire nonequivalent" application mode, use the V_{S1} sensor supply to provide power for channels 0 and 1, and the V_{S2} sensor supply to provide power for channels 2 and 3. The "1oo2, 2 channel 3-wire nonequivalent" application mode uses the V_{S1} sensor supply to provide power for all four inputs and does not use the V_{S2} sensor supply.

Inputs and test circuit

The fail-safe digital inputs consist of four input channels (F-DI x.0 to x.3). You can configure these channels as four one-out-of-one (1oo1) inputs (SIL 2/Cat. 3/PL d), two one-out-of-two (1oo2) inputs (SIL 3/Cat. 3 or Cat. 4/PL e), or combinations of 1oo1 and 1oo2 inputs.

Connections	Input channel pairs
X10	0 and 2
X12	1 and 3

The fail-safe digital inputs use two microcontrollers to implement the safety function. One microcontroller monitors inputs 0 and 1, and the other microcontroller monitors inputs 2 and 3. The corresponding channels (0, 2) and (1, 3) form a 1oo2 channel group. The lower numbered channel of the group is called the primary input and the other channel is called the secondary input. The first of the two inputs in the channel group conveys the signal in a 1oo2 configuration. For example, if you wire F-DI 0.0 and F-DI 0.2 in a 1oo2 configuration and configure STEP 7 to use 1oo2 sensor evaluation, the signal state is reported at only the F-DI 0.0 input when you close or open the circuit for both.

When you configure a channel group as 1oo2, the two microcontrollers must sense the same input change within a configured time. Otherwise, the two microcontrollers detect a discrepancy error.

You can enable short-circuit testing if you use a sensor supply output to provide power to a sensor. The short-circuit test checks for shorts to 24 V DC by periodically pulsing the sensor output off and verifying that the associated input is off.

This short-circuit test also checks for shorts to the other circuit in "1oo2, 2 channel equivalent" and "1oo2, 2 channel 4-wire nonequivalent" application modes because the test pulses the two sensor outputs off at different times.

The microcontrollers provide internal test pulses to each other's process input circuits to verify that sensing electronics are responsive to both "1" and "0" inputs.

See also

Accessories for the ET200AL distributed I/O system (https://support.industry.siemens.com/cs/us/en/view/89254965)

2.4 Fail-safe digital outputs

The digital outputs of the F-DI 4/F-DQ 2 Fail-Safe module are for use in fail-safe applications and are suitable for various actuators such as the following:

- Solenoid valves
- DC contactors
- Indicator lights

The two digital outputs each have P- and M-switches that are rated to connect 24 V DC actuators with up to a 2.0 A rating. The two digital outputs use the load voltage 2L+ with a maximum current of 4.0 A. This means that the total current usage by the two digital outputs cannot exceed 3.96 A because the 2L+ supply uses about 40 mA.

Outputs

The fail-safe digital outputs consist of two output channels (F-DQ x.0 to x.1). You can use each output for SIL 3 applications.

Connections	Output channel
X14	0
X16	1

Each output consists of two switches:

- A P-switch connects 24 V DC positive (L+) to the load.
- An M-switch connects the load to M or 24 V DC return.

Both switches must be ON for current to flow to the load.

The fail-safe digital outputs use two microcontrollers to implement the safety function. One microcontroller controls the P-switch while the other microcontroller controls the M-switch. Status of the P-switch is fed back to the other microcontroller (the one that controls the M-switch). Likewise, status of the M-switch is fed back to the other microcontroller (the one that controls the P-switch). The microcontrollers use the feedback to verify that the output switches are operating properly and in the commanded state.

You must configure a "Maximum readback time" that specifies the allowed delay for the output voltage to respond to the switch change.

The fail-safe digital outputs regularly test each P- and M-switch to verify that each switch is still functional and under independent control. Your configured "Maximum readback time" also sets the duration of the "OFF" test pulse. You must configure a "Maximum readback time switch on test" which sets the duration of the "ON" test pulse. Choose these durations short enough to not affect your load.

The module can detect a broken wire or missing load when the output PV is OFF. If the broken wire diagnostic is enabled, then the load must be wired in the PM configuration or a broken wire diagnostic will occur (see applications 1, 3 or 4 in section 5.2 Digital output applications (Page 48)).

Wiring

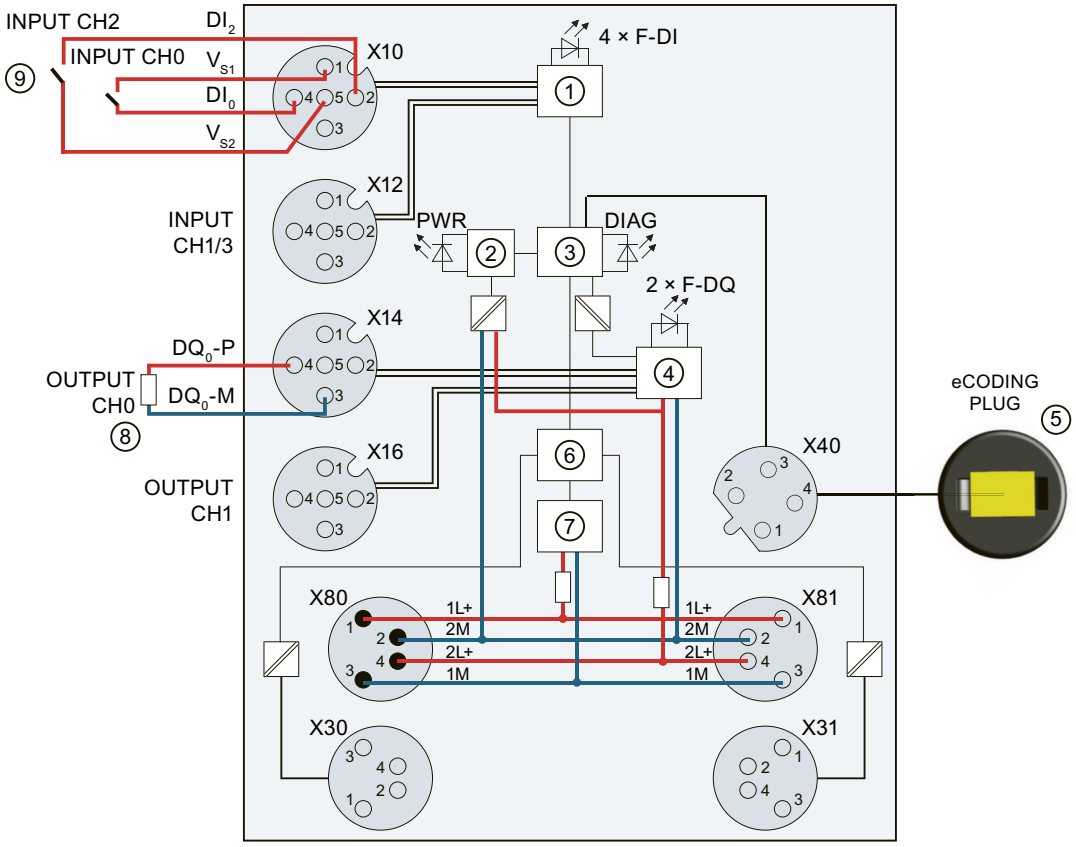
3

WARNING

You can come into contact with live electrical wires connected to the main power supply.
Death or serious personal injury and damage to machines and equipment may result if proper precautions are not taken.
Shut off the supply and load voltage before you wire the fail-safe module.

3.1 Terminal and block diagram

The following figure shows an example of the pin assignment of signal inputs with 4-wire connection as well as signal outputs:



①	F-DI circuit (1L+)	X40	eCoding socket
②	Diagnostic monitoring	X80	Infeed of supply voltages
③	Microcontrollers	X81	Loop-through of supply voltages
④	F-DQ circuit (2L+)	V_{Sn}	24 V sensor supplies
⑤	eCoding plug	1L+	Supply voltage 1L+

⑥	ET-Connection interface	1M	Ground 1M
⑦	Internal supply voltage	2L+	Load voltage 2L+
⑧	Outputs	2M	Ground 2M
⑨	Inputs: Configured as 1oo1 sensor using internal sensor supply	DI_n	Input signal
X10, X12	F-DI input channels	DQ_n-P	Output signal, P-switch
X14, X16	F-DQ output channels	DQ_n-M	Output signal, M-switch
X30	Infeed of the ET-Connection	DIAG	LED diagnostic status (red/green)
X31	Loop-through of the ET-Connection	PWR	LED load voltage 2L+ status (green)

Figure 2-176 Terminal and block diagram

3.2 Pin assignment

NOTE

Color coding

The sockets for ET-Connection and the power supply of the modules are color-coded. These colors correspond to the colors of the offered cables.

Pin assignment of the sockets for fail-safe digital inputs/outputs

The tables below show the pin assignments of the four sockets for connection of the fail-safe digital inputs/outputs:

Table 2-380 Pin assignment for fail-safe digital input sockets

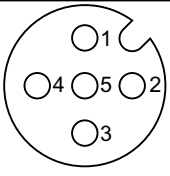
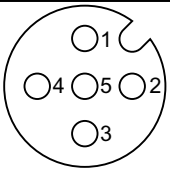
Pin	Assignment	Front view of the sockets
	X10 and X12 - sockets for fail-safe digital inputs	**X10, X12**
1	24 V DC sensor supply V_{S1}	
2	Input signal DI_2: Connector X10 Input signal DI_3: Connector X12	
3	Sensor supply ground 1M	
4	Input signal DI_0: Connector X10 Input signal DI_1: Connector X12	
5	24 V DC sensor supply V_{S2}	

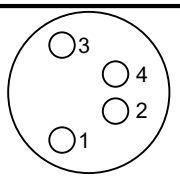
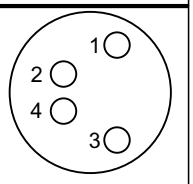
Table 2-381 Pin assignment for fail-safe digital output sockets

Pin	Assignment	Front view of the sockets
	X14 and X16 - sockets for fail-safe digital outputs	**X14, X16**
1	Unassigned	
2	Unassigned	
3	Output signal DQ_0-M: Connector X14 Output signal DQ_1-M: Connector X16	
4	Output signal DQ_0-P: Connector X14 Output signal DQ_1-P: Connector X16	
5	Functional earth FE	

Pin assignment of the sockets for ET-Connection

The table below shows the pin assignments of the two sockets for the connection of ET-Connection:

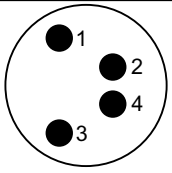
Table 2-382 Pin assignment for ET-Connection

Pin	Assignment		Assignment of the wire color of the bus cable for ET-Connection	Front view of the sockets	
	X30 socket (ET-Connection IN)	X31 socket (ET-Connection OUT)		X30	X31
1	TXP	RXP	Yellow		
2	RXP	TXP	White		
3	RXN	TXN	Blue		
4	TXN	RXN	Orange		
Shielding	Functional earth FE		-		

Pin assignment of the connector for infeed of the supply voltage

The table below shows the pin assignment of the connector for infeed of the supply voltage:

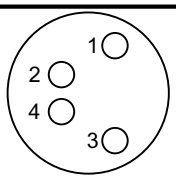
Table 2-383 Pin assignment of the supply voltage connector

Pin	Assignment	Assignment of the wire color of the power line cable	Front view of the connector
	X80 connector (POWER input)		
1	Supply voltage 1L+	Brown	
2	Ground 2M	White	
3	Ground 1M	Blue	
4	Load voltage 2L+	Black	

Pin assignment of the socket for loop-through of the supply voltage

The table below shows the pin assignment of the socket for loop-through of the supply voltage:

Table 2-384 Pin assignment of the supply voltage socket

Pin	Assignment X81 socket (POWER output)	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+	Brown	
2	Ground 2M	White	
3	Ground 1M	Blue	
4	Load voltage 2L+	Black	

NOTE

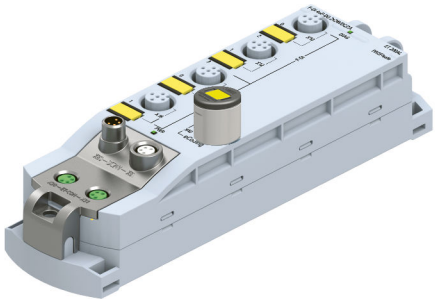
ET-Connection/supply voltage

Installing a supply voltage cable in an ET-connection socket or an ET-connection cable in the supply voltage loop-through socket can destroy the module.

Observe the correct wiring of the M8 sockets for ET-Connection and the supply voltage.

3.3 Connecting the M12 eCoding plug

The eCoding plug (6ES7194-6KB01-0AA0) stores the PROFIsafe addresses that you assign to the F-DI 4/F-DQ 2 Fail-Safe module:

eCoding Plug (side view)	F-DI 4/F-DQ 2 with eCoding Plug Attached (front view)	F-DI 4/F-DQ 2 with eCoding Plug Attached (side view)
		

The eCoding plug stores the following information:

- PROFIsafe source address
- PROFIsafe destination address
- Address validity information

The eCoding plug occupies the X40 M12 socket, utilizing a B-coded plug. You use the eCoding plug to facilitate module replacement.

The eCoding plug stores assigned PROFIsafe source and destination addresses. The "Assign PROFIsafe address option" is selected in STEP 7 during the F-DI 4/F-DQ 2 Fail-Safe module set-up. The module checks the PROFIsafe addresses stored in the eCoding plug against the PROFIsafe reference addresses provided to the module during start-up parameterization.

Protection mechanisms prevent you from damaging the eCoding plug or an I/O channel due to attempted plugging of the eCoding plug into an I/O M12 socket or plugging of an I/O M12 cable into the X40 socket.

Install the eCoding plug into the M12 socket at X40 with a torque of 1 Nm. Do not overtighten the eCoding plug as it could damage the threading.

⚠ WARNING

If you remove/insert the eCoding plug with the power connected, this can lead to undefined states in your system.

Death or serious personal injury and damage to the fail-safe module and associated machines/equipment may result if proper precautions are not taken.

Only remove or replace the eCoding plug when the power is disconnected. Always comply with the required standards and safety guidelines when configuring a system.

NOTE

When replacing the F-DI 4/F-DQ 2 Fail-Safe module, transfer the eCoding plug of the failed module to the replacement module to retain the PROFIsafe addresses stored in the eCoding plug. Otherwise, use STEP 7 to configure the PROFIsafe address in the replacement module. Ensure that the eCoding plug is not accidentally inserted in a module other than the intended F-DI 4/F-DQ 2 Fail-Safe module.

4 Parameters/address space

All connected fail-safe I/O must have their operating properties configured by the STEP 7 Safety configuration software. You have the responsibility to ensure that no unconfigured modules are connected in a fail-safe automation system.

F-Parameters

You must assign the PROFIsafe addresses (F-destination address together with F-source address) to the F-module before you put it into operation as follows:

- You define the F-source address using the "Central F-source addresses" parameter in the F-CPU.
- An F-destination address unique throughout the project's hardware configuration is automatically assigned for each F-module. You can manually change the F-destination addresses assigned in the hardware configuration.

You can find further information on F-parameters such as the F-monitoring time, the PROFIsafe address assignment (F-source address, F-destination address), F-parameter signature (with or without addresses) and the F-I/O DB in the *SIMATIC, Industrial Software, SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* on the Internet (https://support.industry.siemens.com/cs/ww/en/view/54110126).

4.1 Configuring module I/O properties

To configure fail-safe module I/O properties, follow these steps:

1. Select the image of a fail-safe I/O device (on the Device view or Device overview) and view the module's "Properties" tab.
2. On the "Properties" view, select the "General" tab.
3. Select a property category in the left-side property tree and then set values in the right-side property fields.
4. A successful compile and download of your hardware configuration to one of the following CPUs automatically puts your new configuration settings in the I/O modules:
   - ET 200pro F
   - ET 200SP F
   - S7-1200 F
   - S7-1500 F
   - Prior generation S7-300 F and S7-400 F

4.2 Parameters

The following table shows the parameters for the F-DI 4/F-DQ 2 Fail-Safe module:

Channel	Value range	Default	Parameter reassignment in RUN	Scope
F-parameters				
Manual assignment of F-monitoring time	• disable • enable	disable	no	Module
F-monitoring time	1 to 65535 ms	150 ms	no	Module
F-source address	1 to 65534	1 (always disabled)	no	Module
F-destination address	1 to 65534	65534 (always enabled)	no	Module
F-parameter signature (with addresses)	0 to 65535	always disabled	no	Module
F-parameter signature (without addresses)	0 to 65535	always disabled	no	Module
Behavior after channel fault	• Passivate channel • Passivate entire module	Passivate channel (always enabled)	no	Module
Reintegration after channel fault	• Adjustable • All channels automatically • All channels manually	All channels manually (always enabled)	no	Module
F-I/O DB manual number assignment	• disable • enable	disable	no	Module
F-I/O DB number	• Fixed value, if DB manual number assignment is disabled • Value can be edited by user, if DB manual number assignment is enabled	Fixed value	no	Module
F-I/O DB name	-	always disabled	no	Module
DI parameters				
Sensor supply				
Short-circuit test	• disable • enable	enable	no	Channel
Interval for short-circuit test	• 12.8 ms • 25.6 ms • 51.2 ms • 102.4 ms • 204.8 ms • 409.6 ms • 819.2 ms	25.6 ms	no	Channel
Duration of short-circuit test	• 1.6 ms • 3.2 ms • 6.4 ms • 12.8 ms	1.6 ms	no	Channel

Channel	Value range	Default	Parameter reassignment in RUN	Scope
Channel n, n+2				
Sensor evaluation	• 1oo1 evaluation • 1oo2 evaluation: – 2 channel equivalent – 2 channel - 3 wire non-equivalent – 2 channel - 4 wire non-equivalent	1oo2 evaluation, 2 channel equivalent	no	Channel
Discrepancy behavior	• Supply value 0 • Supply last valid value	Supply value 0	no	Channel
Discrepancy time	5 ms to 30 s	5 ms	no	Channel
Reintegration after discrepancy error	• Test 0-Signal not necessary • Test 0-Signal necessary	Test 0-Signal not necessary	no	Channel
Channel n				
Activated	• disable • enable	enable	no	Channel
Input filters	• 0.8 ms • 1.6 ms • 3.2 ms • 6.4 ms • 12.8 ms	6.4 ms	no	Channel
Channel failure acknowledge	• Automatic • Manual	Manual	no	Channel
Sensor supply	• Internal • External	Internal	no	Channel
DQ parameters				
Maximum test period	• 100 s • 1000 s	1000 s	no	Channel
Channel n				
Wire break	• disable • enable	disable	no	Channel
Activated	• disable • enable	enable	no	Channel
Channel failure acknowledge	• Automatic • Manual	Manual	no	Channel
Maximum readback time	1.0 ms to 400.0 ms	2.0 ms	no	Channel
Maximum readback time switch on test	0.5 ms to 5.0 ms	1.0 ms	no	Channel
Disable dark test (max. SIL 2, Cat. 3, PL d)	• dark test is disabled • dark test is enabled	dark test is enabled	no	Channel

4.3 Explanation of parameters

4.3.1 F-parameters

Information on F-parameters is available in the *SIMATIC Safety – Configuring and Programming* manual (https://support.industry.siemens.com/cs/us/en/view/54110126).

Behavior after channel fault

Use this parameter to specify whether the entire F-module is passivated or just the faulty channel(s) in the event of channel faults:

- "Passivate the entire module"
- "Passivate channel"

Reintegration after channel fault

Use this parameter to select how the channels of the fail-safe module are reintegrated after a fault.

Use in S7-300/400 F-CPUs
This parameter is always set to "Adjustable" when you use the fail-safe module in S7- 300/400 F-CPUs. You make the required setting in the F-I/O DB of the fail-safe module.

Use in ET 200pro, ET 200SP and S7-1200/1500 F-CPUs
When using the fail-safe module in ET 200pro, ET 200SP and S7-1200/1500 F-CPUs, you set this parameter in the STEP 7 dialog of the fail-safe module:

- "Adjustable"
- "All channels automatically"
- "All channels manually"

If you have set the "Behavior after channel fault" parameter to "Passivate channel", you enable individual setting of the reintegration type per channel with the parameter assignment "Adjustable". The reintegration type of the respective channel is specified with the "Channel failure acknowledge" channel parameter.

If you have set the "Behavior after channel fault" parameter to "Passivate the entire module", you can only select the same reintegration type for all channels.

4.3.2 DI parameters

Short-circuit test

You can enable the short-circuit detection for the channels of the F-module for which "Internal sensor supply" is set.

The short-circuit test is only useful if you are using simple switches that do not have their own power supply. For switches with a power supply, for example, 3/4-wire proximity switches, a short-circuit test is not possible.

The short-circuit test switches off the sensor supply briefly. The length of the deactivation period is equivalent to the configured "Duration of short-circuit test".

If a short-circuit is detected, the fault is reported to the F-CPU and the input is passivated.

The following short-circuits are detected:

- Short-circuit of input to L+
- Short-circuit of the input to another channel when it has a 1 signal
- Short-circuit between the input and sensor supply of another channel
- Short-circuit between the sensor supply and the sensor supply of another channel

If the short-circuit test is disabled, you must make your wiring short-circuit and cross-circuit proof or select a connection type (discrepancy, nonequivalent) which also detects the cross circuits using discrepancy.

During the execution time (duration of short-circuit test + startup time of sensor after the short-circuit test) of the short-circuit test, the last valid value of the input before the start of the short circuit test is passed to the F-CPU. The activation of the short-circuit test thus affects the response time of the respective channel or channel pair.

Discrepancy time variation with short-circuit test
If your process input changes near when a short-circuit test is in progress, a discrepancy is detected in less time than your configured discrepancy time.

Elements of discrepancy time variations are defined as follows:

- **Tdisc** = configured discrepancy time
- **Tsct** = configured short circuit test duration
- **Tfilter** = configured input filter time
- **Tda** = actual discrepancy time, time between process signal changes that can be detected as a fault

The range of detected discrepancy time is as follows:

- **If Tfilter < Tsct**: {Tdisc - (Tfilter + Tsct)} <= Tda <= Tdisc
- **If Tfilter >= Tsct**: {Tdisc - (2 x Tsct)} <= Tda <= Tdisc

Your configured discrepancy time should account for this variation to avoid unexpected passivations.

Interval for short-circuit test

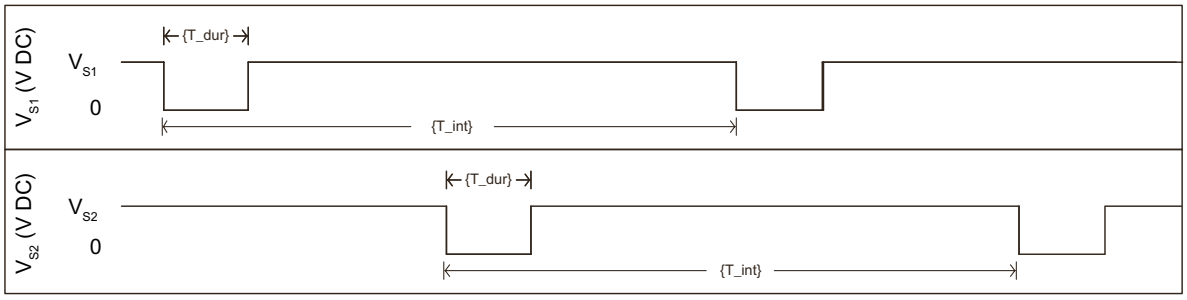
You can specify how often the short-circuit test is executed (Interval) when the "Short-circuit test" check box is selected. The interval defines the period of time between two consecutive sensor supply OFF test pulses.

This value is the time between the OFF pulses of the sensor supply.

NOTE

The interval between pulses must be a minimum of eight times the duration of a pulse.

Short-circuit testing is performed on V_{S1} and V_{S2} independently, allowing module circuitry to detect shorts between the two sensor supplies as follows:



V_{Sn} V_{S1} or V_{S2} sensor supplies (V DC)
T_int Short-circuit test interval (time period) between the OFF pulses of the sensor supply (ms)
T_dur Short-circuit test OFF pulse time duration (ms)

Duration of short-circuit test

You can specify the duration of the test pulse applied to the sensor supply when the "Short-circuit test" check box is selected.

This value is the time that the power supply remains off during the test. The short-circuit test OFF pulse must be long enough for the external sensors and wiring to respond and present a "0" to the inputs.

Sensor evaluation

You can assign whether “channel n” input operates individually (1oo1) or is paired with its companion channel "n+2" input (1oo2).

Defines signal evaluation and wiring definitions. These selections correspond with the various application mode wiring examples.

1oo1 evaluation: One sensor is connected to the module on a single channel.

1oo2 evaluation: Two input channels are occupied by either:

- **2 channel equivalent** (with equivalent signals): One two-channel equivalent sensor or two single-channel equivalent sensors are connected to the two channels, in a channel pair.
- **2 channel - 3 wire nonequivalent**: One two-channel nonequivalent sensor is connected to the two channels, in a channel pair.
- **2 channel - 4 wire nonequivalent** One two-channel nonequivalent sensor or two single-channel nonequivalent sensors are connected to the two channels, in a channel pair.

If 1oo2 is selected, you must assign the discrepancy properties.

Refer to "Digital input applications (Page 35)" for illustrations of connection modes.

When you select the channel group as 1oo2, STEP 7 (TIA Portal) enables the parameters in the first channel of the group and completely disables the parameters in the second channel of the group. The second channel derives its parameter values from the first channel's parameter values. When you select the channel group as 1oo1, STEP 7 (TIA Portal) enables all of the parameters in both channels.

NOTE

Safety program access to 1oo2 input data
For 1oo2 evaluation, two paired input channels (for example, F-DI 0 and F-DI 2) are connected to one or two sensors. The F-DI performs the discrepancy analysis and sends the result to the safety program, at the input address of the low-numbered channel of the pair (F-DI 0, in the example).

Discrepancy behavior

A 1oo2 input configuration allows a logical difference between the two signals, without error, for the configured discrepancy time. You assign the value that is supplied to the safety program in the F-CPU during a discrepancy between two relevant input channels, which means while discrepancy time is running. You assign the discrepancy behavior as follows:

- "Supply last valid value"
- "Supply value 0"

NOTE

Sensor-actuator response time is increased when you add more input discrepancy time
The discrepancy time adds directly to the maximum response time of a 1oo2 evaluation if the two signals do not agree in logical state. If you select the "Supply value 0" option, then the F-DI does not delay a transition from "1" to "0" but can delay the transition from "0" to "1". If you select the "Supply last valid value" option, then the F-DI can delay both transitions from "1" to "0' and "0" to "1". The discrepancy time is influenced by sensor specifications, installation tolerances, and wiring. For best response time, select the smallest discrepancy time that provides reliable normal operation. Refer to "Response times (Page 76)" for further information.

Discrepancy time

The two signals in a 1oo2 input configuration will not change exactly at the same time, due to differences in sensors, contacts, and wiring. You can configure a maximum expected duration for a mismatch between signals during transition.

Reintegration after discrepancy error

You can assign whether a zero state must be detected on both 1oo2 inputs before a previously declared discrepancy can be cleared.

"Test 0-signal necessary"
If you have assigned "Test 0-signal necessary", a discrepancy error is not regarded as corrected until a 0-signal is present at both of the relevant input channels for a duration of at least 100 ms.

If you are using nonequivalent sensors, which means you have set "Sensor evaluation" to "1oo2 evaluation, nonequivalent", a 0-signal must be present again at the low order channel of the channel pair.

"Test 0-signal not necessary"
If you have assigned "Test 0-Signal not necessary", a discrepancy error is regarded as corrected when a discrepancy no longer exists between the two relevant input channels.

Activated

You can enable the corresponding channel for signal processing in the safety program.

If you disable a channel, channel diagnostics are no longer reported to the F-CPU for the deactivated channel. Whenever you disable all output channels, you do not have to power 2L+ and 2L+ undervoltage reporting is suspended.

Input filters

The module filters the digital inputs to remove contact bounce and short duration noise. This parameter assigns the duration of the filter time.

Channel failure acknowledge

Controls whether the channel is automatically reintegrated after a fault clears or requires an acknowledgement (manual) in the user program. Refer to "Reactions to faults (Page 57)" for the reintegration procedure.

NOTE

The configuration of the "F-Parameters": "Reintegration after channel fault" parameter can determine your ability to modify the "Channel failure acknowledge" parameter's selection.

Sensor supply

You can assign whether to supply 24 V DC power to sensors from the module's integrated sensor supply (internal) or from an external power supply (external).

Short-circuit tests are not performed for any channel where external power is selected.

4.3.3 DQ parameters

Maximum test period

You can assign the time interval between bit pattern tests for F-DQ DC output faults to a value of either 100 seconds or 1000 seconds.

Functional bit pattern tests are applied to the output switches. These tests detect faulted P- or M- output switches and wiring faults. Short circuits to other signals or power rails can be detected. Open circuits between the wiring terminals and the load are not detected.

If an error is detected on a channel, the test interval is shortened to 60 seconds. If an error is no longer detected on any output channel, the configured test interval is used again.

A persistent fault is reported to the fail-safe CPU and the affected channels are passivated.

Wire break

You can enable or disable wire break testing. Wire break is only detected when the channel is in the OFF state (process value is "0").

Activated

You can enable the corresponding channel for signal processing in the safety program.

If you disable a channel, channel diagnostics are no longer reported to the F-CPU for the deactivated channel.

NOTE

Whenever you disable all output channels, you do not have to power 2L+ and 2L+ undervoltage reporting is suspended.

Channel failure acknowledge

Controls whether the channel is automatically reintegrated after a fault clears or requires an acknowledgement (manual) in the user program. Refer to "Reactions to faults (Page 57)" for the reintegration procedure.

NOTE

The configuration of the "F-Parameters": "Reintegration after channel fault" parameter can determine your ability to modify the "Channel failure acknowledge" parameter's selection.

Maximum readback time

The maximum readback time is a user-configured parameter that assigns the maximum time allowed for an output to reach the new state (ON or OFF) due to a process value change without generating an error. Also, this is the maximum width of a diagnostic test pulse applied during the bit pattern test to verify that an output can be turned OFF while it is in the ON state. The time of the OFF pulse should be as long as possible, but short enough so that the actuator cannot react.

The "Maximum readback time" parameter allows you to set the maximum time for verification that the channel's output switch states are as expected after a process value change.

If the expected output switch states (as reported by P-readback and M-readback signals) are not reached upon expiration of the "Maximum readback time", the output channel is passivated.

No new process values are switched to the output channels while a test pattern is applied to the outputs. This means that a higher "Maximum readback time" increases the response time of the F-module.

⚠ WARNING

Short-circuit (cross-circuit) detection may not be possible for high frequency signals
Through the configured "Maximum readback time", short-circuits (cross-circuits) to a signal with a frequency greater than 1/(2 x configured "Maximum readback time") Hz cannot be detected (50:50 sampling ratio).
You must take this into consideration for your application and respective requirements of your product standards.
Short-circuits (cross-circuits) to an output of the same module are recognized regardless of the frequency of the output channel.
You can adjust the maximum readback time to change the frequency of the signal that can be detected.

The parameter also effects the short-circuit detection (cross-circuit) with a "1" signal when the output signal is changed from "1" to "0" with the safety program.

Setting the parameter "Maximum readback time"

Because the fault response time is extended by the configured maximum readback time, we recommend that you set the "Maximum readback time" as low as possible, but high enough that the output channel is not passivated.

You determine the readback time required for your actuator with the diagram in "Connecting capacitive loads (Page 79)".

If the capacitance of the actuator is not known, it may be necessary for you to determine the value for the "Maximum readback time" by trial and error. This may also be necessary due to the part variances in the actuator or external influences.

Proceed as follows:

- Set the "Maximum readback time" so that the output channel can be read back correctly but your actuator does not respond yet.
- For verification, use the process value "0" with a minimum duration that corresponds to the "maximum test period" parameter. Execute a process value change from "1" to "0".
- If the output channel is passivated, the "Maximum readback time" is too small for the connected capacitive load. The discharge cannot take place within the configured "Maximum readback time". Increase the "Maximum readback time".

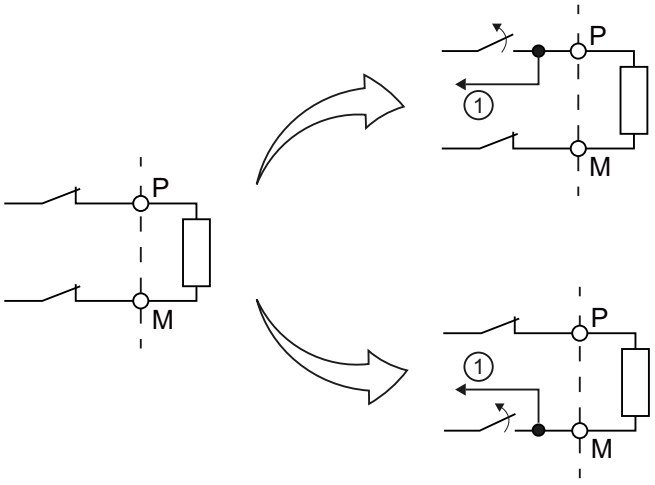
If you have set the "Maximum readback time" to the maximum value of 400 ms and there is still a passivation of the output channel, there is either an external fault or the connected capacitance is outside the permitted range.

Dark test

Dark tests are switch-off tests which occur during an output bit-pattern test sequence.

When dark test is disabled on an output channel, the parameter "Maximum readback time" is only relevant for the process value change.

For a dark test, one of the output channel's switches is briefly turned OFF while the output channel is active (output signal "1"). As a result, current flow through the output is interrupted for a short time. A sufficiently slow actuator does not respond to this and remains switched on.



① Readback

Figure 2-177 Functional principle of the dark test (PM switching)

Test pulses of the dark test

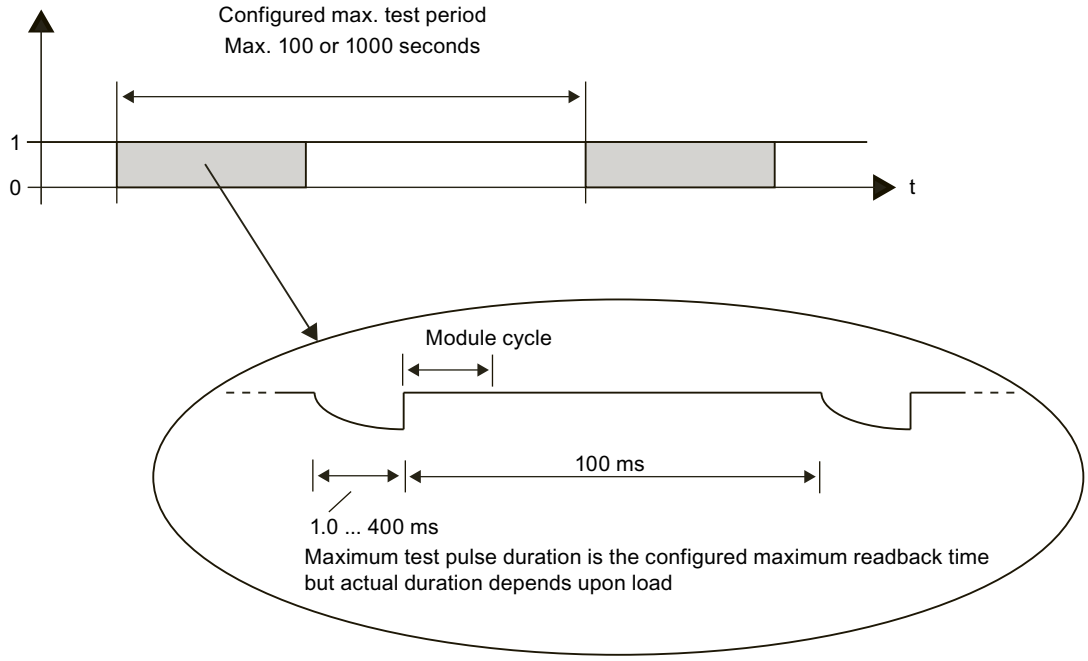


Figure 2-178 Test pulses of the dark test

You configure the time between output bit pattern test sequences to either 100 or 1000 seconds. Each output bit pattern test sequence includes multiple test pulses. The interval between two test pulses is at least 100 ms.

Maximum readback time switch on test

You can configure the maximum readback time switch on test parameter to assign the maximum time for which the P-switch or the M-switch of a channel that is currently in OFF state can be switched ON during a bit pattern test step. This action tests the P- and M-switches on a channel such that only one switch is turned on at a time. Unless there is a fault in the system (for example, actuator shorted to ground), the actuator is not energized during either the P- or M-switch on tests. Under single fault conditions (either internal or external to the module), test pulses applied to either the P- or the M-switch of channels in the OFF state can repeatedly energize the actuator. You must select the parameter so that the duration of such pulses is too short to cause the actuator to react and, therefore, cannot have a hazardous effect on the equipment under control.

Disable dark test (max. SIL 2, Cat. 3, PL d)

You can select the check box to disable channel dark testing.

To prevent an unwanted reaction of the actuator to a dark test, you can disable the dark test at the F-module output. An unwanted reaction can be for example, the brief de-energizing of a magnetic drive.

A capacitive load that does not meet the load curve (see "Switching of loads (Page 79)") can result in a passivation of the output in case of a process value change or switch-on test, even if the dark test is disabled.

You can only reach up to SIL 2/Cat. 3/PL d with the dark test disabled.

⚠ WARNING

Loss of SIL 2/Cat. 3/PL d rating, loss of output control due to potential undetected faults
With the dark test disabled, an output that is turned on for more than 1 year may not be able to be turned off.
SIL 2/Cat. 3/PL d requires that there is a signal change from "1" to "0" at the corresponding output at least once a year.
Ensure the "0" signal has a duration of at least 2 seconds. It is not enough to simply turn off the supply or load voltage of the F-module and turn it on again.

⚠ WARNING

Loss of cross-circuit detection between channels
When you use the function "Disable dark test", cross-circuits between channels with "1" signal are not detected.
You must take this into consideration for your application and respective requirements of your product standards.
You must also take into consideration the respective requirements of your product standards regarding error detection time.

4.4 Address space

NOTE

The F-DI 4/F-DQ 2 Fail-Safe module uses more I and Q memory than required for the physical number of inputs and outputs on the module. The extra bytes carry the PROFIsafe safety status and data integrity information. The number of input (I) bytes and output (Q) bytes that the F-DI 4/F-DQ 2 Fail-Safe module requires depends upon which PROFIsafe profile your fail-safe CPU uses.

Module	PROFIsafe profile	Input (I) bytes required	Output (Q) bytes required
F-DI 4+F-DQ 2x24VDC/2A, 4xM12	V2.4 (with S7-300/S7-400)	7	5
	V2.6 (with ET 200pro, ET 200SP and S7-1200/1500)	8	6

The figure below shows the assignment of the address space for the F-DI 4/F-DQ 2 Fail-Safe module with value status (Quality Information (QI)).

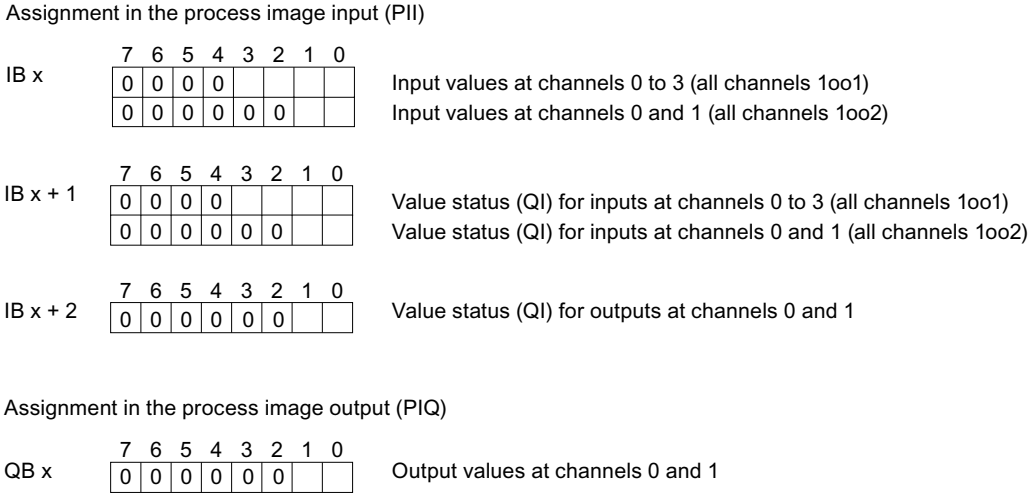


Figure 2-179 Address space

Evaluating the value status

The value status bits provide information regarding the validity of the digital values or channel status:

- Bit = 1: Corresponding process value is valid
- Bit = 0: Channel is passivated

Applications of the F-I/O module

5

The PLC system has an extremely low failure rate and therefore contributes only a small part of the total probability of dangerous failure of an automated system. The probability of dangerous failures of the sensors and actuators is typically far larger than the probability of dangerous failure per hour (PFH)/probability of dangerous failure on demand (PFD) of the PLC system. Estimates for quantitative safety properties like PFD and PFH are calculated using the following methods:

- standard data tables
- calculation methods according to international standards which include the following standards:
  - IEC 61508
  - ISO 13849
  - IEC 61131-6

The values are based on the following assumptions:

- continuous full nominal load
- nominal voltage
- equipment ambient temperature of 55 °C

Faults in the wiring system can also be a substantial contributor to failures.

To achieve a targeted level of safety performance for each safety function, perform these actions:

- Choose an appropriate architecture.
- Choose sensors and actuators that are appropriately rated.
- Provide a safety program that meets the requirements of the safety function.
- Provide diagnostics and proof-tests to maintain the ratings of the sensors and actuators.
- Use wiring installation practices, diagnostics, and proof-tests to assure wiring integrity.
- Generate and control operating and maintenance procedures for the lifetime of the installation.

The ET 200AL, ET 200pro, ET 200SP, and S7-1200/1500 Fail-Safe systems provide a high level of internal diagnostic coverage. Diagnostic coverage of your external circuits, sensors, and actuators depends on your design choices using features of the PLC system and other measures.

The PFH/PFD of each fail-safe PLC component is stated assuming there is no field proof-test within the lifetime of the product. Sensors and actuators typically require regular proof-tests to maintain an expected level of safety performance.

The reaction time of each safety function depends on the reaction time of each component, including the sensor, the PLC system, and the actuator. "Maximum response time (Page 76)" gives further information on delay times through the PLC components. You must choose PLC parameters and external component reaction times to achieve a total safety reaction time goal.

In addition to the total delay from the safety demand input to the safe actuator response, you must consider these additional time-related factors. Refer to "Maximum response time (Page 76)" for exact information:

- To be assured of a safety response, a safety demand signal from the input sensor lasts long enough to be seen by the safety program. Your configured filter time, discrepancy resolution time, and short-circuit test duration all contribute to determining the required signal duration.
- The F-DI 4/F-DQ 2 Fail-Safe module digital outputs regularly test each P- and M-switch to verify that each switch is still functional and under independent control. The OFF test pulse duration can be as long as your configured "Maximum readback time". The ON test pulse duration can be as long as your configured "Maximum readback time switch on test". For a given output, the ON test pulse is only provided to one of the P- or M-switches at a time, but in the presence of single fault this could apply energy to your load. Your actuator should not respond to an OFF signal up to the "Maximum readback time" duration, or to an ON signal up to the "Maximum readback time switch on test" duration.
- The F-DI 4/F-DQ 2 Fail-Safe module digital outputs expect to complete and confirm any commanded transition from the ON to OFF output state. After your program changes the process output value from "1" to "0", do not change the "0" back to a "1" until the output's configured "Maximum readback time" has elapsed. The affected output passivates on commanded "0" states that are too short to confirm.

⚠ WARNING

The safety performance of your installation depends on your design and continued maintenance of each complete safety function.
The ET 200pro, ET 200SP and S7-1200/1500 Fail-Safe CPUs and F-DI 4/F-DQ 2 Fail-Safe module provide components for logic processing with a certified level of safety integrity when used in accordance with ratings, specifications, and instructions.
Failure to comply with these guidelines could cause damage or unpredictable operation which could result in death or severe personal injury and/or property damage.
You must choose all components of your installation and complete your design and maintenance according to accepted safety standards and practices to achieve your required level of safety.

5.1 Digital input applications

You should consider the application modes presented here along with the features of the F-DI 4/F-DQ 2 Fail-Safe module as described in the overview. Refer to "Fail-safe digital inputs (Page 13)".

The main features of the F-DI 4/F-DQ 2 Fail-Safe module digital inputs include the following items:

- Inputs are 24 V DC rated inputs that meet the requirements of IEC 61131-2 as Type 1 inputs.
- Configure each channel as 1oo1 or part of a 1oo2 channel group. The corresponding channels (x.0, x.2) and (x.1, x.3) form a 1oo2 channel group. The lower numbered channel of the group is called the primary input and the other channel is called the secondary input. Within this restriction, you can assign 1oo1 and 1oo2 in any order.

- Short-circuit testing requires use of the internal sensor supply. For all evaluation and sensor interconnections except for 1oo2, 2 channel - 3 wire nonequivalent, use V_{S1} with inputs x.0 to x.1 and V_{S2} with inputs x.2 to x.3. For evaluation and sensor interconnection for 1oo2, 2 channel - 3 wire nonequivalent, use V_{S1} with inputs x.0 to x.3, and do not use V_{S2}.
- If you enable the short-circuit test, you configure both V_{S1} and V_{S2} with the same parameters. All channels that you configure for internal sensor supply are subject to the same short-circuit test. You configure a test duration (length of dark time) and test interval (time between the start of the dark tests).
- The module performs these short-circuit functions for F-DI channels:
  - Monitors the sensor supply to detect short-circuit or overload.
  - Cycles the sensor supply once on each power up to assure control and readback are working. This ensures operational integrity of the sensor supply at power up even when disabled.
  - Monitors the readback during input short-circuit tests.
- Configure a discrepancy time to identify unacceptable differences between 1oo2 inputs.
- Configure a filter time for each channel or each 1oo2 pair.

You can achieve Cat. 3 in 1oo1 configurations if you diagnose external wiring faults or exclude them according to standards by proper routing, protection, and proof-testing of conductors:

- Each F-DI input includes sufficient diagnostics and redundant components such that no single internal fault can cause a dangerous failure.
- An appropriately-rated, single sensor can reach Cat. 3 by internal fault tolerance.
- The external wiring of a single sensor to a single input is vulnerable to single fault dangerous failures unless you apply additional measures.

You can achieve Cat. 4 in 1oo2 configurations if you diagnose external wiring faults or exclude them according to standards by proper routing, protection, and proof-testing of conductors:

- With 1oo2 evaluation, a pair of F-DI inputs is not subject to dangerous internal failure within a reasonable number of accumulated internal faults.
- Appropriately-rated, external-paired sensors or equivalent redundancy can achieve Cat. 4.
- The duplicated external wiring of two sensors to two input points is vulnerable to accumulated fault dangerous failure unless you apply additional measures.

The fail-safe digital inputs are certified for SIL 3/PL e only when you select 1oo2 evaluation.

Input architectures for achieving Safety Integrity Level (SIL)/Category/Performance Level (PL)

The following are the minimum conditions which must be met for achieving the corresponding safety requirements:

Table 2-385 Safety Integrity Level (SIL)/Category/Performance Level (PL) requirements

Application	Sensor supply [1]	Sensor evaluation	Channel connection	Type of sensor connection	Achievable SIL/Category/PL	
					Without short-circuit detection	With short-circuit detection
1	Internal	1oo1 evaluation	Single input	1 channel	2/3/d	
2	External					
3	Internal	1oo2 evaluation	Two inputs	2 channel equivalent	3/3/e	3/4/e
4	External				3/3/e	
5	Internal			2 channel - 3 wire nonequivalent	3/3/e	3/4/e
6	External				3/3/e	
7	Internal			2 channel - 4 wire nonequivalent	3/3/e	3/4/e
8	External				3/3/e	

[1] The F-DI 4/F-DQ 2 Fail-Safe module uses M12 I/Oconnections and is intended for use outside a cabinet in IP67 applications (everything sealed). If you require the use of an external supply, cut the M12 cable and make the connection inside a sealed cabinet or inside a sealed sensor. For external supplies, do not connect the pin 1 wire (V_{S1}) or the pin 5 wire (V_{S2}) in the M12 cable. This action prevents the sensor supply (which may be ON due to a different channel being configured as internal) from being shorted to the external 24 V DC. In addition, make the external 24 V DC connection inside a sealed cabinet or inside a sealed sensor.

Refer to "Pin assignment" (Page 16) for further information on connector pin assignments.

5.1.1 Applications 1 and 2: 1oo1 evaluation of single-channel sensors

F-DI application mode 1

This application mode uses single-channel sensors with a 1oo1 evaluation as shown in the following illustrations. When you use an internal sensor supply, you can successfully perform short-circuit detection.

NOTE

To incorporate F-DI application mode 1 into a SIL 2-rated application, ensure the sensors are appropriately qualified devices.



Figure 2-180 F-DI application mode 1: Internal sensor supply (1oo1 evaluation of a single-channel sensor shown)

Use Y cable (6ES7194-6KB00-0XA0) for F-DI application mode 1 to connect two single-channel sensors in 1oo1 evaluation as follows:

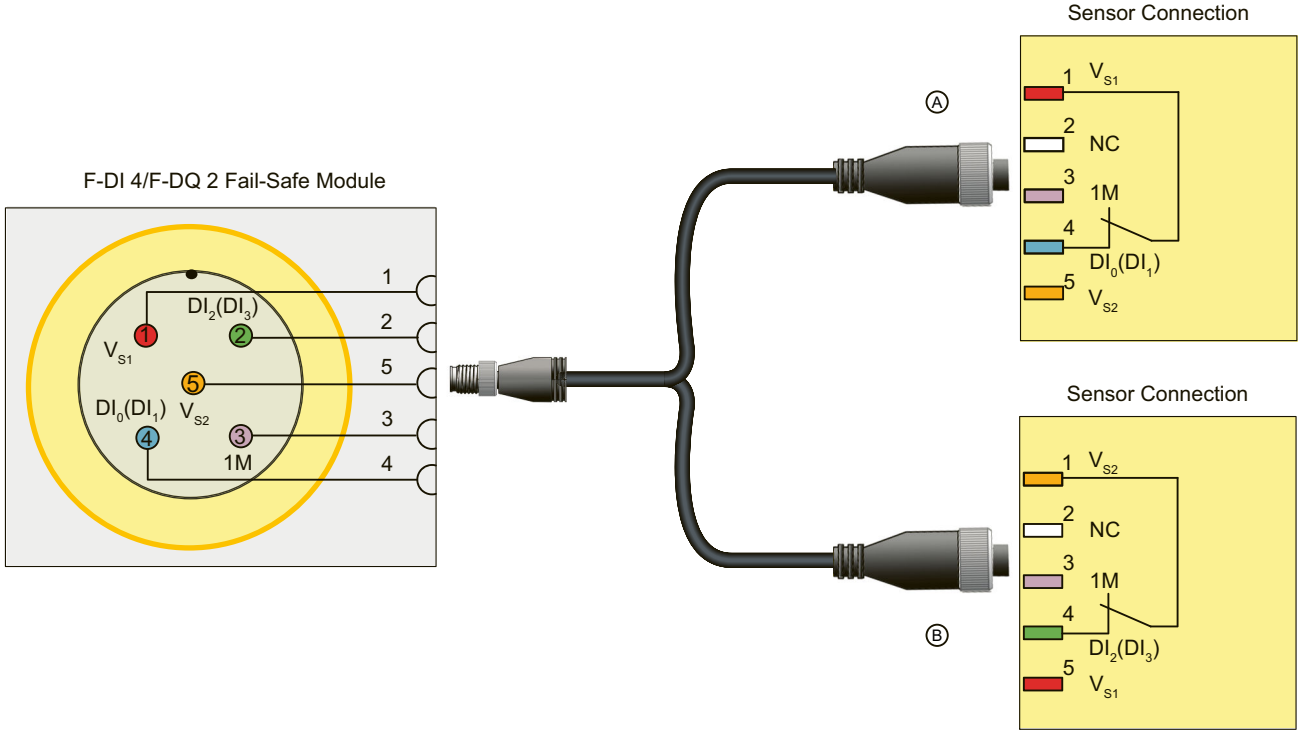


Figure 2-181 F-DI application mode 1: Internal sensor supply (1oo1 evaluation of two single-channel sensors shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo1 evaluation
Sensor supply	Internal
Short-circuit test	Enable

F-DI application mode 2

This application mode uses single-channel sensors with a 1oo1 evaluation. When you use an external sensor supply, the module does not evaluate that channel for short-circuit testing.

NOTE

To incorporate F-DI application mode 2 into a SIL 2-rated application, ensure the sensors are appropriately qualified devices.

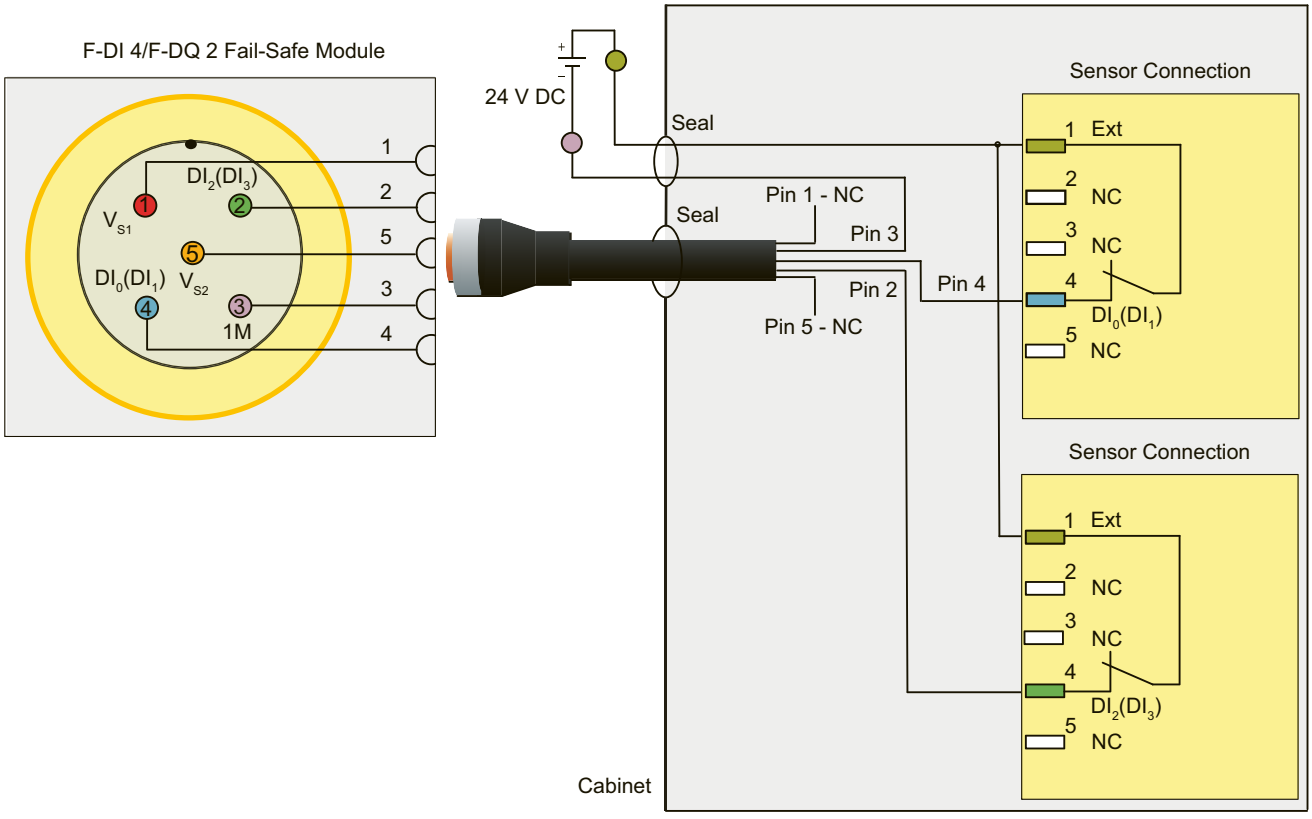


Figure 2-182 F-DI application mode 2: External sensor supply (1oo1 evaluation of two single-channel sensors shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo1 evaluation
Sensor supply	External

5.1.2 Applications 3 and 4: 1oo2 evaluation of equivalent sensors

F-DI application mode 3

This application mode uses a two-channel sensor or two single-channel sensors in a 1oo2 voting with discrepancy evaluation. When you use an internal sensor supply, you can successfully perform short-circuit detection.

NOTE

To incorporate F-DI application mode 3 into a SIL 3-rated application, ensure the sensors are appropriately qualified devices.



Figure 2-183 F-DI application mode 3: Internal sensor supply (1oo2 evaluation of two-channel sensor shown)

Use Y cable (6ES7194-6KB00-0XA0) for F-DI application mode 3 as follows:

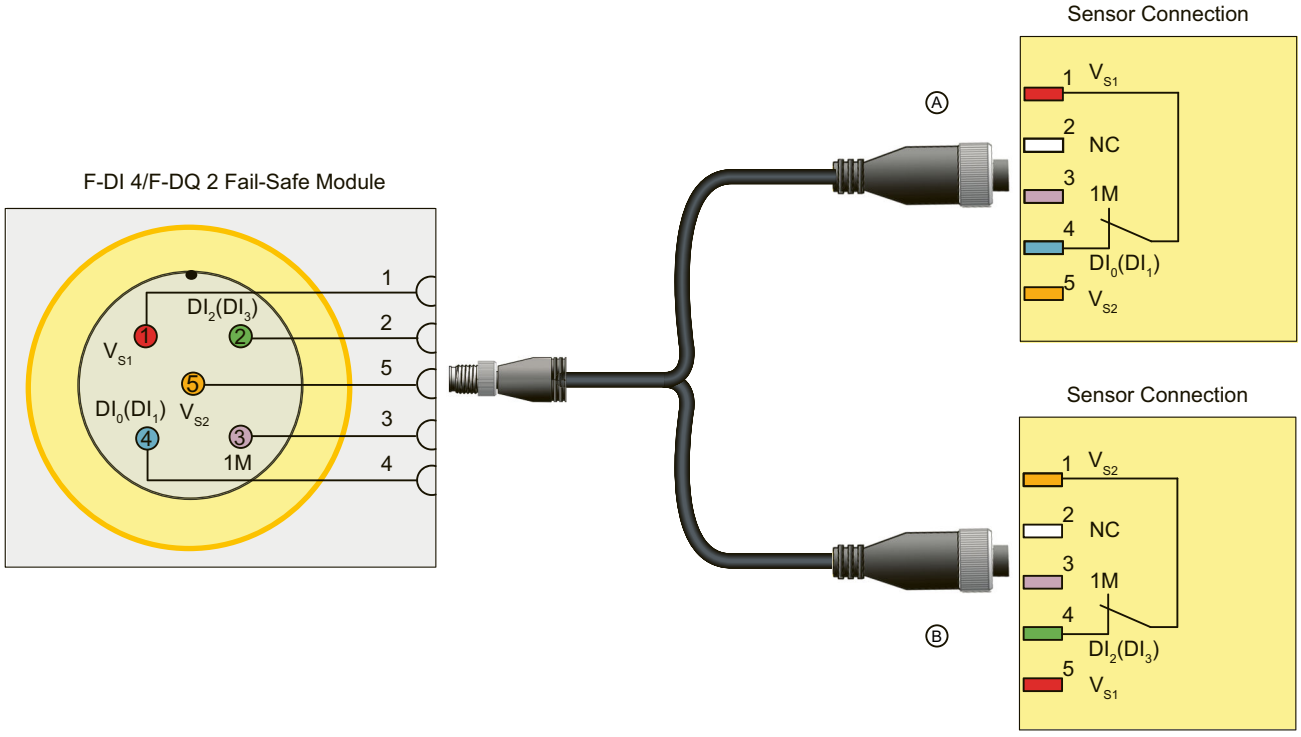


Figure 2-184 F-DI application mode 3: Internal sensor supply (1oo2 evaluation of two single-channel sensors shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo2 evaluation, 2 channel equivalent
Sensor supply	Internal
Short-circuit test	Enable

F-DI application mode 4

This application mode uses a two-channel sensor or two single-channel sensors in a 1oo2 voting with discrepancy evaluation. When you use an external sensor supply, the module does not evaluate that channel for short-circuit testing.

NOTE

To incorporate F-DI application mode 4 into a SIL 3-rated application, ensure the sensors are appropriately qualified devices.

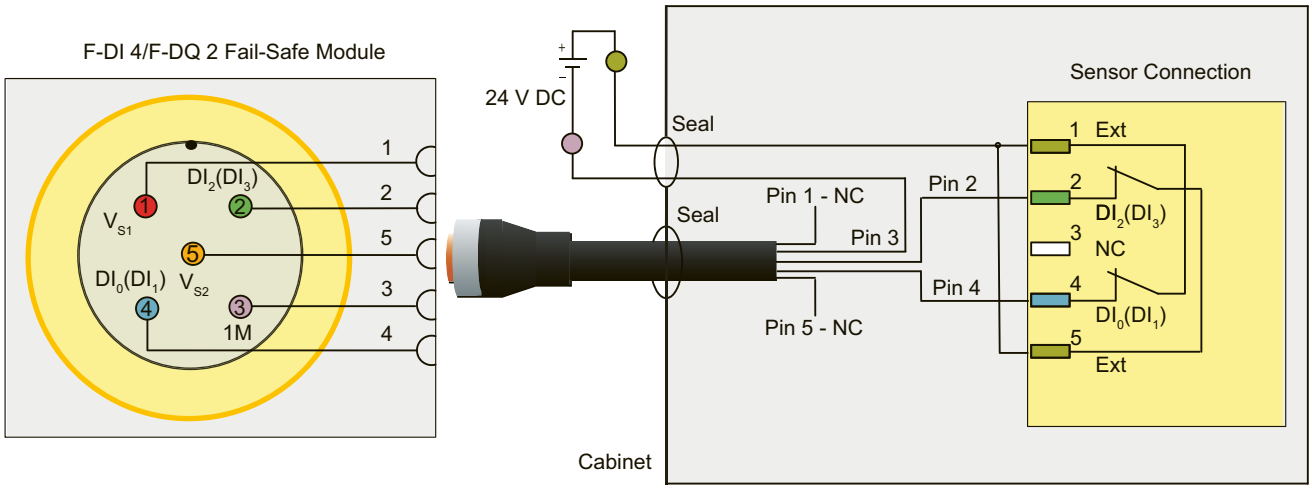


Figure 2-185 F-DI application mode 4: External sensor supply (1oo2 evaluation of two-channel sensor shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo2 evaluation, 2 channel equivalent
Sensor supply	External

5.1.3 Applications 5 and 6: 1oo2 evaluation of a 3-wire, nonequivalent sensor circuit

F-DI application mode 5

This application mode uses a two-channel sensor or two single-channel sensors with two nonequivalent outputs in a 1oo2 voting with discrepancy evaluation. When you use an internal sensor supply, you can successfully perform short-circuit detection. The application mode uses the following pins:

- Pin 2 (channels 2 and 3) is the inverted input of the nonequivalent configuration
- Pin 4 (channels 0 and 1) is the non-inverted input of the nonequivalent configuration

NOTE

To incorporate F-DI application mode 5 into a SIL 3-rated application, ensure the sensors are appropriately qualified devices.

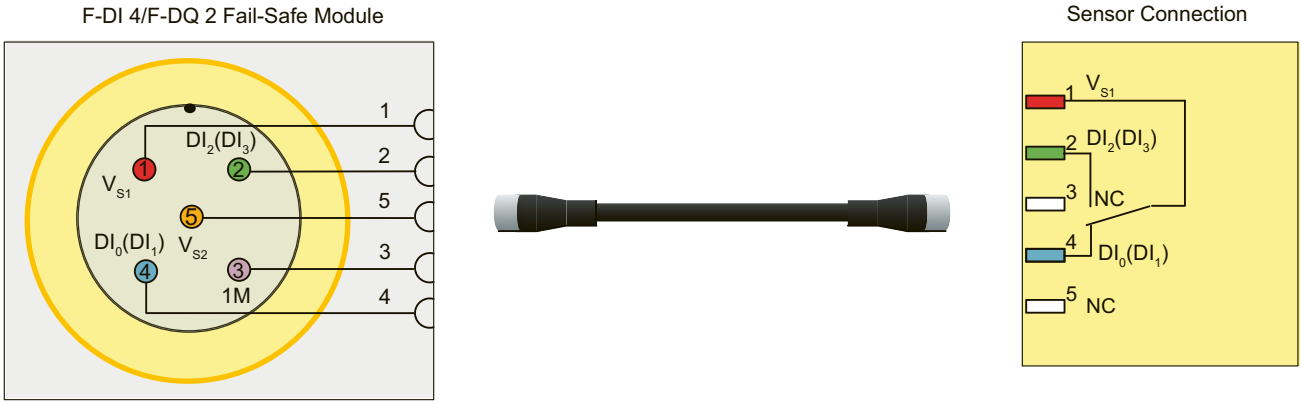


Figure 2-186 F-DI application mode 5: Internal sensor supply (1oo2 evaluation of two-channel sensor with nonequivalent outputs shown)

Use Y cable (6ES7194-6KA00-0XA0) for application mode 5 as follows:

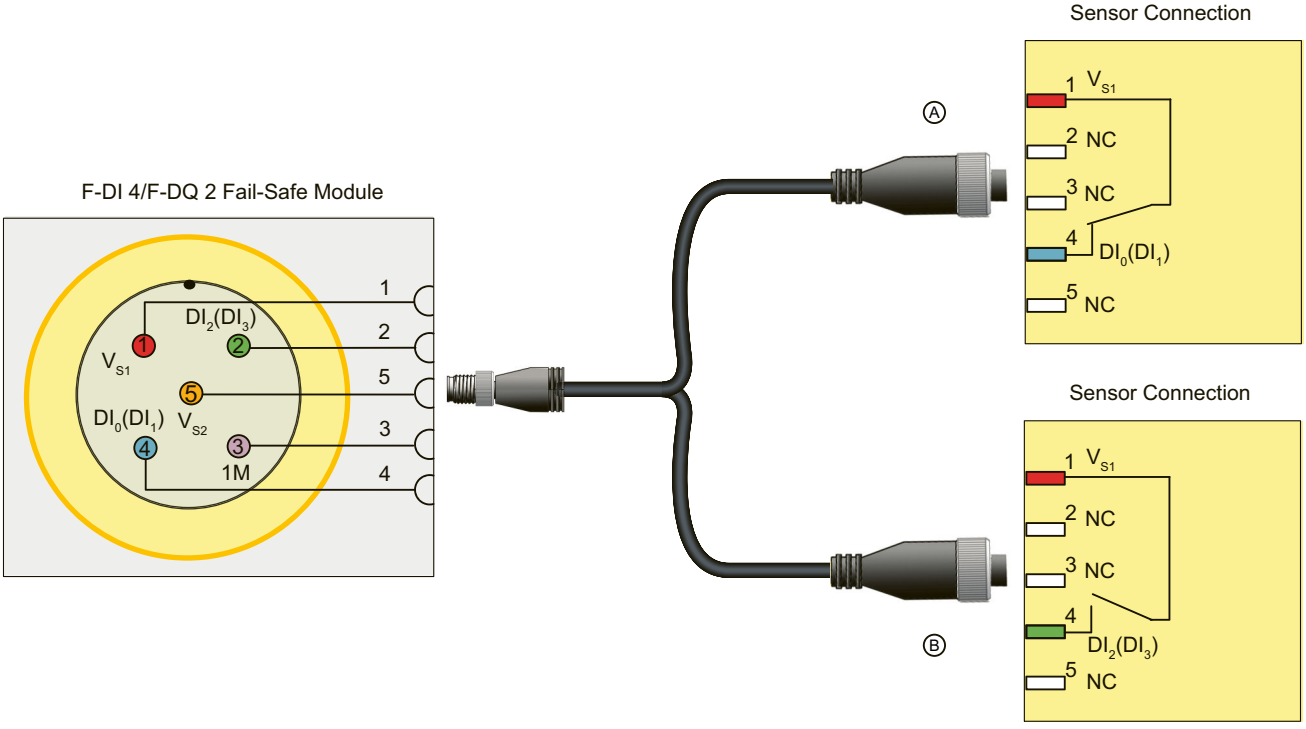


Figure 2-187 F-DI application mode 5: Internal sensor supply (1oo2 evaluation of two single-channel sensors with nonequivalent outputs shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo2 evaluation, 2 channel - 3 wire nonequivalent
Sensor supply	Internal
Short-circuit test	Enable

F-DI application mode 6

This application mode uses a two-channel sensor or two single-channel sensors with two nonequivalent outputs in a 1oo2 voting with discrepancy evaluation. When you use an external sensor supply, the module does not evaluate that channel for short-circuit testing. The application mode uses the following pins:

- Pin 2 (channels 2 and 3) is the inverted input of the nonequivalent configuration
- Pin 4 (channels 0 and 1) is the non-inverted input of the nonequivalent configuration

NOTE

To incorporate F-DI application mode 6 into a SIL 3-rated application, ensure the sensors are appropriately qualified devices.

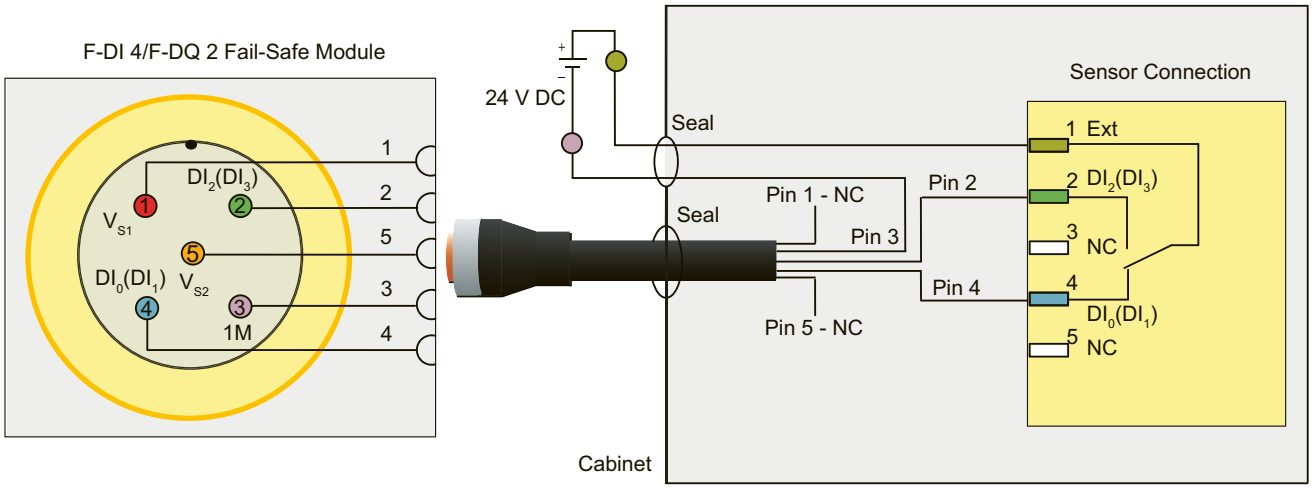


Figure 2-188 F-DI application mode 6: External sensor supply (1oo2 evaluation of two-channel sensor with nonequivalent outputs shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo2 evaluation, 2 channel - 3 wire nonequivalent
Sensor supply	External

5.1.4 Applications 7 and 8: 1oo2 evaluation of a 4-wire, nonequivalent sensor circuit

F-DI application mode 7

This application mode uses a two-channel sensor or two single-channel sensors in nonequivalent configuration (4-wire connection) in a 1oo2 voting with discrepancy evaluation. When you use an internal sensor supply, you can successfully perform short-circuit detection. The application mode uses the following pins:

- Pin 2 (channels 2 and 3) is the inverted input of the nonequivalent configuration
- Pin 4 (channels 0 and 1) is the non-inverted input of the nonequivalent configuration

NOTE

To incorporate F-DI application mode 7 into a SIL 3-rated application, ensure the sensors are appropriately qualified devices.



Figure 2-189 F-DI application mode 7: Internal sensor supply (1oo2 evaluation of two-channel sensor with nonequivalent outputs shown)

Use Y cable (6ES7194-6KB00-0XA0) for application mode 7 as follows:

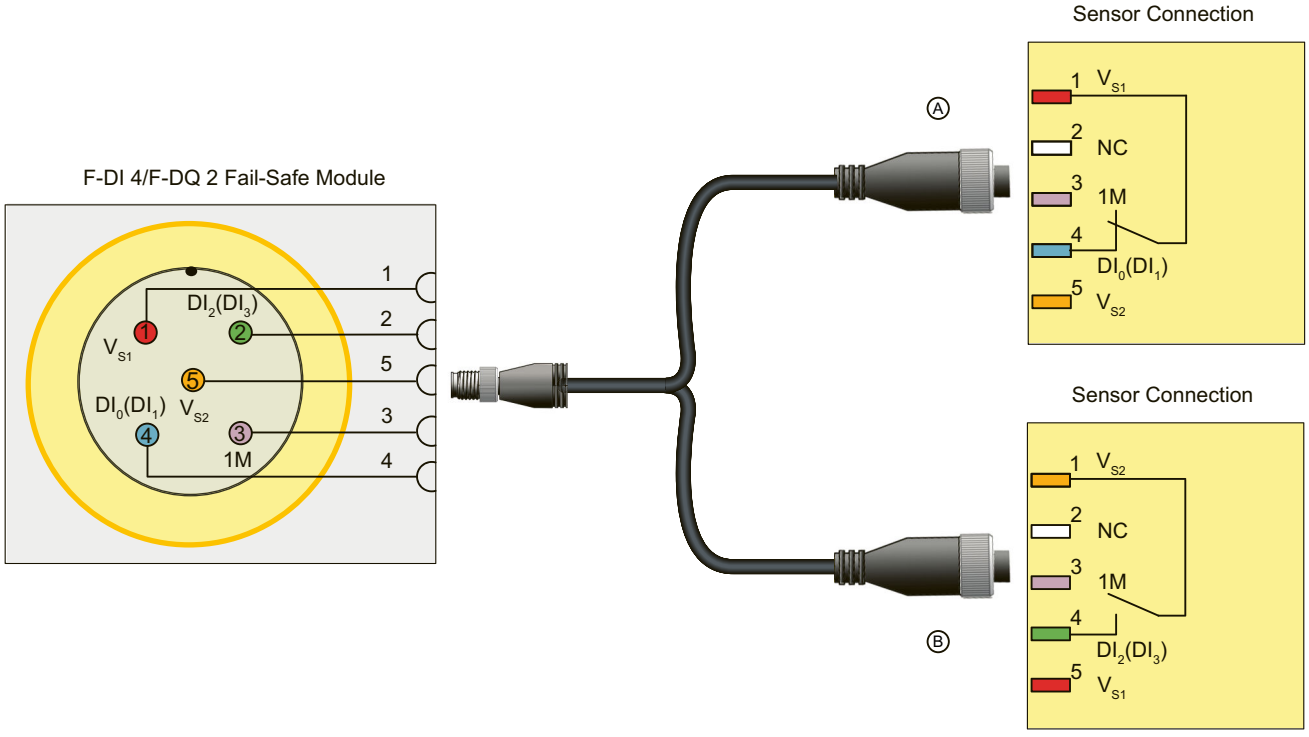


Figure 2-190 F-DI application mode 7: Internal sensor supply (1oo2 evaluation of two single-channel sensors with nonequivalent outputs shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo2 evaluation, 2 channel - 4 wire nonequivalent
Sensor supply	Internal
Short-circuit test	Enable

F-DI application mode 8

This application mode uses two single-channel sensors or a two-channel sensor with two nonequivalent outputs in a 1oo2 voting with discrepancy evaluation. When you use an external sensor supply, the module does not evaluate that channel for short-circuit testing. The application mode uses the following pins:

- Pin 2 (channels 2 and 3) is the inverted input of the nonequivalent configuration
- Pin 4 (channels 0 and 1) is the non-inverted input of the nonequivalent configuration

NOTE

To incorporate F-DI application mode 8 into a SIL 3-rated application, ensure the sensors are appropriately qualified devices.

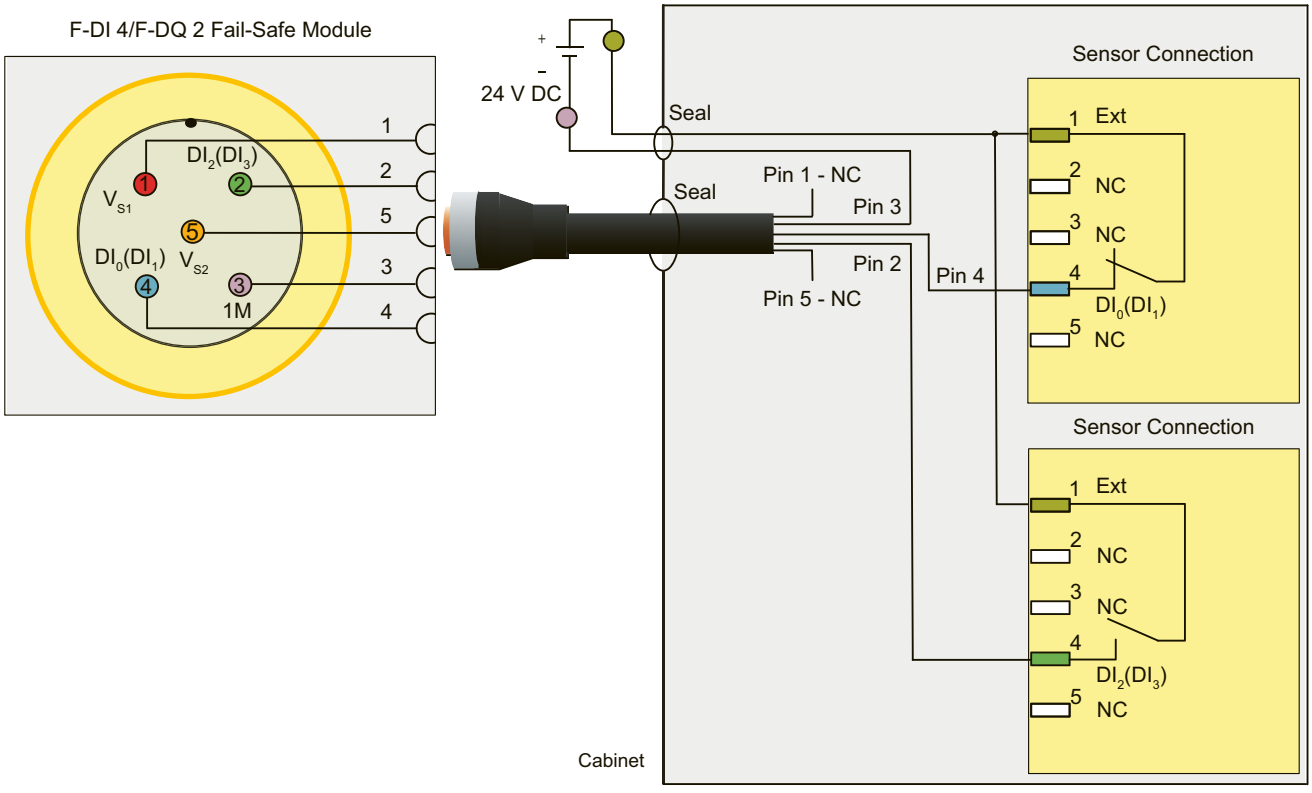


Figure 2-191 F-DI application mode 8: External sensor supply (1oo2 evaluation of two single channel sensors with nonequivalent outputs shown)

Parameter assignment

Parameter name	Parameter value
Sensor evaluation	1oo2 evaluation, 2 channel - 4 wire nonequivalent
Sensor supply	External

5.2 Digital output applications

You should consider the application modes presented here along with the features of the F-DI 4/F-DQ 2 Fail-Safe module as described in the overview. Refer to "Fail-safe digital outputs (Page 14)".

The main features of the F-DI 4/F-DQ 2 Fail-Safe module digital outputs include the following items, which apply to each output channel:

- The fail-safe module separately controls current flow in the P output and M output.
- The voltage at the P and M outputs is read back to confirm proper state.
- The P and M outputs are regularly tested with short ON and OFF pulses to confirm control.

Ensure that the following steps are accomplished:

- Configure readback times that are sufficiently long to allow the channel's external voltages to respond to process value changes and applied test patterns from the bit pattern test. However, configuring readback times that are too long can cause your load to physically respond to applied test patterns during dark tests.
- Verify that internal current limiting as described in the data sheet is sufficient in combination with your 24 V DC supply. Consider whether additional current limits or fuses are necessary. Refer to "Specifications" and "Connecting" in the *ET 200AL distributed I/O system* system manual (https://support.industry.siemens.com/cs/ww/en/view/89254965).

The module controls all output channels as 1oo2 with cross-diagnostics.

All applications shown are capable of reaching SIL 3/Cat. 4/PL e unless you have dark testing disabled.

To reach Cat. 4, ensure that the following conditions are met:

- The dark testing is enabled.
- The external contactors are SIL-rated with sense contacts.
- The diagnostics are within limits when you read the sense contacts back and confirm the external contactor response in your program. Siemens recommends using an F-DI input for sense contact and other safety diagnostic inputs.

Output architectures for achieving Safety Integrity Level (SIL)/Category/Performance Level (PL)

The following are the minimum conditions which must be met for achieving the corresponding safety requirements:

Table 2-386 Safety Integrity Level (SIL)/Category/Performance Level (PL) requirements

Application	Type of actuator connection	Achievable SIL/Category/PL	
		Dark test disabled	Dark test enabled
1	Directly-connected SIL-rated actuator	2/3/d	3/4/e
2	External contactors: Separate P and M controlled contactors	2/3/d	3/4/e
3	External contactors: Parallel-connected contactors between P and M	2/3/d	3/4/e
4	External contactors: Separate output channels for each contactor	2/3/d	3/4/e

Refer to "Pin assignment (Page 16)" for further information on connector pin assignments.

Refer to "Disable Dark Test (max. SIL 2, Cat. 3, PL d)" in "DQ parameters (Page 28)" for additional information on enabling and disabling dark testing.

5.2.1 Application 1: Wiring a directly-connected SIL-rated actuator

The module supports application mode 1, where there is a direct connection of a load between the P and M outputs of one channel. Both switches are opened when de-energizing the load.

NOTE

This configuration achieves SIL 3/Cat. 4/PL e if neither channel is configured to disable the dark test.

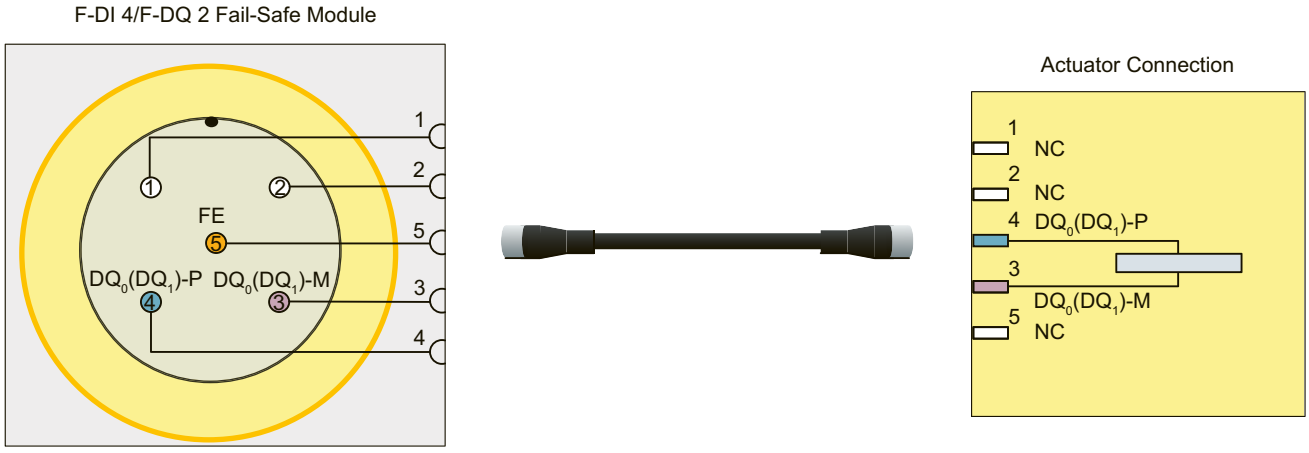


Figure 2-192 F-DQ application mode 1

5.2.2 Application 2: Wiring external contactors: Separate P and M controlled contactors

The module supports application mode 2, where the module controls the load using series-connected, normally-open contacts of two relays. The coil of one relay connects the P-output of a channel and M. The coil of the other relay connects the M-output of the same channel and L+.

NOTE

This configuration achieves SIL 3/Cat. 4/PL e if you fulfill the following conditions:

- The CPU checks the relay status (feedback) using a separate digital input.
- You adequately protect the wiring against shorts from the P output to L+ and shorts from the M output to M. The CPU cannot switch off the actuator if both faults occur.
- You do not disable dark test for either output.

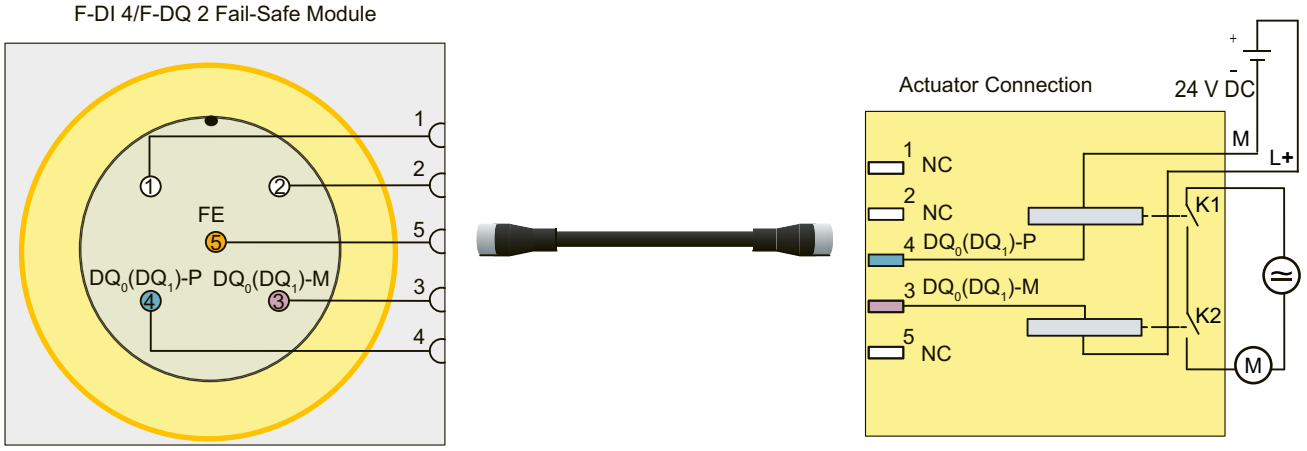


Figure 2-193 F-DQ application mode 2

5.2.3 Application 3: Wiring external contactors: Parallel-connected contactors between P and M

The module supports application mode 3, where the module controls the load using the series-connected, normally-open contacts of two relays. You connect the coils of both relays, in parallel, across the outputs of one channel.

NOTE

This configuration achieves SIL 3/Cat. 4/PL e if the CPU checks the relay status (feedback) using a separate digital input and if neither channel is configured to disable the dark test. Application mode 3 is the preferred way of controlling an actuator using relays in a safety-related application. Application mode 3 avoids the problems mentioned for Application mode 2, regarding short-circuits of the P and M outputs.

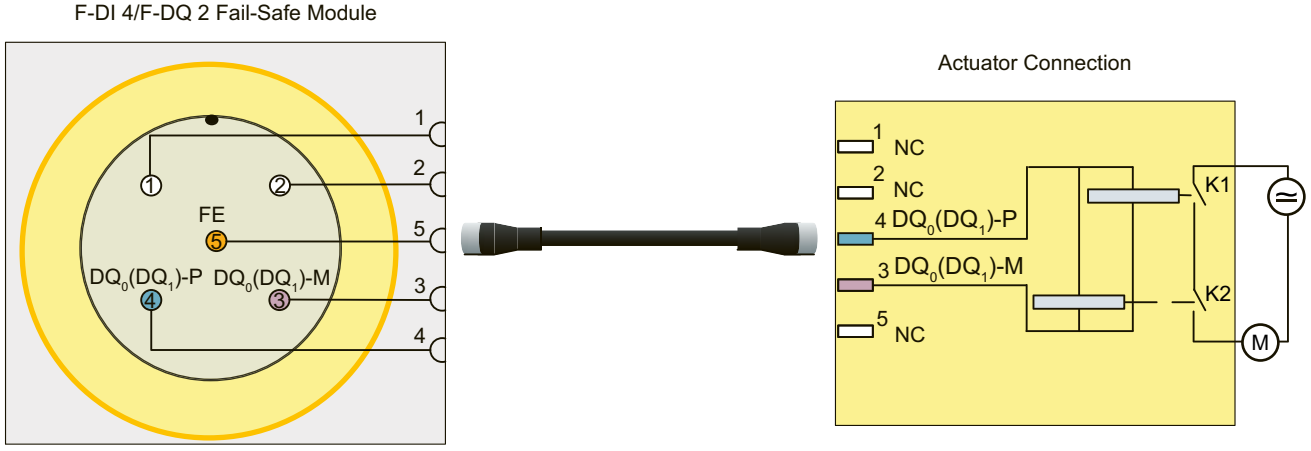


Figure 2-194 F-DQ application mode 3

5.2.4 Application 4: Wiring external contactors: Separate output channels for each contactor

The module supports application mode 4, where the module controls the load using the series-connected, normally-open contacts of two relays. Connect the coils of both relays across the outputs of two channels. In the safety program, write the same process value (ON or OFF) to both output channels.

NOTE

This configuration achieves SIL 3/Cat. 4/PL e if the CPU checks the relay status (feedback) using a separate digital input and neither channel is configured to disable the dark test.

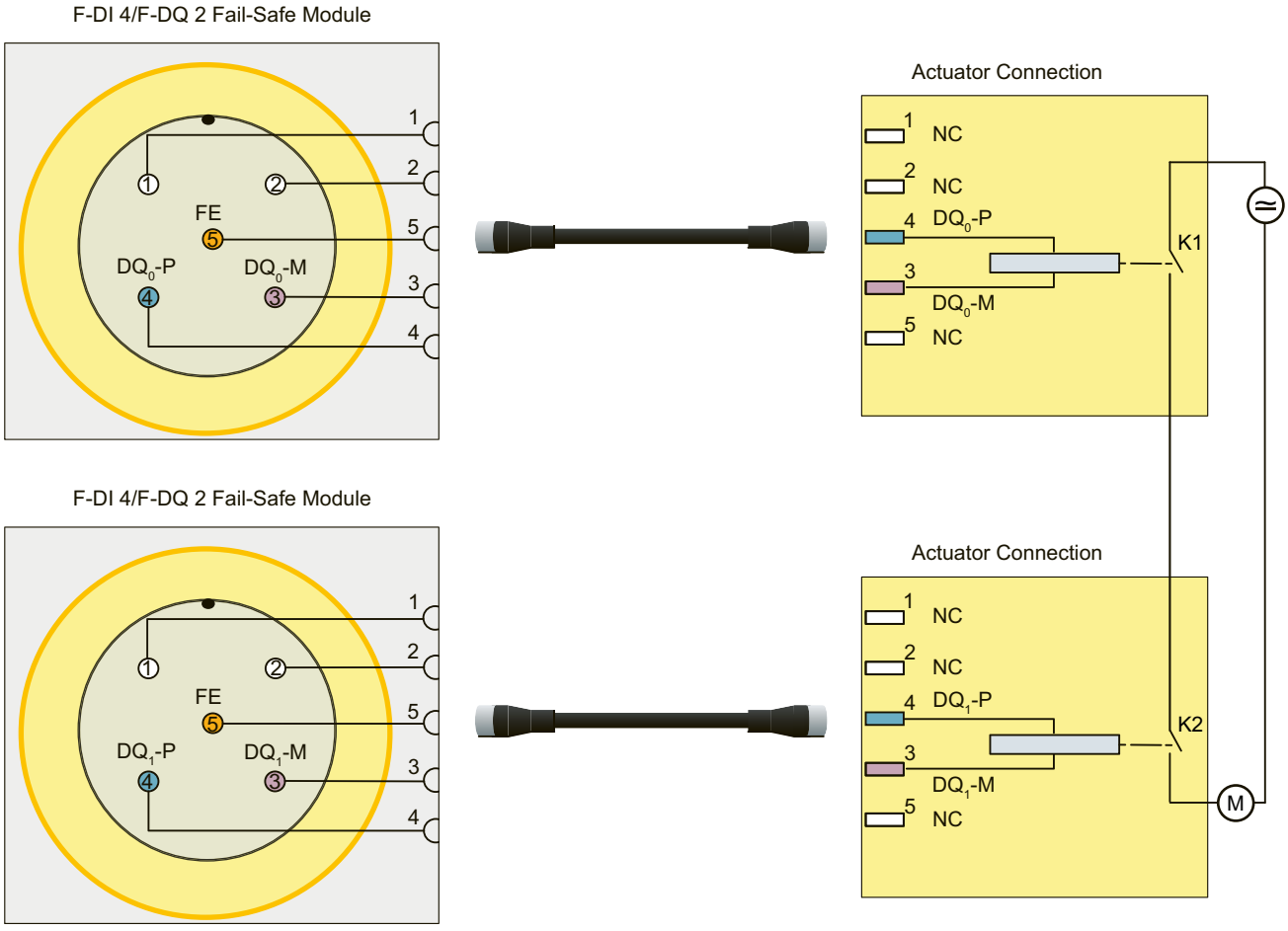


Figure 2-195 F-DQ application mode 4

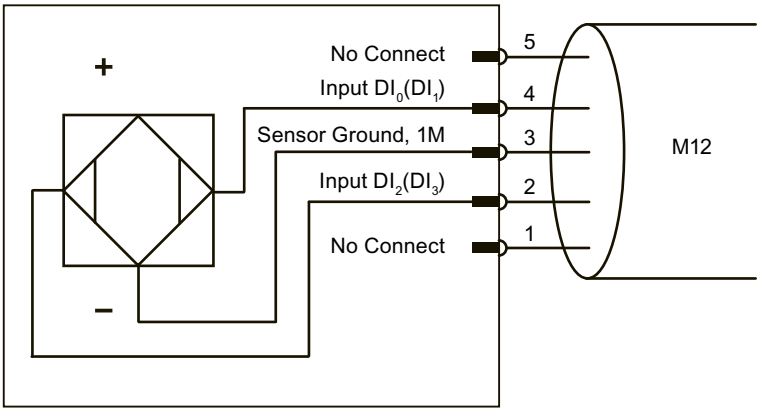
5.3 Examples of application modes for the F-DI 4/F-DQ 2 Fail-Safe module

You can connect field devices to the F-DI 4/F-DQ 2 Fail-Safe module as shown below.

Laser scanner (1oo2 evaluation)

For the output signal switching device (OSSD) sensors of a Laser Scanner, use F-DI application mode 4 to connect the Laser Scanner output signal switching device with 1oo2 evaluation to the F-DI 4/F-DQ 2 Fail-Safe module:

Laser Scanner (1oo2)

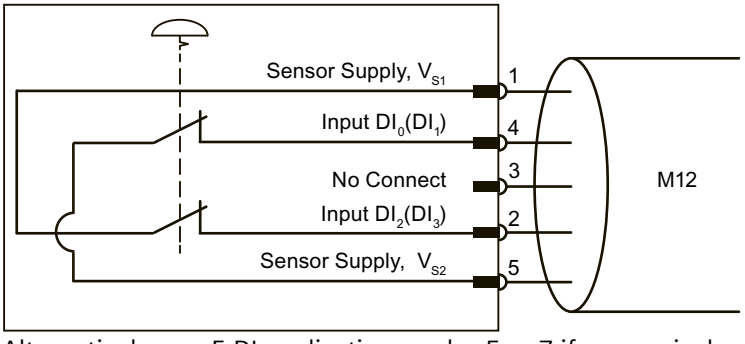


Alternatively, use F-DI application mode 3 and disable the parameter "Short-circuit test" for both sensor supplies.

ESTOP (Emergency Stop) (1oo2 evaluation)

For the ESTOP, use F-DI application mode 3 to connect an ESTOP device with 1oo2 evaluation to the F-DI 4/F-DQ 2 Fail-Safe module:

ESTOP (1oo2)

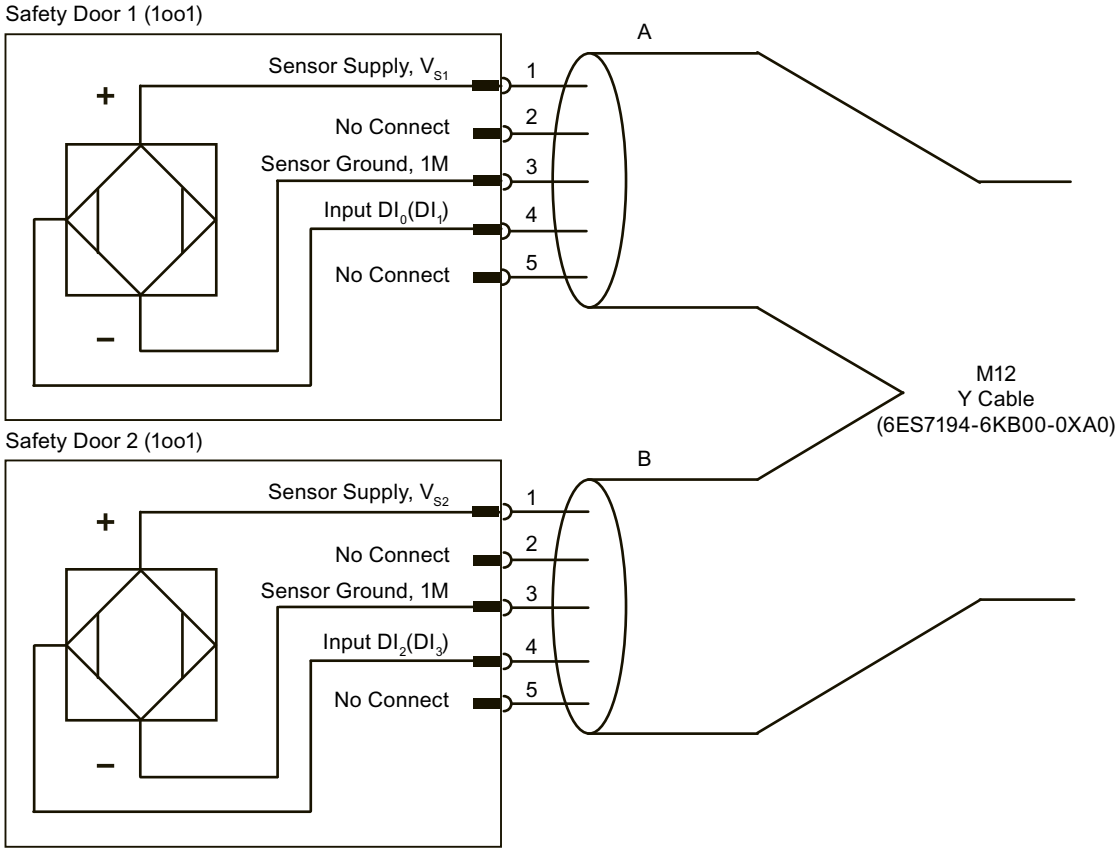


Alternatively, use F-DI application modes 5 or 7 if nonequivalent evaluation is required for your ESTOP device.

Safety doors (1oo1 or 1oo2 evaluation)

For the Safety Doors, you can do one of the following:

- Use F-DI application mode 1 with the fail-safe Y cable (6ES7194-6KB00-0XA0) to connect two single-channel sensors with 1oo1 evaluation to one input connection of the F-DI 4/F-DQ 2 Fail-Safe module.
- Use F-DI application mode 3 (1oo2 evaluation), using two single-channel sensors on the same safety door.



Alternatively, use F-DI application mode 5 with the fail-safe Y cable (6ES7194-6KA00-0XA0) to connect two nonequivalent single-channel sensors with 1oo2 evaluation on the same safety door.

Safety position switch with interlock (1oo2 evaluation)

Use F-DI application mode 3 and F-DQ application mode 1 to connect the safety position switch with interlock to the F-DI 4/F-DQ 2 Fail-Safe module.

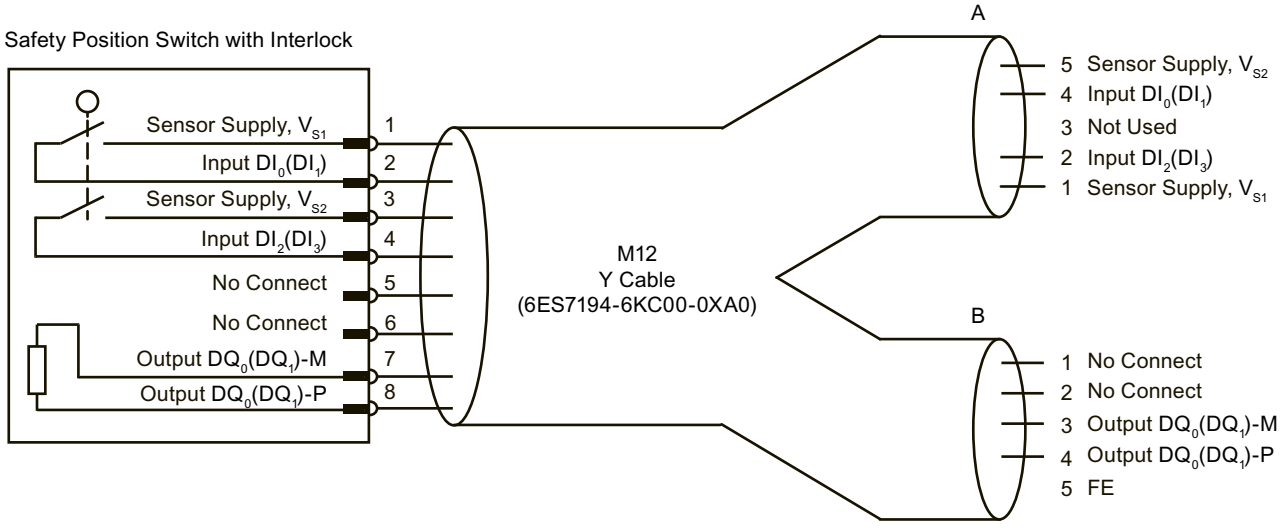
Use inverted Y cable (6ES7194-6KC00-0XA0) for a safety position switch with interlock. The inverted Y cable is designed to properly connect the fail-safe module F-inputs and F-output to the safety position switch.

NOTE

This configuration achieves SIL 3/Cat. 4/PL e if neither output channel is configured to disable the dark test.

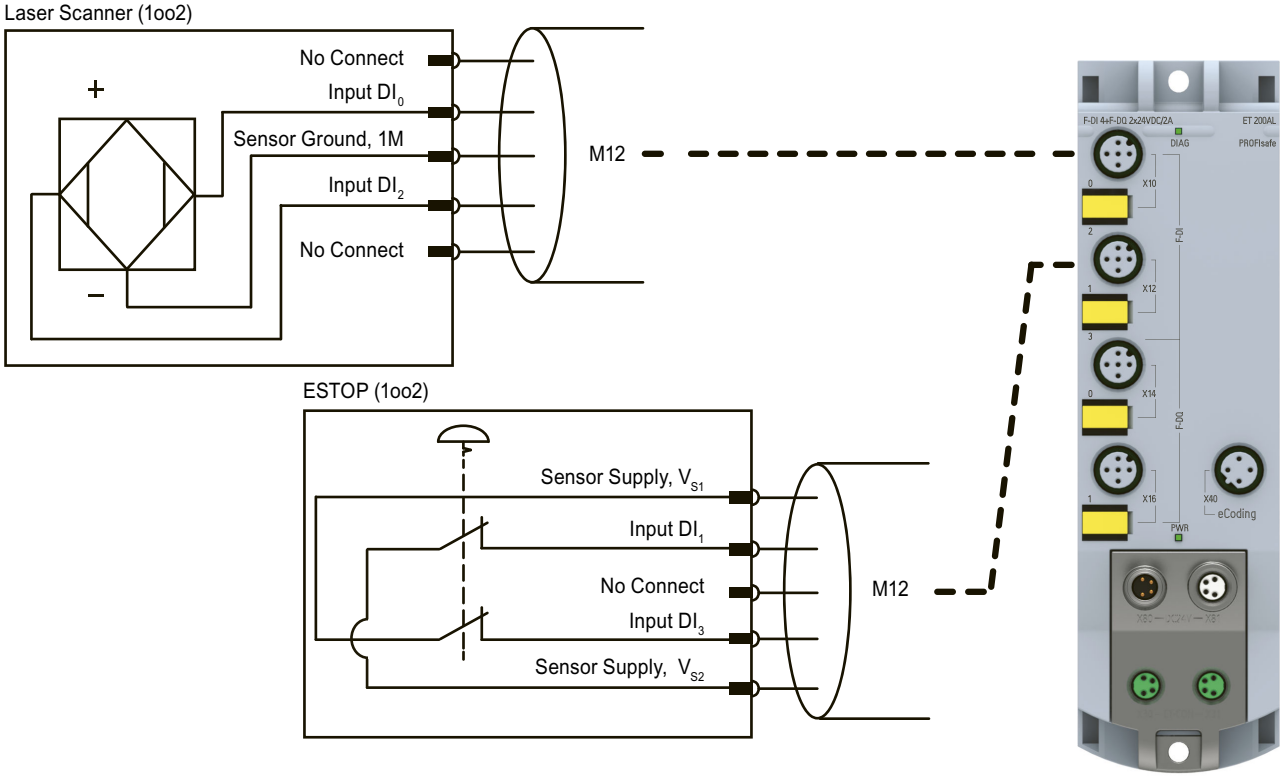
NOTE

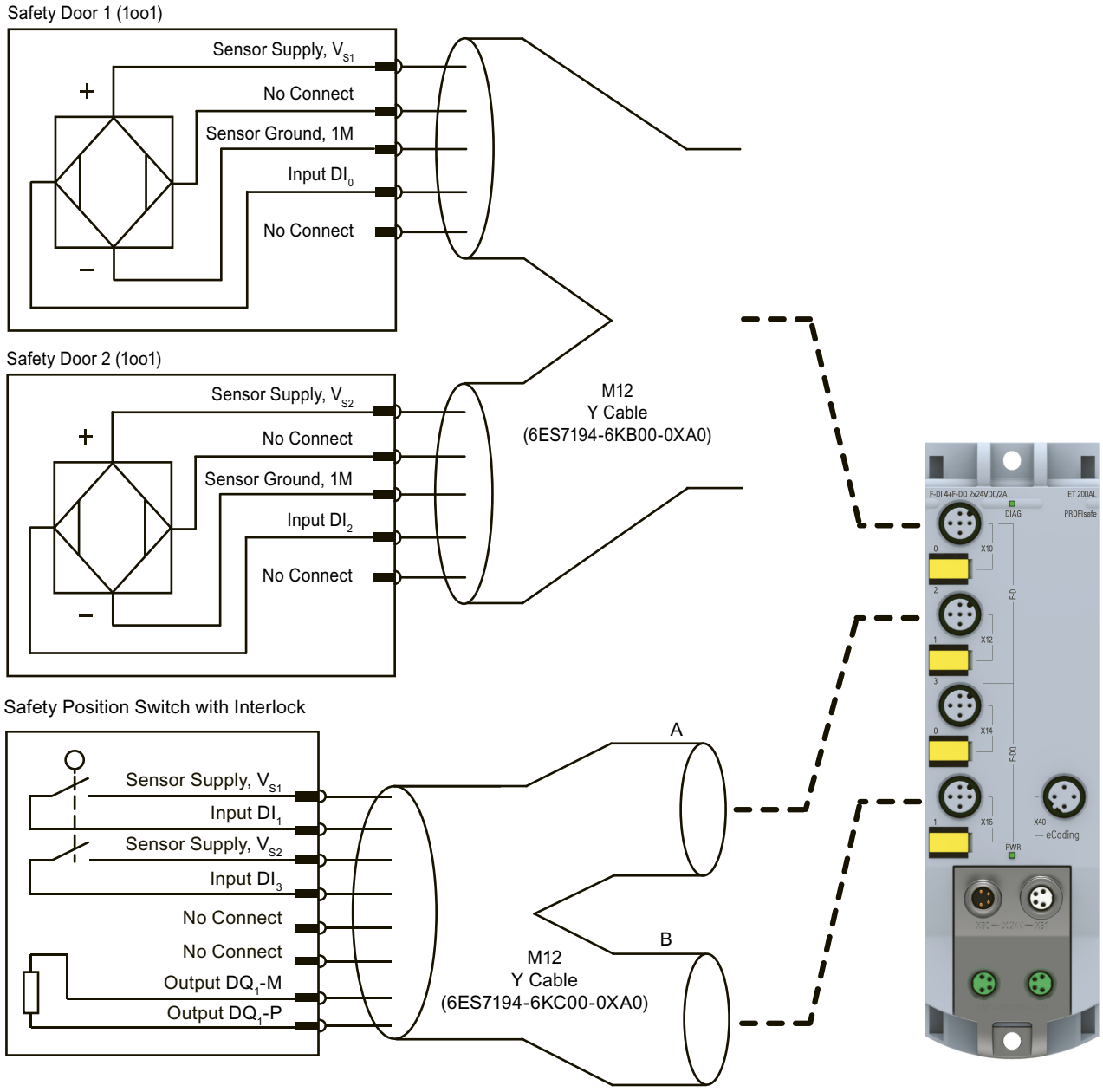
To incorporate this application into a SIL 3-rated application, ensure the sensors are appropriately qualified devices: either SIL 3 or SIL 2 with the Systematic Capability rules defined in the SIRIUS documentation. For further information, refer to the *Industrial Controls, Detecting devices SIRIUS 3SE5/3SF1/3SE66/3SE67 position switches configuration manual* on the Internet (https://support.industry.siemens.com/cs/us/en/view/43920150).



Connect devices to F-DI 4/F-DQ 2 Fail-Safe module

The figures below are examples of field devices connected to the input and output sockets of the F-DI 4/F-DQ 2 Fail-Safe module:




Safety Door 1 (1oo1)
Sensor Supply, V_{S1}
No Connect
Sensor Ground, 1M
Input DI_0
No Connect
+
–
Safety Door 2 (1oo1)
Sensor Supply, V_{S2}
No Connect
Sensor Ground, 1M
Input DI_2
No Connect
+
–
M12
Y Cable
(6ES7194-6KB00-0XA0)
Safety Position Switch with Interlock
Sensor Supply, V_{S1}
Input DI_1
Sensor Supply, V_{S2}
Input DI_3
No Connect
No Connect
Output DQ_1-M
Output DQ_1-P
A
B
M12
Y Cable
(6ES7194-6KC00-0XA0)
F-DI 4xF-DQ 2x24VDC/2A
ET 200AL
DIAG
PROFIsafe
X10
X12
X14
X16
X40
eCoding
PWR
F-DI
F-DQ

Interrupts/diagnostic messages/diagnostics 6

6.1 Reactions to faults

Reactions to startup of the fail-safe system and to faults

The fail-safe concept depends on the identification of a safe state for all process variables. The value "0" (de-energized) represents this safe state for digital fail-safe modules. This applies to both sensors and actuators.

The safety function requires that safe state values be applied to the fail-safe channel(s) instead of process values (passivation of the fail-safe module or channel(s)) in the following situations:

- When the fail-safe system is started up
- If module faults are detected, such as RAM or processor failures
- If errors are detected during safety-related communication between the fail-safe CPU and the fail-safe module through the PROFIsafe safety protocol (communication error)
- If module channel faults occur (for example, short-circuit and discrepancy errors)

The fail-safe CPU enters information about detected system faults into the diagnostic buffer.

Automatic safety measures and the PROFIsafe protocol ensure that the safe state is set if the system detects a fault.

Fail-safe modules do not remember errors upon power cycle. When the system is powered down and then restarted, the modules detect any faults still existing again. The exception to this is a permanent deactivation fault such as "sustained overvoltage".

Fail-Safe value for fail-safe modules

If digital input channels are passivated, the fail-safe system always provides safe state values ("0") for the safety program instead of the process values applied to the fail-safe inputs.

If digital output channels are passivated in the fail-safe module digital outputs, the fail-safe system always transfers safe state values "0" to the fail-safe outputs instead of the output values provided by the safety program. The output channels are de-energized.

The passivation safe state value and the output state value in CPU STOP mode are always "0", de-energized. You cannot select or program a default "ON" state for passivation or STOP mode.

Passivation is applied to individual channels when a channel-specific diagnostic failure is detected. Failures that can affect the entire module result in passivation of all channels.

NOTE

In the **F-DI 4/F-DQ 2 Properties** > **F-parameter**s > "Behavior after channel fault" field, if you select "Passivate the entire module", a single channel fault will result in passivation of all channels.

Timeout of the PROFIsafe message (F-monitoring time exceeded) passivates all module channels.

Table 2-387 Module signal type and passivation result

Module signal type	Passivation result
Fail-safe digital inputs	• Tests are evaluated per channel, in order to allow channel-granular passivation of defective inputs. • If a channel fault occurs for a 1oo1 configuration, depending on your configuration, only the affected channel or all channels may be passivated. For a 1oo2, both inputs of the channel group in the 1oo2 configuration are passivated.
Fail-safe digital outputs	• Tests are evaluated per channel, in order to allow channel-granular passivation of defective outputs. • Diagnostic evaluations are performed separately for each of the two switches of a channel. Depending on your configuration, failure detection for one switch may lead to passivation of only the affected channel or all channels.

Response to faults in the fail-safe system

You should prepare maintenance procedures for your system to assure that return to operation after a detected fault is controlled and documented.

Perform the following steps:

1. Diagnosis and repair of the fault
2. Revalidation of the safety function
3. Recording in the service report

Reintegration of a fail-safe module

A channel or module can be reintegrated after diagnostics determine that a fault has cleared successfully.

You can configure reintegration as automatic or manual. You can make this selection on a per channel basis in the Device Configuration. Module wide errors such as PROFIsafe communication errors or supply voltage errors are always manually reintegrated. Fatal diagnostic errors require a power cycle with successful diagnostics to reintegrate.

Automatic

Channels that you select to be automatically reintegrated are immediately reintegrated when the fault has cleared.

Manual

Channels that you select to be manually reintegrated are acknowledged in your program after the fault has cleared.

The "ACK_REQ" bit for that module goes true to indicate that reintegration is possible. After the "ACK_REQ" bit is true, your program can set the "ACK_REI" bit to allow the reintegration of all channels in that module that are ready to be reintegrated.

You can also acknowledge all faults in an F-runtime group using the "ACK_REI_GLOB" input of the "ACK_GL" instruction.

Reintegration after high stress events

High temperature, high voltage, or excessive current stress can damage electronics, reducing the reliability while components continue to work apparently as expected. Passivation does not remove the potentially damaging effects of high ambient temperature or high applied voltage. Solid state switch outputs can be damaged by high currents prior to protective device activations. The PFD and PFH reliability calculations assume the fail-safe module is operated within its specified operating parameters. When a module has passivated due to a high stress event, even though it apparently works correctly and passes all diagnostics, the probability of a future dangerous failure may be increased.

⚠ WARNING

It is possible to reintegrate a channel or module while some fault is still present that is not readily detected by the module diagnostics.
Reintegration of a faulty system can result in unexpected machine or process operation, which may cause death or serious injury to personnel, and/or damage to equipment.
After any reported fault, the steps outlined in this chapter and in safety standards applicable to your system should be followed to assure that the fault is completely understood and corrected before reintegration.

For an exact list of faults for the module, refer to "Fault types, causes, and corrective measures (Page 65)".

At reintegration, the following occurs:

- For a fail-safe module digital input, the process values pending at the fail-safe inputs are again provided for the safety program.
- For a fail-safe module digital output, the output values provided in the safety program are again transferred to the fail-safe outputs.

Safety repair time

The repair time used for PFH and PFD calculations is 100 hours.

Passivation is designed to provide the safe state of the safety function in the event of a single fault. While a channel is passivated and energy is still available to the channel, there is a possibility that additional faults can cause a dangerous failure of the safety function. You should respond to passivations by repairing the fault or taking the passivated channel out of service in less than 100 hours to preserve the safety integrity level of your system.

Deactivated fail-safe I/O are not being diagnosed and are subject to dangerous failure without warning.

If any error persists for 100 hours, the entire module is passivated and can only be recovered by power cycling.

If a repair within 100 hours is not possible, passivated fail-safe outputs should be taken out of service by physically disconnecting or opening circuits so that faults in the fail-safe module cannot apply energy to the load. To remove input channels from service in an operating PLC system, references to any passivated fail-safe inputs are removed from any operating F-CPU Safety program logic that can result in activation of a safety function output.

Do not depend on channel or module passivation to maintain safe state for more than 100 hours.

Do not depend on deactivation or lack of configuration to maintain safe state in any circumstances.

⚠ WARNING

Unintentional activation of F-I/O module with fail-safe output
If a fail-safe output is passivated for a period longer than the safety repair time (> 100 hours) and the fault remains uncorrected, you need to be aware that an F-output could be activated unintentionally due to a second fault. This would place the F-system in a dangerous state. Even though it is highly unlikely that such hardware faults occur, you must prevent the unintentional activation of a fail-safe output by using measures for the physical circuits or other organizational measures. One possibility is the shutdown of the power supply to the affected F-module. Required measures are often standardized for operations with defined design and risk reduction principles. For all other situations, necessary measures must be defined and approved.

Additional information on passivation and reintegration

For further information about fail-safe module access, refer to the *SIMATIC Safety - Configuring and Programming, Programming and Operating Manual* on the Internet (https://support.industry.siemens.com/cs/ww/en/view/54110126).

6.2 Fault diagnostics overview

Diagnostics detect faults that can affect the integrity of safety-related I/O. The faults can be in the fail-safe module, communication with the CPU, or external circuits. Diagnostic information is assigned either to a single channel or to the entire fail-safe module.

Most diagnostics operate without user selection. You can configure the following diagnostic options:

- Short-circuit testing using the digital input sensor supply can be enabled. The interval and duration of short-circuit tests is configurable.
- The readback times for 24 V DC digital outputs are configurable.
- The timeout intervals for failures in the safety communication or failure of a safety program to run is configurable.
- Dark testing of the digital outputs can be disabled (max. SIL 2, Cat. 3, PL d).

Refer to "Parameters/address space (Page 20)" for a complete description of these options.

The safety-critical and validated action of the diagnostics is to passivate I/O when faults are detected. The reporting of status and diagnostic results through the LED displays and diagnostic messages is subject to single point failures in electronics or software. These reports are offered as maintenance and debugging aids. Observe and interpret the reports with caution.

In the presence of single faults, any or all LED indications can be wrong. You should not rely solely on the presence or absence of red or green LED indicators to make safety decisions.

In the presence of single faults, diagnostic messages may fail to be delivered, or the numerical event ID or text message can be wrong. You should not rely solely on the presence, absence, or content of diagnostic reports to make safety decisions.

⚠ WARNING

Diagnostic and status reports through LEDs and text messages are subject to single point failure errors.
Reliance on such reported information to determine that a system or I/O point is in a safely-controlled state can result in death, severe personal injury, or property damage.
If the integrity of your fail-safe system is in doubt, you should use additional measures such as restricted access or power removal to control hazards during maintenance and debug activities.

6.3 Diagnostics performed at startup

Each fail-safe module executes self-diagnostics at power-up to assure that the electronics and software meet testable expectations before allowing the module to participate in process control. If tests are not successful, the module passivates either individual or all channels.

In addition to internal tests, some tests create signal changes at the terminals.

The F-DI 4/F-DQ 2 Fail-Safe module executes tests for its digital outputs of the P- and M-switches as defined by your configured parameters for "Maximum readback time" and "Maximum readback time switch on test" after receiving configuration parameters from the fail-safe CPU at power-up. P- and M-switch ON tests are sequenced so that normally or in the presence of a single detected fault, there is no complete PM circuit to energize the load.

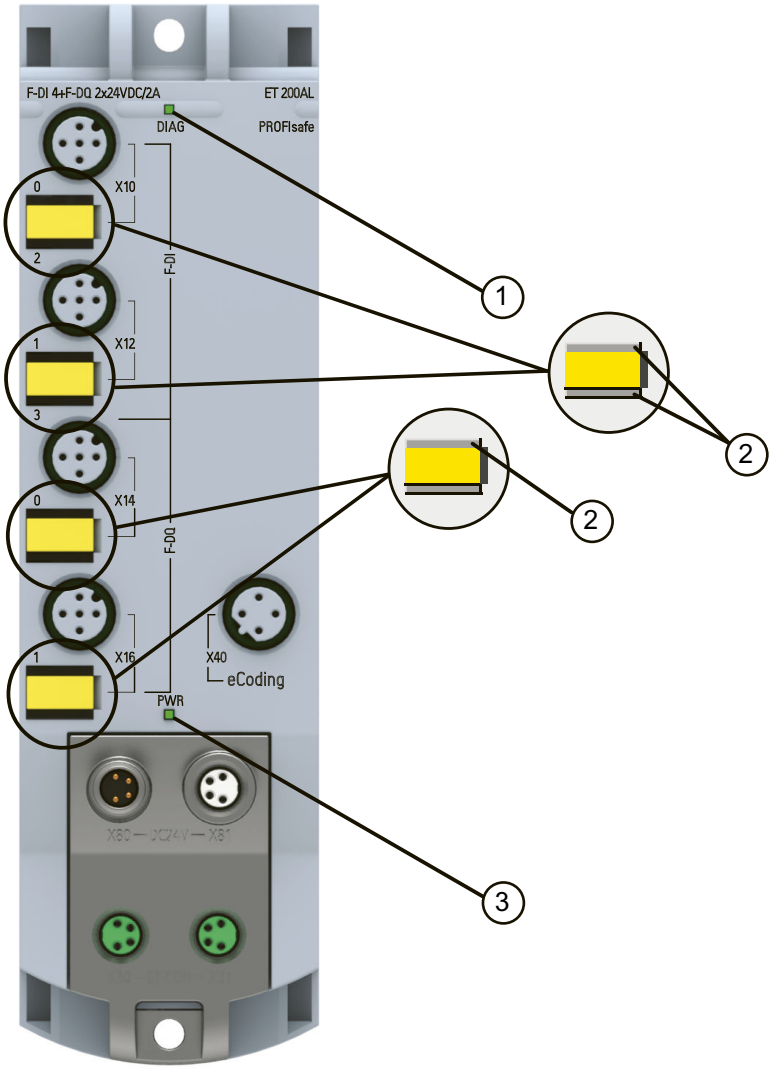
The F-DI 4/F-DQ 2 Fail-Safe module executes tests for its digital inputs of the sensor supply at power-up, including ON and OFF pulses, whether or not you have enabled the sensor supply or short-circuit testing in your configuration. If your configuration includes short-circuit testing, the module also executes a short-circuit test according to your configured parameters after receiving the parameters from the fail-safe CPU at power-up.

6.4 Diagnostics by LED display

6.4.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) of the F-DI 4/F-DQ 2 Fail-Safe module:



① Diagnostic status (DIAG (red/green))
② Channel status and channel error (red/green) for each channel (F-DI 0 - 3, F-DQ 0 and 1)
③ Load voltage 2L+ status (PWR (green))

Figure 2-196 LED displays

Meaning of the LEDs

The following tables set out the meaning of the status and error displays. Remedial measures for diagnostic alarms can be found in section Fault types, causes, and corrective measures (Page 65).

PWR LED

Table 2-388 Meaning of the PWR LED

PWR	Meaning
Off	Load voltage 2L+ missing or supply voltage 1L+ is too low or not present
On green	Load voltage 2L+ available

DIAG LED

Table 2-389 Meaning of the DIAG LED

DIAG LED	Meaning
Off	No supply voltage 1L+
Flashes green	Configuration/parameterization has not been received and no module diagnostics
Alternately Flashes red/green	Module-wide reintegratable faults such as the following are resolved and are awaiting reintegration: • Overvoltage • Undervoltage • PROFIsafe CRC error • PROFIsafe timeout error
On green	Module parameters assigned and no module or channel diagnostics
Flashes red	• Module diagnostic and/or one or more channel diagnostics • Module has inconsistent hardware and/or firmware versions

Channel LED for 1oo1 input channels

Table 2-390 Meaning of the channel LED for 1oo1 input channels

DIAGInput LEDs	Meaning
Off	Process signal = 0
On green	Process signal = 1
On red	Channel fault or module fault affecting the channel
Alternately Flashes red/green	Fault resolved, awaiting reintegration

Channel LEDs for 1oo2 input channels

Table 2-391 Meaning of the channel LEDs for 1oo2 input channels

Primary input LED	Secondary input LED	Meaning
Off	Off	Process signal = 0 (equivalent)
On green	On green	Process signal = 1 (equivalent)
Off	On green	Process signal = 0 (nonequivalent)
On green	Off	Process signal = 1 (nonequivalent)
On red	On red	Channel fault or module fault affecting the channel
Alternately Flashes red/green	Alternately Flashes red/green	Fault resolved, awaiting reintegration

Channel LED for output channels

Table 2-392 Meaning of the channel LED for output channels

Output LED	Meaning
Off	Process signal = 0 or channel deactivated
On green	Process signal = 1
On red	Channel fault or module fault affecting the channel
Alternately Flashes red/green	Fault resolved, awaiting reintegration

6.5 Fault types, causes, and corrective measures

The "Fault types, causes, and corrective measures" table below lists the messages of the F-DI 4/F-DQ 2 Fail-Safe module. These messages are displayed in the TIA Portal under "Online & diagnostics" > "Diagnostics" > "Diagnostic buffer". When you highlight an individual text line in the diagnostic buffer, the Event ID for that text item is displayed, along with module identity and location that generated the message. You may need to expand the window to see all information.

Table 2-393 Fault types, causes, and corrective measures

Event ID	Diagnostic message	F-DI 4/F-DQ 2 Fail-Safe module	Description	Possible causes	Corrective measures [1]
16x0001	Short-circuit	F-DI 4/F-DQ 2 digital outputs	A channel problem has been detected where either the P terminal or M terminal is at an unexpected potential	• Short-circuit of the output • Short-circuit between channels with different signals • Output overload • "Maximum readback time switch on test" value is configured too small • Short-circuit of output to M • Defective output driver	• Eliminate the short-circuit • Eliminate the overload • Increase "Maximum readback time switch on test" if permissible • Replace the fail-safe module
16x0005	Overtemperature	Module	• Overtemperature at microcontoller • Overtemperature at I/O	Shutdown due to violation of high temperature limit value in the module case	Check the ambient temperature. Once the fault has been eliminated, switch the power off and on
16x0006	Wire break	Module	Wire break failure. The module can detect a wire break when all of the following are true: • The channel is wired using a PM load • The PV=0 • The wire break diagnostic is enabled	Output is activated: • No load is connected to the PM output • Output is wired in output application mode 2 • Too small of a load is detected	• Change the output load characteristics • Deactivate unused channels • Disable wire break diagnostic for the offending channels
16x0009	Hardware revision mismatch	Module	• The module detects hardware mismatch • DIAG LED is flashes red		Replace module

[1] Once the fault is eliminated, reintegrate the fail-safe module (return to normal state) from passivation into the safety program.

Event ID	Diagnostic message	F-DI 4/F-DQ 2 Fail-Safe module	Description	Possible causes	Corrective measures [1]
16x0010	Parameterization failure (invalid parameters)	Module	When the module receives new parameters, the module checks for parameter failures. On detection of invalid parameters, the module stays in the configured state and signals the rejection of the faulty parameter to the fail-safe CPU. The module LEDs give an immediate indication of this fault.	• i-Parameter CRC error • Invalid i-parameters (for example, invalid selection, parameter out-of-range, unsupported feature selected, and wrong value of reserved field) • Any PROFIsafe parameterization problem detected by the PROFIsafe driver	Correct the parameter assignment
	Parameterization failure (address assignment failure)	Module	• On detection of an address assignment failure that indicates a hardware fault, the module enters the fatal error state. • The module performs this fault reaction if the address verification information provided by the F parameters is different than what has been previously assigned to the module	• Indicates assignment of an incorrect F address to one or more module(s) • Missing eCoding plug	• Reinsert the eCoding plug • Reassign the PROFIsafe F addresses using STEP 7 (TIA Portal) • Replace the eCoding plug
16x0040	Mismatch of safety destination address (F_Dest_Add)	Module	The PROFIsafe driver has detected a destination address mismatch. Checked after new parameters received.	• eCoding plug has been replaced with a different plug • eCoding plug is defective • Incorrect F-source address was downloaded as part of hardware configuration	• Reassign the PROFIsafe F addresses using STEP 7 (TIA Portal) • Replace the eCoding plug • Correct the F-destination address in hardware configuration and re-download
16x0041	Safety destination address not valid (F_Dest_Add)	Module	The PROFIsafe driver has detected an invalid destination address. Checked after new parameters received.	• eCoding plug has been replaced with a different plug • eCoding plug is defective	• Reassign the PROFIsafe F addresses using STEP 7 (TIA Portal) • Replace the eCoding plug

[1] Once the fault is eliminated, reintegrate the fail-safe module (return to normal state) from passivation into the safety program.

Event ID	Diagnostic message	F-DI 4/F-DQ 2 Fail-Safe module	Description	Possible causes	Corrective measures [1]
16x0042	Safety source address not valid (F_Source_Add)	Module	The PROFIsafe driver has detected a source address mismatch or an invalid source address. Checked after new parameters received.	• eCoding plug has been replaced with a different plug • eCoding plug is defective • Incorrect F-source address was downloaded as part of hardware configuration	• Reassign the PROFIsafe F addresses using STEP 7 (TIA Portal) • Replace the eCoding plug • Correct the F-source address in hardware configuration and re-download
16x004B	Inconsistent iParameters (iParCRC error)	Module	The firmware of the F-module has detected a CRC error.	• Communication between the F-CPU and F-module is disturbed • Impermissibly high electromagnetic interference is present	• Check PROFINET communications between the F-module and F-CPU • Eliminate the electromagnetic interference • Power switched OFF and ON for station • Reassign the PROFIsafe F addresses using STEP 7 (TIA Portal)
16x004D	PROFIsafe communication error (CRC)	Module	Transmission error in data message frame: Data inconsistent (CRC (cyclic redundancy check) error). Checked after new output telegram received.	Communication interference between the fail-safe CPU and the fail-safe module (for example, due to electromagnetic interference in excess of limits or sign-of-life monitoring error)	• Check the communications connection • Eliminate the interference
16x004E	PROFIsafe communication failure (timeout)	Module	Monitoring time exceeded for data message frame (timeout). Checked after new output telegram received.	F-monitoring time exceeded. Transmission error: timeout (watchdog time 1 or 2 elapsed)	• Adjust F-monitoring time • Check Safety program and all other CPU activities for excessive execution or demands: – Interrupts – Ethernet communication – OB scheduling conflicts – Long program paths
16x004F	Channel failure acknowledgement	Module	Channel configured for manual acknowledgement is ready to reintegrate	Manual acknowledgement required	Manually acknowledge correction of channel fault so that reintegration can occur
16x0100	Module is defective	Module	Fatal internal error	Fail-safe module is defective	Replace the fail-safe module

[1] Once the fault is eliminated, reintegrate the fail-safe module (return to normal state) from passivation into the safety program.

Event ID	Diagnostic message	F-DI 4/F-DQ 2 Fail-Safe module	Description	Possible causes	Corrective measures [1]
16x0103	Watchdog tripped	Module	The watchdog timer in the module communications processor timed out	Fail-safe module is defective	Replace the fail-safe module
16x0105	Short-circuit to L+	F-DI 4/F-DQ 2 digital outputs	Output shorted to P. The fail-safe module detects a channel problem where the P-terminal is unexpectedly at L+ potential.	• Short-circuit to L+ • Short-circuit between channels with different signals • Defective output driver • "Maximum readback time" value is configured too small	• Eliminate the short-circuit • Increase readback time • Replace the fail-safe module
16x0106	Short-circuit to ground	F-DI 4/F-DQ 2 digital outputs	The fail-safe module detects a channel problem where the M-switch output terminal is unexpectedly at M potential	• Short-circuit of output to M, ground, or another channel • Defective output driver • "Maximum readback time" value is configured too small	• Eliminate the short-circuit • Increase readback time • Replace the fail-safe module
16x011B	Invalid/ inconsistent firmware present	Module	Inconsistency between bus ASIC firmware and fail-safe controller firmware.	A firmware update operation was performed using an update file not suitable for the module (incorrect article number or hardware revision)	• The firmware update operation should be repeated with a suitable update file • Replace the fail-safe module
16x013E	Diagnostic event queue overflow	Module	Overflow of the diagnostic events queue has occurred. A newly-occurred diagnostic event could not be queued for transmission to the CPU because the buffer is full.	This can happen if channel errors come and go very quickly (for example, discrepancy errors)	Examine the Diagnostics buffer to see what errors are occurring, then address that issue

[1] Once the fault is eliminated, reintegrate the fail-safe module (return to normal state) from passivation into the safety program.

Event ID	Diagnostic message	F-DI 4/F-DQ 2 Fail-Safe module	Description	Possible causes	Corrective measures [1]
16x0300	Discrepancy failure, channel state 0/0	F-DI 4/F-DQ 2 digital inputs	External discrepancy failure: Channel state 0/0 with 1oo2 nonequivalent configuration	• Process signal faulty, sensor may be defective • Configured discrepancy time too short • Short-circuit • Sensor mechanical activation or alignment out of tolerance	• Check the process signal, replace sensor if necessary • Check the configured discrepancy time • Check the wiring • Check that both sensors are mounted and aligned to be activated together
16x0301	Discrepancy failure, channel state 0/1	F-DI 4/F-DQ 2 digital inputs	External discrepancy failure: Channel state 0/1 with 1oo2 equivalent configuration		
16x0302	Discrepancy failure, channel state 1/0	F-DI 4/F-DQ 2 digital inputs	External discrepancy failure: Channel state 1/0 with 1oo2 equivalent configuration		
16x0303	Discrepancy failure, channel state 1/1	F-DI 4/F-DQ 2 digital inputs	External discrepancy failure: Channel state 1/1 with 1oo2 nonequivalent configuration		
16x0306	Internal sensor supply short-circuit to P	F-DI 4/F-DQ 2 digital inputs	Module-provided sensor supply voltage shorted to P	• Sensor supply shorted to P • Short-circuit test duration configured too short • Failed sensor supply	• Eliminate the short-circuit • Increase short-circuit test duration • Replace the fail-safe module
16x0307	Overload or internal sensor supply short-circuit to ground	F-DI 4/F-DQ 2 digital inputs	Internal sensor supply voltage shorted to M, ground, or excessive load on sensor supply	• Short-circuit • Excessive load on sensor supply • Failed sensor supply	• Eliminate the short-circuit • Reduce load on sensor supply • Replace the fail-safe module
16x030D	F-address memory not accessible	Module	The memory where the F-address is stored is not accessible	• eCoding plug is missing • eCoding plug is defective	• Install an eCoding plug into X40 of the module • Replace the defective eCoding plug
16x030E	No valid F-address available	Module	Fail-safe address is not valid (F-address and CRC inconsistent)	• eCoding plug has never been assigned a PROFIsafe address • eCoding plug is defective	• Assign the PROFIsafe Address • Replace the eCoding plug
16x0311	Frequency too high	F-DI 4/F-DQ 2 digital outputs	Switching frequency exceeded; readback not in time	Process value from safety program changing too rapidly for module to follow	Change Safety program logic to guarantee more time between output changes
16x0312	Undertemperature	Module	• Under-temperature at microcontrollers • Under-temperature at I/O	Shutdown due to violation of low temperature limit value in the module case	• Check the ambient temperature • Once the fault has been eliminated, switch the power off and on

[1] Once the fault is eliminated, reintegrate the fail-safe module (return to normal state) from passivation into the safety program.

Event ID	Diagnostic message	F-DI 4/F-DQ 2 Fail-Safe module	Description	Possible causes	Corrective measures [1]
16x0313	Failure in the input circuit	F-DI 4/F-DQ 2 digital inputs	Internal fault at the read circuit/test circuit	• The module digital inputs detect a failure during bit pattern testing of inputs • EMI or module hardware fault	• If intermittent, it is probably due to interference; eliminate the interference • If persistent, or repeats after efforts to eliminate interference, replace the fail-safe module
16x031C	Input shorted to P	F-DI 4/F-DQ 2 digital inputs	Input shorted to P failure	• External wiring or sensor shorts input signal to L+ • Input configured for internal sensor supply with short-circuit detection enabled, but wired to external L+ • Input defective	• Check/correct external short-circuit • Make wiring and configuration agree • Replace the fail-safe module
16x031E	Read back failure	F-DI 4/F-DQ 2 digital outputs	The module has detected a channel problem where the expected terminal voltage(s) are not reached	• "Maximum readback time" or "Maximum readback time switch on test" configured value is too small • Output switch failure	• Increase readback time • Replace the fail-safe module if output does not respond
16x0320	Overload	F-DI 4/F-DQ 2 digital outputs	Overload condition at the output driver that leads to passivation of the channel	Overload at output	Eliminate overload
16x0321	Supply or load voltage too high	Module	Supply voltage (1L+) or load voltage (2L+) maximum exceeded	Supply or load voltage is set too high	Adjust supply or load voltage
16x0322	Supply or load voltage too low	Module	Supply voltage (1L+) or load voltage (2L+) minimum exceeded	Supply or load voltage is set too low	Adjust supply or load voltage

[1] Once the fault is eliminated, reintegrate the fail-safe module (return to normal state) from passivation into the safety program.

Electromagnetic interference and diagnostic reports

Electromagnetic interference can cause communication errors, disturb external and internal signal measurements, and cause processing errors. When error reports do not apparently relate to an identifiable device failure, wiring problem, programming, or configuration error, consider sources of electromagnetic interference and installation and wiring problems that might introduce electromagnetic interference in your installation. Typical problem sources include poor suppression of inductive loads and voltage dips due to excessive load inrush currents.

Technical specifications

7

7.1 Specifications

	6ES7146-5FF00-0BA0
General information	
Product type designation	F-DI 4+F-DQ 2x24VDC/2A, 4xM12
HW functional status	FS01
Firmware version	V1.0.x
Product function	
I&M data	Yes; I&M0 to I&M3
Engineering with	
STEP 7 TIA Portal configurable/integrated as of version	Step 7 V17 or higher
Operating mode	
DI	Yes
DQ	Yes
Supply voltage	
Load voltage 1L+	
Rated value (DC)	24 V
permissible range, lower limit (DC)	20,4 V
permissible range, upper limit (DC)	28,8 V
Reverse polarity protection	Yes; against destruction
Load voltage2 L+	
Rated value (DC)	24 V
permissible range, lower limit (DC)	20,4 V
permissible range, upper limit (DC)	28,8 V
Reverse polarity protection	Yes; against destruction; outputs applied with reversed polarity for loads connected between M-switch and 2L+ will conduct
Input current	
Current consumption (rated value)	55 mA (1L+) / 40 mA (2L+); without load
from load voltage 1L+ (unswitched voltage)	4 A; Maximum value
from load voltage 2L+, max.	4 A; Maximum value
Encoder supply	
Number of outputs	2
24 V encoder supply	
Short-circuit protection	Yes; per load voltage, electronic (response threshold 0.7 A to 1.7 A)
Output current, max.	1 A; total current of all encoders, max. 0.5 A per load voltage; maximum of 2.0 V drop
Power loss	
Power loss, typ.	4,7 W

	6ES7146-5FF00-0BA0
Digital inputs	
Number of digital inputs	4
Input characteristic according to IEC 61131	Type 1
Number of simultaneously controllable inputs	
all mounting positions	
up to 55 °C, max.	4
Input voltage	
Rated value (DC)	24 V
for signal "0"	-30 to +5 V
for signal "1"	+15 to +30 V
Input current	
for signal "1", typ.	4,85 mA
Input delay (for rated value of input voltage)	
for standard inputs	
parameterizable	Yes
at "0" to "1", min.	0,8 ms
at "0" to "1", max.	12,8 ms
at "1" to "0", min.	0,8 ms
at "1" to "0", max.	12,8 ms
Cable length	
unshielded, max.	30 m
Digital outputs	
Number of digital outputs	2
in groups of	2
Short-circuit protection	Yes; per channel, electronic
Response threshold, typ.	10 A; measured at M-switch, threshold for P-switch is higher
Open-circuit detection	Yes; per channel, only detects when output is off
Overload protection	Yes
Response threshold, typ.	3,4 A; measured at P-switch
Limitation of inductive shutdown voltage to	P-switch: -26 V DC referenced to 2M, M-switch: +48 V DC referenced to 2M
Switching capacity of the outputs	
on lamp load, max.	10 W
Load resistance range	
lower limit	12 Ω
upper limit	2 kΩ
Output voltage	
for signal "1", min.	L + (-2.0 V), P-switch is L+ (-1.5 V), M-switch is 0.5 V
Output current	
for signal "1" rated value	2 A
for signal "0" residual current, max.	0,5 mA
Switching frequency	
with resistive load, max.	30 Hz
with inductive load, max.	0,1 Hz
on lamp load, max.	10 Hz

	6ES7146-5FF00-0BA0
Total current of the outputs	
Current per group, max.	4 A
Cable length	
unshielded, max.	30 m
Encoder	
Connectable encoders	
2-wire sensor	No
permissible quiescent current (2-wire sensor), max.	0.5 mA
Interrupts/diagnostics/status information	
Substitute values connectable	No
Alarms	
Diagnostic alarm	Yes; Parameterizable
Diagnoses	
Monitoring the supply voltage	Yes
Wire-break	Yes; outputs when off
Short-circuit	Yes; inputs, outputs, encoder supply
Diagnostics indication LED	
Channel status display	Yes; green LED
for channel diagnostics	Yes; red LED
for module diagnostics	Yes; green/red LED
For load voltage monitoring	Yes; green LED
Potential separation	
between the load voltages	Yes
Potential separation channels	
between the channels. in groups of	4 DI channels are isolated from 2 DQ channels
between the channels and backplane bus	Yes
between the channels and the power supply of the electronics	DI channels are not isolated from supply voltage 1L+ and DQ channels are isolated from supply voltage 1L+
Isolation	
Isolation tested with	707 V DC (type test)
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Highest safety class achievable in safety mode	
Performance level according to ISO 13849-1	PLd (DI single-channel), PLe (DI two-channel, DQ)
Category according to ISO 13849-1	Cat. 3 (DI single-channel), Cat. 4 (DI two-channel, DQ)
SIL acc. to IEC 61508	SIL 2 (DI single-channel), SIL 3 (DI two-channel, DQ)
Probability of failure (for service life of 20 years and repair time of 100 hours)	
Low demand mode: PFDavg in accordance with SIL2	< 1.0E-03 DI single-channel; < 1.0E-03 DQ with dark test disabled
Low demand mode: PFDavg in accordance with SIL3	< 1.0E-05 DI two-channel; < 2.0E-05 DQ with dark test enabled

	6ES7146-5FF00-0BA0
High demand/continuous mode: PFH in accordance with SIL2	< 1.0E-08 1/h DI single-channel; < 1.0E-07 1/h DQ with dark test disabled
High demand/continuous mode: PFH in accordance with SIL3	< 1.0E-09 1/h DI two-channel; < 1.0E-08 1/h DQ with dark test enabled
Ambient conditions	
Ambient temperature during operation	
min.	-30 °C
max.	55 °C
Connection method	
Design of electrical connection for the inputs and outputs	M12, 5-pin
Design of electrical connection for supply voltage	M8, 4-pin
ET-Connection	
ET-Connection	M8, 4-pin, shielded
Dimensions	
Width	45 mm
Height	159 mm
Depth	40 mm
Weights	
Weight, approx.	220 g

Dimension drawing

A

A.1 Dimension drawing

The figure below shows the dimension drawing of the F-DI 4/F-DQ 2 Fail-Safe module in front and side views. The dimensions are in mm.

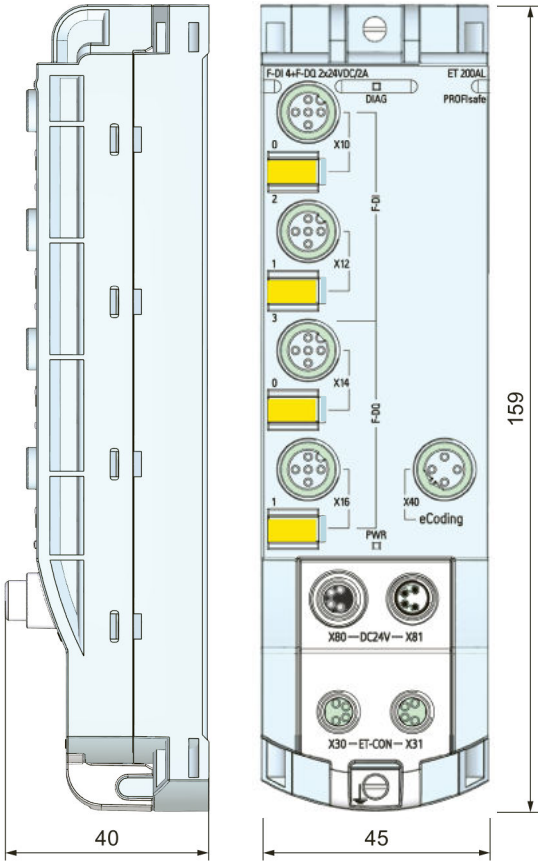


Figure 2-197 Dimension drawing

Response times

B

B.1 Maximum response time

This section shows the response times of the F-DI 4/F-DQ 2 Fail-Safe module. The response times are included in the calculation of the F-system response time.

Definition of response time for fail-safe digital outputs

The response time represents the interval between an incoming safety message frame from the ET-Connection and the signal change at the digital output.

Times required for the calculation

Maximum cycle time: T_{cycle} = 23 ms

Maximum acknowledge time (Device Acknowledge Time): T_{dat} = 18 ms

You assign the "Maximum readback time" and "Maximum readback time switch on test" settings in STEP 7.

Calculating the maximum response time of the system

You can calculate your maximum system response time using the "SIMATIC STEP 7 Safety Advanced: F-Execution Times, F-Runtimes, F-Monitoring and Reaction Times (http://support.automation.siemens.com/WW/view/en/49368678/133100)" Excel file (RT_calculator). Use your configured individual fail-safe module timing parameters and the module characteristic parameters found in this appendix to determine the maximum response time of your system.

Data transport delays included

The T_{cycle} parameter values given above include an allowance for the fail-safe module to acquire and deliver PROFIsafe messages in transactions with the PLC I/O bus. The execution time of the Safety FB in the fail-safe CPU includes the physical transport delay time for PROFIsafe messages moving between the fail-safe module location and the fail-safe CPU. There are no separate transport delay parameters that you can include in your calculations.

B.2 Response time parameters for the F-DI 4/F-DQ 2 digital inputs

Maximum Device Acknowledge Response Time of the F-DI 4/F-DQ 2 Fail-Safe module digital inputs

1oo1 evaluation:

$T_{WCDT_i} = T_{filter} + T_{sct} + 2 \times T_{cycle}$

$T_{OFDT_i} = T_{WCDT_i} + T_{scf}$

1oo2 evaluation:

$T_{WCDT_i} = T_{filter} + T_{sct} + 2 \times T_{cycle}$

$T_{OFDT_i} = T_{WCDT_i} + MAX (T_{scf}, T_{dis})$

Where:

T_{cycle}	Internal cycle time of the fail-safe module
T_{dis}	Discrepancy time: • Configured "Discrepancy time" for 1oo2 channels changing from "0" to "1" • Configured "Discrepancy time" for 1oo2 channels changing from "1" to "0" and "Supply last valid value" option configured for discrepancy behavior • "0" for 1oo2 channels changing from "1" to "0" and "Supply value 0" option configured for discrepancy behavior You should include the expected discrepancy time between your sensor inputs in your external sensor delay. Your configured T_{dis} contributes to T_{OFDT_i} as the time delay for the fail-safe module's digital inputs to passivate the channel due to fault case extension of the discrepancy time. This parameter can be listed separately in the RT_calculator. Do not include T_{dis} in the value of T_{OFDT_i} that you enter into the RT_calculator if you enter T_{dis} as a separate item.
T_{filter}	Configured "Input filters" time for the channel
T_{OFDT_i}	One Fault Delay Time: Maximum response time for the fail-safe module's digital input to report a channel as passivated
T_{scf}	Time delay for short-circuit fault duration: • Configured "Interval for short-circuit test", when operating in high demand or continuous mode and depending on the short-circuit test to achieve your required level of safety integrity • "0" when not depending on the short-circuit test to achieve your required level of safety integrity
T_{sct}	Time delay for short-circuit test duration: • "0" if no short-circuit test configured • "0" for 1oo2 channels changing from "1" to "0" and "Supply value 0" option configured for discrepancy behavior • "Duration of short-circuit test" + "Input filters" time if short-circuit test is configured (Confirmation: "Input filters" can occur twice in equation for T_{WCDT_i} if short-circuit test is configured.)
T_{WCDT_i}	Worst Case Delay Time: Maximum response time from a signal transition at the digital input to the reliable availability of the safety message frame available for the fail-safe CPU request

The term "2 x T_{cycle}" for "maximum response time of the fail-safe module" allows for other input delays to complete just after the beginning of a cycle. The fail-safe module's digital inputs process and report the changed input data on the next cycle.

B.3 Response time parameters for the F-DI 4/F-DQ 2 digital outputs

Maximum response time of the F-DI 4/F-DQ 2 Fail-Safe module digital outputs

$T_{WCDT_q} = T_{rb} + MAX (T_{rb}, T_{rb_swon}) + 2 \times T_{cycle}$

$T_{OFDT_q} = T_{WCDT_q}$

When dark testing is disabled, a channel fault might not be detected until a process value change "1" to "0" takes place on the corresponding output. When dark testing is disabled and the process value is "1" for a given channel, the respective output switches are not manipulated by the various safety measures.

Where:

T_{cycle}	Internal cycle time of the fail-safe module
T_{OFDT_q}	One Fault Delay Time: Maximum response time for the module's digital outputs to turn an output OFF upon detection of a channel or module fault
T_{rb}	Configured "Maximum readback time" for the channel
T_{rb_swon}	Configured "Maximum readback time switch on test" for the channel
T_{WCDT_q}	Worst Case Delay Time: Maximum response time of the fail-safe module's digital output DC from the receipt of a safety message frame from the safety program in the fail-safe CPU to the signal transition at the digital output

The term "2 x T_{cycle}" allows for a new process value to be delivered from the fail-safe CPU just after the beginning of a cycle. The fail-safe module's digital outputs process the changed output request and apply new data to the output switches on the next cycle.

After the fail-safe module's digital outputs command the output switch to change, the actual voltage on the load might not be realized until the configured readback time completes. If a bit pattern test is in progress, the new process value cannot be applied to the switches until the applicable readback time completes.

Minimum permissible OFF time for F-DI 4/F-DQ 2 Fail-Safe module digital outputs

The fail-safe module's digital outputs expect to complete and confirm each ON to OFF transition before receiving a new command to go from OFF to ON. A process value of "0" presented for less than T_{WCDT_q} can cause the channel to passivate.

Switching of loads

C

C.1 Connecting capacitive loads

If an F-DI 4/F-DQ 2 Fail-Safe module is interconnected with loads that require little current and have capacitance, this can lead to detection of a short circuit or overload. Reason: The capacitance cannot be sufficiently discharged or charged during the configured readback time of the bit pattern test.

Load capacitance can delay the voltage response as seen at the P- and M-switches of the F-DI 4/F-DQ 2 Fail-Safe module digital outputs. For a capacitive load with capacitance C across P and M, and a parallel load resistance R, the "Maximum readback time" needs to be in the range of 2.0 to 2.5 time constant (R * C) of the load. This allows enough time for an appreciable voltage change to be seen when you briefly de-energize an energized load during bit pattern testing. If the resulting "Maximum readback time" is too long for your application, you can reduce this time constant by adding parallel resistance across the load to reduce the realized R * C time constant.

Alternatively, you can add a diode between the P-output and the load (capacitor and resistors) so that when you turn off the output, the voltage on the capacitor is not present at the P-output. Typically, power supplies with input capacitors that have reverse voltage protection have this diode built into the power supply. Using the added diode, you can greatly reduce the "Maximum readback time" to some portion of the hold-up time of the power supply/capacitor. This reduced "Maximum readback time" allows the load to operate normally (load stays ON) during the bit pattern tests.

Stray capacitance between the load circuit and ground, M, and P increases the time required for the "Maximum readback time switch on test". When module diagnostics switch "ON" a P- or M-switch to a de-energized load during bit pattern testing, both sides of the load are driven towards L+ or M, limited by stray capacitance. This effect is typically small.

Your "Maximum readback time switch on test" setting should be long enough for the load circuit voltage to react, but short enough that if one side of the load faults to P or M, testing of the opposite switch should not cause the load to mechanically react.

Capacitive loads (including power supplies with input capacitors) with low series resistance can have a large inrush current. If you have a large capacitive load, you should add series resistance to reduce the inrush current to reduce the risk of opened fuses or overcurrent fault detection on normal load switch ON events.

C.2 Switching of inductive loads

The diagram below shows the maximum permitted inductive load and switching frequency allowed using only the internal suppression circuits of the F-DI 4/F-DQ 2 Fail-Safe module digital outputs. You should equip larger or more frequently switched inductive loads with external suppression circuits to avoid early failure of the F-DI 4/F-DQ 2 Fail-Safe module digital output switch. External suppression conducts the load current at a voltage less than the internal suppression threshold to avoid overloading the internal suppression.

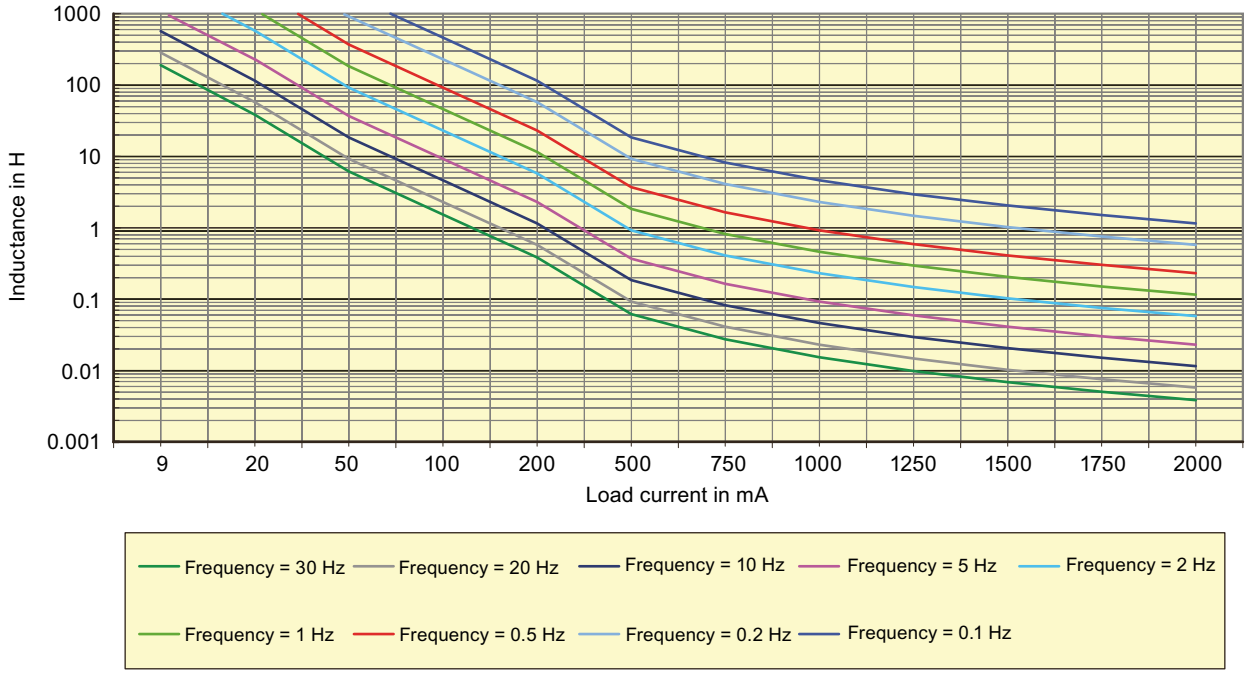


Figure 2-198 Switching of inductive loads for the F-DI 4/F-DQ 2 Fail-Safe module depending on the load current and switching frequency

⚠ WARNING

Unsuppressed inductive loads can lead to failures.
The following failures can result:

- Unsuppressed inductive loads can lead to early "stuck-on"' failures of the fail-safe module digital outputs.
- Unsuppressed inductive load switching generates an EMI hazard to the PLC system and correct processing of the safety function.

Death or serious personal injury and damage to machines and equipment may result if proper precautions are not taken.
You should use suppressor circuits with inductive loads to limit the voltage rise when a control output turns off and to limit the electrical noise generated when switching inductive loads.

SIEMENS

SIMATIC
ET200
Product Information for ET 200AL F-IO Firmware Update V1.0.1

Product Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/cert).

Description

Description
The firmware update V1.0.1 for the ET 200AL F-IO module is now available.

The firmware update includes the following features:

- Corrections for problems with the delivery of diagnostic messages. In some situations, diagnostic messages for resolved fault conditions were not successfully delivered by the module.

Refer to the ET 200AL System Manual (https://support.industry.siemens.com/cs/us/en/view/95242965) for more information about the ET 200AL product family. Refer to the the description on the Internet (https://support.industry.siemens.com/cs/us/en/view/109475743) of how to perform a firmware update for the SIMATIC ET 200AL.

NOTE

You cannot accomplish firmware update V1.0.1 by means of a SIMATIC Memory Card installed in a CPU. Please use one of the following approaches:

- Online via PROFINET (with STEP 7)
- Via the integrated web server of an F-CPU
- Via the SIMATIC Automation Tool

Table: Models affected by ET 200AL F-IO firmware update V1.0.1

© Siemens 2022. All rights reserved

ET 200AL model	Description	Article number
ET 200AL F-IO	ET200AL F-DI 4+F-DQ 2x24VDC/2A, 4xM12	6ES7146-5FF00-0BA0

SIEMENS

SIMATIC
Distributed I/O
Configuring ET 200AL F-DI 4+F-DQ 2x24VDC/2A, 4xM12 (6ES7146-5FF00-0BA0) with a GSDML File

Product Information

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.
Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.
For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).
Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.
To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Introduction

Note the following dependencies for PROFINET IO during configuration of ET 200AL fail-safe modules with a GSDML file.

NOTE

When using ET 200AL fail-safe modules with a GSDML file on non-Siemens PROFIsafe masters, note that the warnings, information, and references contained in the F-module device manuals are still valid.
Please also observe the warnings, information, and references of the non-Siemens master.

Requirement

S7-FCT is required to calculate the F_iPar_CRC and perform PROFIsafe addressing for the F-I/O according to PROFIsafe address type 2.
You can find instructions and additional information for the SIMATIC S7-FCT V3.0 - Fail-safe Configuration Tool on the Internet (https://support.industry.siemens.com/cs/us/en/view/109763833).
You can find S7-FCT on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109762827).

NOTE

If identification of the F-module does not succeed during the assignment of the PROFIsafe address (for example, the F-module's channel LEDs flash continuously), you can take the following corrective measures:

- Repeat the assignment of the PROFIsafe address after approximately 5 minutes.
- Power cycle the F-module and then repeat the assignment of the PROFIsafe address.
- Increase the PROFINET update time of F-host and IM for the duration of the PROFIsafe address assignment.

© Siemens 2022. All rights reserved

S7-FCT, in conjunction with a GSDML file, allows you to configure selected F-I/Os from Siemens in versions of STEP 7 that do not natively support the F-I/O and in an engineering system from another manufacturer.

Configuration software	Support as of	Information on installation	Requirements
STEP 7 (TIA Portal) V17	or later	STEP 7 online help	S7-FCT V3.0 or later
STEP 7 (TIA Portal) V16	Upd1 or later		
STEP 7 (TIA Portal) V15.1	Upd5 or later		
STEP 7 (Classic) V5.7	or later	STEP 7 help	
STEP 7 (Classic) V5.6 SP2	HF2 or later		
STEP 7 (Classic) V5.5 SP4	HF19 or later		
Software of other manufacturer		Documentation of the manufacturer	

Configuring the ET 200AL F-DI 4+F-DQ 2x24VDC/2A, 4xM12 (6ES7 146-5FF00-0BA0) as of firmware version V1.0.0 or later

In TIA Portal, the "IO Tags" tab displays more tags than are supported by the F-module.

Configuring F-I/O module parameters using GSDML

You specify the properties of the F-I/O module in STEP 7 using various parameters. Depending on the settings, not all parameters are available.

You set the parameters of the module as follows:

1. Insert the IM 157-1 PN interface module. When using STEP 7, the interface module is found in the hardware catalog under "Other field devices->PROFINET IO->I/O->SIEMENS AG->ET 200AL".
2. Insert the F-I/O module. When using STEP 7, the F-I/O module is found in the hardware catalog under "Module->DIQ->F-DI 4+F-DQ 2x24VDC/2A, 4xM12". Select PROFIsafe V2.4 or PROFIsafe V2.6 based upon the specifications of your fail-safe controller. If you are using Siemens fail-safe controllers, select PROFIsafe V2.4 if you are using an S7-300 or S7-400 F-CPU or select PROFIsafe V2.6 if you are using an S7-1200 or S7-1500 F-CPU.
3. Access the F-I/O module's parameters in your programming package. To display the module's parameters in STEP 7, on the Device view or Device overview select the F-I/O module and select the module's "Properties" tab.
4. In the "Properties" view, on the "General" tab, select "PROFIsafe" and the drop-down arrows for "Module parameters>I/O parameters" to see a subset of the properties of the "PROFIsafe" and "I/O parameters".
5. Set values for "PROFIsafe" or "I/O parameters" in the right side property fields.
6. Right click the F-I/O module name in the Device view and click "Start device tool ..." to launch S7-FCT.
   - Select "F_iPar_CRC calculation" and click Start.
   - If asked, choose and confirm the desired communication interface.
   - Examine the parameters, and if correct, press "Confirm i-parameters" to calculate the F_iPar_CRC.
   - If parameters are not correct, close out of S7-FCT and return to the module Properties dialog to correct the parameter settings.
   - Click the copy button next to the hexadecimal representation of the F_iPar_CRC (left value) to place this value on the clipboard.
   - Close out of S7-FCT.
7. In the "Properties" view on the "General" tab for the module, select "PROFIsafe" in the tree and paste the clipboard value into the F_iPar_CRC field.
8. A successful compile and download of your hardware configuration to an F-CPU automatically configures your F-I/O module.

Assigning PROFIsafe addresses for F-I/Os

These are the three basic steps for assigning PROFIsafe addresses:

1. Configure the F-destination address of each F-module and the F-source address of the F-CPU in the hardware configuration in STEP 7 Safety and download the hardware configuration.
2. Identify the F-I/O module to which you want to assign the configured F-destination and F-source addresses. F-destination addresses are generally assigned with lower numbers (for example, less than 100) for GSDML configured devices.
3. Use "Assigning the PROFIsafe addresses to the F-I/Os" section in the instructions for the SIMATIC S7-FCT V3.0 - Fail-safe Configuration Tool on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109763833) to assign the PROFIsafe address (F-destination address together with F-source address) to each F-module before you put it into operation. To launch the PROFIsafe-Address Assignment dialog:
   - Right click the F-I/O module name in the Device view and click "Start device tool ..." to launch S7-FCT.
   - Select "PROFIsafe address assignment" and click Start.
   - If asked, choose and confirm the desired communication interface.

NOTE

Refer to the *SIMATIC Safety - Configuring and Programming* manual (https://support.industry.siemens.com/cs/ww/en/view/54110126) for further information about PROFIsafe address identification and assignment.

Dependencies ET 200AL F-DI 4+F-DQ 2x24VDC/2A, 4xM12 (6ES7146-5FF00-0BA0) as of firmware version V1.0.0 or later

Dependencies for 1oo2 evaluation

In a 1oo2 channel configuration, you must set the following 1oo2 DI channel parameters to the same value:

- Activated check box
- Input filter
- Channel failure knowledge (PROFISAFE V2.6 only)
- Sensor supply

SIEMENS

SIMATIC

ET 200AL
Voltage distributor PD 24VDC (6ES7194-2CA00-0AA0)

Equipment Manual

Introduction 1

Product overview 2

Connecting 3

Interrupts/diagnostic messages 4

Technical specifications 5

Dimension drawing A

08/2025
A5E53729593-AA

Table of contents

1 Introduction 3

1.1 Introduction 3

1.2 ET 200AL Documentation Guide 3

1.3 SIMATIC Technical Documentation 5

2 Product overview 7

2.1 Properties 7

2.2 Operator controls and display elements 9

3 Connecting 10

3.1 Terminal and block diagram 10

3.2 Pin assignment 11

4 Interrupts/diagnostic messages 13

4.1 Status and error displays 13

5 Technical specifications 15

5.1 Technical specifications 15

5.2 Derating 17

A Dimension drawing 18

A.1 Dimension drawing 18

Introduction

1

1.1 Introduction

Purpose of the documentation

This Equipment Manual supplements the System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965). Functions that are generally applicable to the ET 200AL distributed I/O system are described there.

The information provided in the present manual, the system manual and the function manuals enables you to commission the ET 200AL distributed I/O system.

Conventions

Also observe notes marked as follows:

NOTE

A note contains important information:

- On the product described in the documentation
- On handling the product
- On the part of the documentation to which particular attention is paid

---

1.2 ET 200AL Documentation Guide



The documentation for the SIMATIC ET 200AL distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109742667)

Basic information



The System Manual describes in detail the configuration, installation, wiring and commissioning of the SIMATIC ET 200AL distributed I/O system.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- ET 200AL System Manual
- STEP 7 Professional
- Product information

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC ET 200AL distributed I/O system.

Examples:

- Function Manual ET 200AL/ET 200SP Mixed Configuration
- Function Manual Diagnostics
- Function Manual Communication
- PROFINET Function Manual
- PROFIBUS Function Manual
- Function Manual Designing Interference-free Controllers
- Function Manual IO-Link system

Manual Collection ET 200AL

The Manual Collection contains the complete documentation on the SIMATIC ET 200AL distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/95242965)

1.3 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Product overview

2

2.1 Properties

Article number

6ES7194-2CA00-0AA0

View of the module



Figure 2-199 View of the voltage distributor PD 24VDC

Properties

The module has the following technical properties:

- 24 V DC supply voltage
- 1 input M12 connector, L-coded
- 4 outputs M8 socket, 4-pole
- Max. input current for 1L+ and 2L+ is 15 A each
  Derating (Page 17) of the max. input current for temperatures > 25 °C

- Max. output current per output for 1L+ and 2L+ is 4 A each

NOTE

The electronic short-circuit protection for each output makes an additional fusing of the connected modules superfluous. Check this possibility in the technical specifications of the used module and the connecting cable with connector.

- Dimensions: 45 x 159 x 45 mm

Accessories

The following component is included with the module in the packaging:

- Identification labels

Other components

The following component can be ordered as spare part:

- Identification labels

The following components can be ordered as accessories:

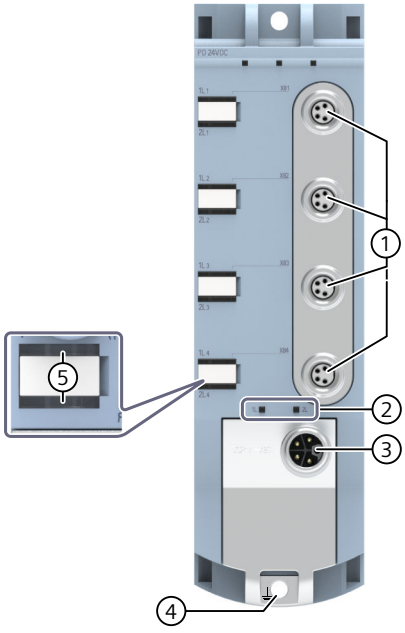
- Connectors
- Cables
- M8 sealing cap

See also

You will find more information on accessories and the other components in the System Manual ET 200AL distributed I/O system (https://support.industry.siemens.com/cs/ww/en/view/89254965) in the Accessories/Spare parts section.

2.2 Operator controls and display elements

The figure below shows the operator controls and display elements of the voltage distributor PD 24VDC.



① X81 ... X84: Socket outputs of the voltages 1L+ and 2L+
② 1L/2L: LED displays for the input voltages 1L+ and 2L+
③ X80: Connector for infeed of input voltages 1L+ and 2L+
④ Functional earth (FE)
⑤ 1L*/2L*: LED displays for the output voltages of the outputs X81 ... X84

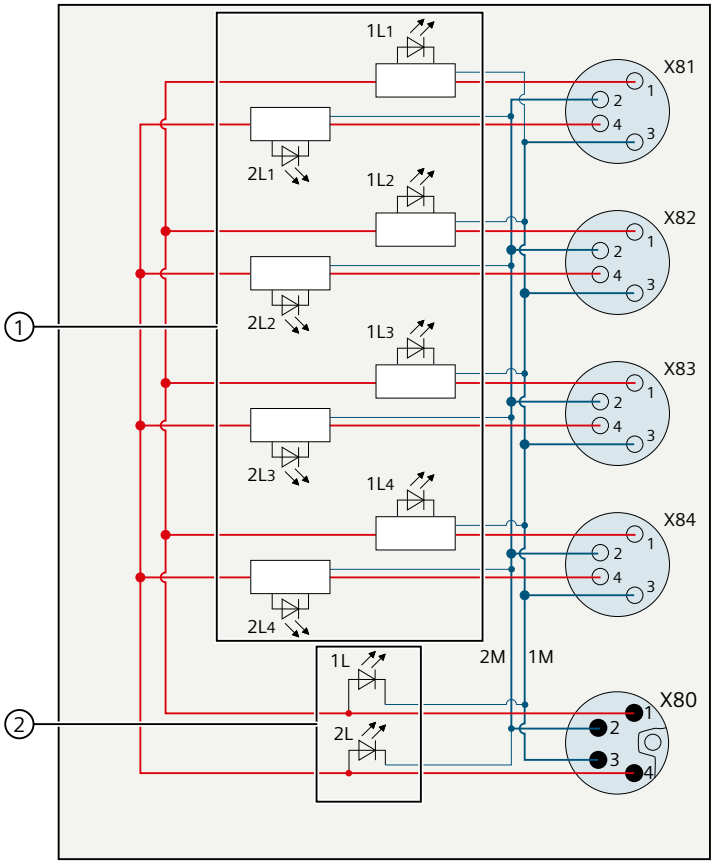
Figure 2-200 View of the voltage distributor

Connecting

3

3.1 Terminal and block diagram

The figure below shows the connection and schematic circuit diagram of the voltage distributor PD 24VDC.



① Electronic short-circuit protection with status LEDs for the outputs
② LED displays for the supply voltages
X80 Infeed of supply voltages
X81 ... X84 Outputs
1L+ Supply voltage 1L+ (non-switched)
1M Ground 1M (non-switched)
2L+ Load voltage 2L+ (switched)
2M Ground 2M (switched)

Figure 2-201 Terminal and block diagram

Connection example

The following figure shows a connection example of the voltage distributor PD 24VDC with different modules.

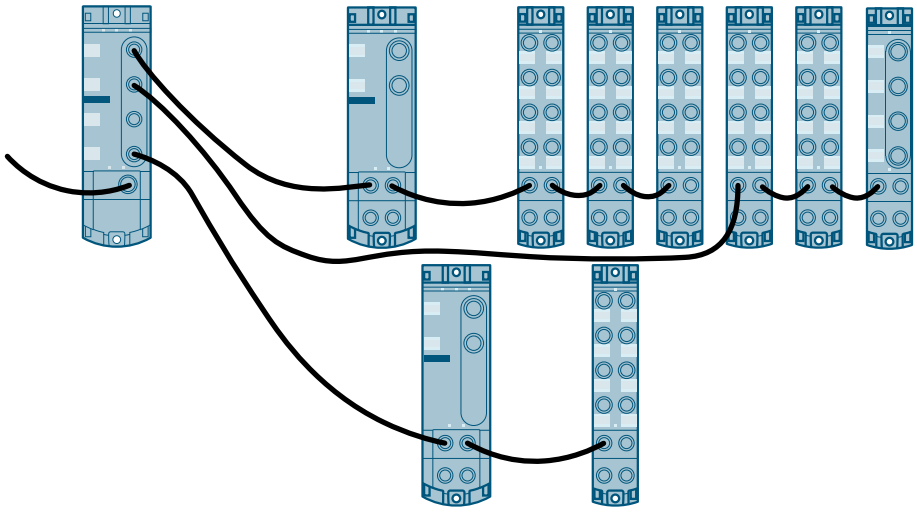


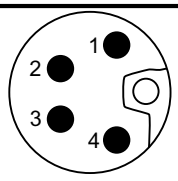
Figure 2-202 Connection example

3.2 Pin assignment

Pin assignment of the connector for infeed of the supply voltage (M12 L-coded)

The table below shows the pin assignment of the M12 L-coded connector for infeed of the supply voltage.

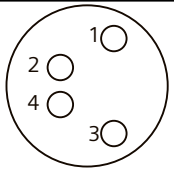
Table 2-394 Pin assignment of the supply voltage connector

Pin	Assignment X80 - connector (POWER input)	Assignment of the wire color of the power line cable	Front view of the connector
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

Pin assignment of the M8 sockets of the outputs

The following table shows the pin assignment of the M8 sockets.

Table 2-395 Pin assignment of the outputs

Pin	Assignment **X81 ... X84 - socket (power output)**	Assignment of the wire color of the power line cable	Front view of the socket
1	Supply voltage 1L+ (non-switched)	Brown	
2	Ground 2M (switched)	White	
3	Ground 1M (non-switched)	Blue	
4	Load voltage 2L+ (switched)	Black	

NOTICE

Do not apply input voltage at the outputs
If you apply an input voltage at the outputs, this can result to a fuse blown or the destruction of modules or of devices.

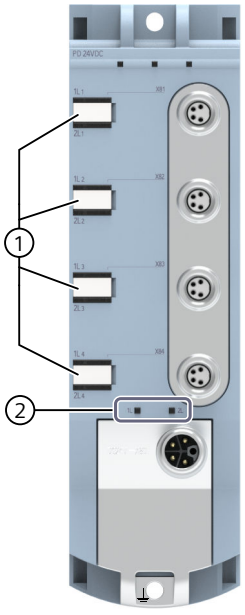
Interrupts/diagnostic messages

4

4.1 Status and error displays

LED displays

The figure below shows the LED displays (status and error displays) on the voltage distributor PD 24VDC.



① Status of the output voltages 1L*/2L* of X81 ... X84
② Status of the supply voltage 1L/2L of X80

Figure 2-203 LED displays PD 24VDC

LED displays of the supply voltage

Table 2-396 Status display of the supply voltages 1L/2L

LED inputs	Meaning
■ On	Voltage present
□ Off	Voltage not present or too low

LED display of the output voltages

Table 2-397 Status display of the output voltages 1L*/2L*

LED outputs	Meaning
■ On	Voltage applied
☼ Flashes	Overload
□ Off	Short-circuit

Technical specifications

5

5.1 Technical specifications

Technical specifications of the voltage distributor PD 24VDC

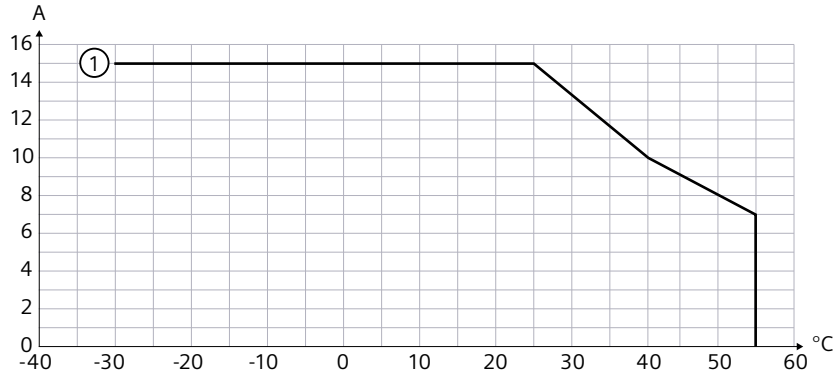
The following table lists the technical specifications as of the issue date. You can find a data sheet including daily updated technical specifications on the Internet (https://support.industry.siemens.com/cs/ww/en/pv/6ES7194-2CA00-0AA0/td?dl=en).

Article number	6ES7194-2CA00-0AA0
General information	
Product type designation	PD 24 V DC
Product description	voltage distributor for the distribution of centrally supplied supply voltage to 4x M8 sockets with integrated electronic short-circuit protection
Suitability for use	for supplying the ET 200AL modules with 1L+ and 2L+ voltages
Supply voltage	
Load voltage 1L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes
Load voltage 2L+	
• Rated value (DC)	24 V
• permissible range, lower limit (DC)	20.4 V
• permissible range, upper limit (DC)	28.8 V
• Reverse polarity protection	Yes
Input current	
from load voltage 1L+ (unswitched voltage)	15 A
from load voltage 2L+, max.	15 A
Output current	
Output current, max.	15 A; each for 1L+ and 2L+
per output	4 A; each for 1L+ and 2L+
Short-circuit protection	Yes; Electronic
Power loss	
Power loss, typ.	5.5 W
Interrupts/diagnostics/status information	
LED status display	green LED "1L" and "2L" for input and output voltage
Potential separation	
between the load voltages	Yes

Article number	**6ES7194-2CA00-0AA0**
Degree and class of protection	
IP degree of protection	IP65/67
Standards, approvals, certificates	
Suitable for safety functions	No
Suitable for safety-related tripping of standard modules	Yes; from FS01
Highest safety class achievable for safety-related tripping of standard modules	
• Performance level according to ISO 13849-1	PL d
• Category according to ISO 13849-1	Cat. 3
• SIL acc. to IEC 62061	SIL 2
• remark on safety-oriented shutdown	https://support.industry.siemens.com/cs/de/en/view/39198-632
Ambient conditions	
Ambient temperature during operation	
• min.	-30 °C
• max.	55 °C
Altitude during operation relating to sea level	
• Ambient air temperature-barometric pressure-altitude	Up to max. 5 000 m, at installation height > 2 000 m additional restrictions, see manual for details
connection method	
Design of electrical connection at output	4x M8 socket, 4-pin
Type of electrical connection for mains supply line	1x M12 plug, L-coded, 4-pin
• connectable cable cross-section for mains supply line, max.	2.5 mm²
Dimensions	
Width	45 mm
Height	159 mm
Depth	45 mm
Weights	
Weight, approx.	200 g

5.2 Derating

The following figure show the load current derating with mounting clearance observed, depending on the ambient temperature.



① Current in A of 1L or 2L

Figure 2-204 Derating load current ambient temperature

NOTE

Observe minimum clearance

With the voltage distributor PD 24VDC (6ES7194-2CA00-0AA0) maintain a minimum clearance of 1 cm from adjacent modules or other devices when mounting.

Dimension drawing

A

A.1 Dimension drawing

The following figure shows the dimension drawing of the voltage distributor PD 24VDC in the front and side views.

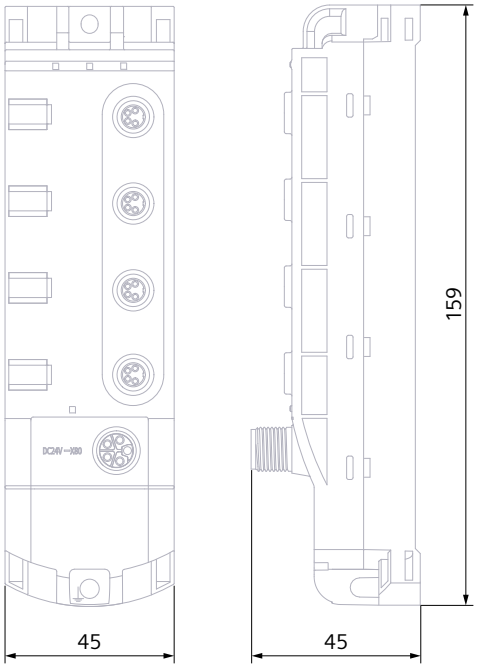


Figure 2-205 Dimension diagram PD 24VDC

SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Diagnostics

Function Manual

Introduction 1

Safety instructions 2

Overview of system diagnostics 3

Quick start 4

Configuring and determining system diagnostics 5

System diagnostics by means of the user program 6

Alarms 7

Diagnostics of the S7-1500R/H redundant system 8

11/2024
A5E03735838-AJ

Table of contents

1 Introduction 4

1.1 Function Manuals documentation guide 7
1.1.1 Information classes Function Manuals 7
1.1.2 Basic tools 9
1.1.3 SIMATIC Technical Documentation 11

2 Safety instructions 13

2.1 Cybersecurity information 13

3 Overview of system diagnostics 14

3.1 Properties of system diagnostics 14
3.2 Benefits of innovative system diagnostics 15

4 Quick start 17

4.1 Using the display of the CPU 17
4.2 Using STEP 7 20

5 Configuring and determining system diagnostics 25

5.1 Configuring system diagnostics in the CPU properties 26
5.2 Configuring alarms for system diagnostics in the project 27
5.3 Options for displaying system diagnostics 28
5.3.1 Diagnostics information at the devices 29
5.3.1.1 LEDs 29
5.3.1.2 Display of the CPU 30
5.3.2 Diagnostics information in STEP 7 31
5.3.2.1 Explanation of diagnostics symbols 31
5.3.2.2 Accessible devices (without project) 34
5.3.2.3 Devices & networks 36
5.3.2.4 Online & diagnostics 38
5.3.2.5 "Diagnostics" tab in the Inspector window 41
5.3.2.6 CPU diagnostics buffer 43
5.3.2.7 "Online tools" task card 46
5.3.2.8 Configuring the settings for I/O modules in STEP 7 48
5.3.3 Diagnostics information using the web server 49
5.3.4 Showing diagnostic information on an HMI device 59
5.3.4.1 Configuring system diagnostics 60
5.3.4.2 Different views of the system diagnostics view 62
5.3.4.3 Inserting system diagnostics indicator 66
5.3.4.4 Configuring button as system diagnostics indicator 68
5.3.4.5 System diagnostics in WinCC Unified 69

6 System diagnostics by means of the user program 75
6.1 Options of system diagnostics in the user program 75
6.2 System diagnostics using process image inputs 77

7 Alarms 80
7.1 Creating alarms with the "Program_Alarm" instruction 81
7.2 Editing alarms in the alarm editor 82
7.3 Display of program alarms 84
7.4 Output of the alarm state with the "Get_AlarmState" instruction 85
7.5 Example program for program alarms 86
7.5.1 Task 86
7.5.2 Example 1: Program alarm without associated values 87
7.5.3 Example 2: Program alarm with associated value 91
7.5.4 Displaying the alarm 97

8 Diagnostics of the S7-1500R/H redundant system 99
8.1 Online and Diagnostics view 100
8.2 "Online Tools" task card 103
8.3 Diagnostics view in the project tree and in the device view and network view 106
8.4 Diagnostics in the RUN-Redundant system state 115
8.5 Restrictions in the RUN-Solo system state 121
8.6 System diagnostics by means of the user program 122

Introduction

1

Purpose of the documentation

This Function Manual provides an overview of the diagnostics options for the SIMATIC S7-1500 automation system, for 1513pro-2 PN and 1516pro-2 PN CPUs based on SIMATIC S7-1500, and for the SIMATIC ET 200MP, ET 200SP, ET 200AL and ET 200eco PN distributed I/O systems.

The documentation covers the following:

- Illustration of the uniformity and consistency of system diagnostics
- Overview of the options for obtaining system diagnostics information

Basic knowledge required

The following knowledge is required in order to understand the function manual:

- General knowledge in the field of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge of working with STEP 7, WinCC , and WinCC Unified
- Knowledge about the use of Microsoft Windows operating systems

Scope of the documentation

This documentation is the basic documentation for all products of the S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200eco PN systems, as well as for the 1513pro-2 PN and 1516pro-2 PN CPUs. The product documentation is based on this documentation.

What's new in the Diagnostics Function Manual, Edition 11/2024 compared with Edition 11/2023

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Configuring system diagnostics in the CPU properties	You receive information on the settings options for the system diagnostics in the CPU properties.	Section Configuring system diagnostics in the CPU properties (Page 26)
Changed contents	Configuring alarms for system diagnostics in the project	You receive information on how to configure system diagnostics settings for your project	Section Configuring alarms for system diagnostics in the project (Page 27)

What's new in the Diagnostics Function Manual, Edition 11/2023 compared with Edition 11/2022

What's new?		What are the customer benefits?	Where can I find the information?
Changed contents	Addition to section "Showing diagnostic information on an HMI device"	You receive information on configuring system diagnostics in WinCC Unified.	Section System diagnostics in WinCC Unified (Page 69)

What's new in the Diagnostics Function Manual, Edition 11/2022 compared with Edition 11/2019

What's new?		What are the customer benefits?	Where can I find the information?
Changed contents	Addition to section "Diagnostics of the S7-1500R/H redundant system"	You receive information on diagnostics of R1 devices. An example shows you how to perform diagnostics for a faulty connection.	Section Diagnostics of the S7-1500R/H redundant system (Page 99)

What's new in the Diagnostics function manual, Edition 11/2019 compared to Edition 10/2018

What's new?		What are the customer benefits?	Where can I find the information?
Changed contents	Updated restrictions for the S7-1500R/H redundant system	Functions with which you are familiar from the SIMATIC S7-1500 automation system are implemented for the S7-1500R/H redundant system.	Section Diagnostics of the S7-1500R/H redundant system (Page 99)

What's new in the Diagnostics function manual, Edition 10/2018 compared to Edition 09/2016

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Description of the diagnostics of the S7-1500R/H redundant system	You obtain information in compact form on the special features of the diagnostics in S7-1500R/H redundant systems.	Section Diagnostics of the S7-1500R/H redundant system (Page 99)
Changed contents	Scope of the Function Manual expanded to include the S7-1500R/H redundant system	Functions with which you are familiar from the SIMATIC S7-1500 automation system are implemented for the S7-1500R/H redundant system.	Redundant System S7-1500R/H System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833)

What's new in the Diagnostics function manual, Edition 09/2016 compared to Edition 06/2014

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Extended functionality of the Web server		Section Diagnostics information using the web server (Page 49), Web server (http://support.automation.siemens.

What's new?		What are the customer benefits?	Where can I find the information?
New contents		• You obtain information about: – Know-how protection or copy protection of the PLC program – Program/communication load and cycle time – Collective signatures, cycle times, and runtimes of the F-runtime group(s) (with an F-CPU) • You can monitor statuses, errors, technology alarms and the current values of technology objects (TOs) with the Web server. • You can read, view and save trace recordings via the Web server and thus obtain plant and project information for diagnostics and maintenance without STEP 7. • You can set four additional languages for the Web server interface.	com/WW/view/en/59193560) function manual, Using the trace and logic analyzer function (https://support.industry.siemens.com/cs/ww/en/view/64897128) function manual
	Assignment of different project languages extended	You can assign up to three different project languages for comments and alarm texts to the user interface languages of display devices.	Section Editing alarms in the alarm editor (Page 82)
Changed contents	Scope of the function manual expanded to include CPU 1516pro-2 PN	Functions that you will be familiar with from the SIMATIC S7-1500 CPUs are implemented in the CPU 1516pro-2 PN (degree of protection IP65, IP66, and IP67).	Operating instructions CPU 1516pro-2 PN (https://support.industry.siemens.com/cs/ww/en/view/109482416)
	Security events added	You know which types of events are registered as security events in the diagnostics buffer and can configure group alarms for them.	Section CPU diagnostics buffer (Page 43)
	Influence of the value status explained	You know which factors influence the bit in the value status and can take this into account during configuration.	Section System diagnostics using process image inputs (Page 77)
	Note added on the maximum configuration limits of program alarms.		Section Creating alarms with the "Program_Alarm" instruction (Page 81).

Conventions

STEP 7: We refer to "STEP 7" in this documentation as a synonym for the configuration and programming software "STEP 7 as of V12 (TIA Portal)" and subsequent versions.

This document contains illustrations of the described devices. The illustrations may differ slightly from the device supplied.

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Industry Mall

The Industry Mall is the catalog and order system of Siemens AG for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).

You can find catalogs for all automation and drive products on the Internet (https://mall.industry.siemens.com).

1.1 Function Manuals documentation guide

1.1.1 Information classes Function Manuals



The documentation for the SIMATIC S7-1500 automation system, for the 1513/1516pro-2 PN, SIMATIC Drive Controller CPUs based on SIMATIC S7-1500 and the SIMATIC ET 200MP, ET 200SP, ET 200AL and ET 200eco PN distributed I/O systems is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742705).

Basic information



The system manuals and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500, SIMATIC Drive Controller, ET 200MP, ET 200SP, ET 200AL and ET 200eco PN systems. Use the corresponding operating instructions for 1513/1516pro-2 PN CPUs.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- Getting Started S7-1500
- System manuals
- Operating instructions ET 200pro and 1516pro-2 PN CPU
- Online help TIA Portal

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment manuals for CPUs
- Equipment manuals for interface modules
- Equipment manuals for digital modules
- Equipment manuals for analog modules
- Equipment manuals for communication modules
- Equipment manuals for technology modules
- Equipment manuals for power supply modules
- Equipment manuals for BaseUnits

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC Drive Controller and the S7-1500 automation system.

Examples:

- Function Manual Diagnostics
- Function Manual Communication
- Function Manuals Motion Control
- Function Manual Web Server
- Function Manual Cycle and Response Times
- PROFINET Function Manual
- PROFIBUS Function Manual

Product Information

Changes and supplements to the manuals are documented in a Product Information. The Product Information takes precedence over the device and system manuals.

You will find the latest Product Information on the Internet:

- S7-1500/ET 200MP (https://support.industry.siemens.com/cs/de/en/view/68052815)
- SIMATIC Drive Controller (https://support.industry.siemens.com/cs/de/en/view/109772684/en)
- Motion Control (https://support.industry.siemens.com/cs/de/en/view/109794046/en)
- ET 200SP (https://support.industry.siemens.com/cs/de/en/view/73021864)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109765611)

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- S7-1500/ET 200MP/SIMATIC Drive Controller (https://support.industry.siemens.com/cs/ww/en/view/86140384)
- ET 200SP (https://support.industry.siemens.com/cs/ww/en/view/84133942)
- ET 200AL (https://support.industry.siemens.com/cs/ww/en/view/95242965)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109781058)

1.1.2 Basic tools

Tools

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities on various SIMATIC S7 stations as bulk operations independent of TIA Portal.

The SIMATIC Automation Tool offers a wide range of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Assignment of addresses (IP, subnet, Gateway) and device name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization through LED flashing
- Reading out of CPU error information
- Reading the CPU diagnostic buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/98161300)

PRONETA

SIEMENS PRONETA (PROFINET network analysis) is a commissioning and diagnostic tool for PROFINET networks. PRONETA Basic has two core functions:

- In the network analysis, you get an overview of the PROFINET topology. Compare a real configuration with a reference installation or make simple parameter changes, e.g. to the names and IP addresses of the devices.
- The "IO test" is a simple and rapid test of the wiring and the module configuration of a plant, including documentation of the test results.

You can find SIEMENS PRONETA Basic on the Internet:
(https://support.industry.siemens.com/cs/ww/en/view/67460624)

SIEMENS PRONETA Professional is a licensed product that offers you additional functions. It offers you simple asset management in PROFINET networks and supports operators of automation systems in automatic data collection/acquisition of the components used through various functions:

- The user interface (API) offers an access point to the automation cell to automate the scan functions using MQTT or a command line.
- With PROFIenergy diagnostics, you can quickly detect the current pause mode or the readiness for operation of devices that support PROFIenergy and change these as needed.
- The data record wizard supports PROFINET developers in reading and writing acyclic PROFINET data records quickly and easily without PLC and engineering.

You can find SIEMENS PRONETA Professional on the Internet.
(https://www.siemens.com/proneta-professional)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

1.1.3 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:



Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Safety instructions 2

2.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

Overview of system diagnostics

3

3.1 Properties of system diagnostics

Introduction

In the SIMATIC environment, the term "system diagnostics" refers to diagnostics of devices and modules.

All SIMATIC products have integrated diagnostic functions that you can use to detect and remedy faults. The components automatically flag a potential fault in the operation and provide detailed information. You can minimize unscheduled standstill times with plant-wide diagnostics.

The SIMATIC automation system monitors the following states in the running plant:

- Device failure/recovery
- Insert/remove event
- Module fault
- I/O access error
- Channel fault
- Parameter assignment error
- Failure of the external auxiliary voltage

Properties ofSIMATIC system diagnostics

- Integrated as standard in the hardware
- System-wide across bus limits
- Automatic localization of the error source
- Automatic output of the cause of the error in plain text
- Plant-wide diagnostics of all components
- Archiving and logging of alarms
- Configurability of alarms

Consistent diagnostics from the field level all the way to the management level

The various diagnostics media give you a uniform view of maintenance-related information of every automation component in the plant: System status (module and network status, alarms for system errors) are available plant-wide in a uniform display.

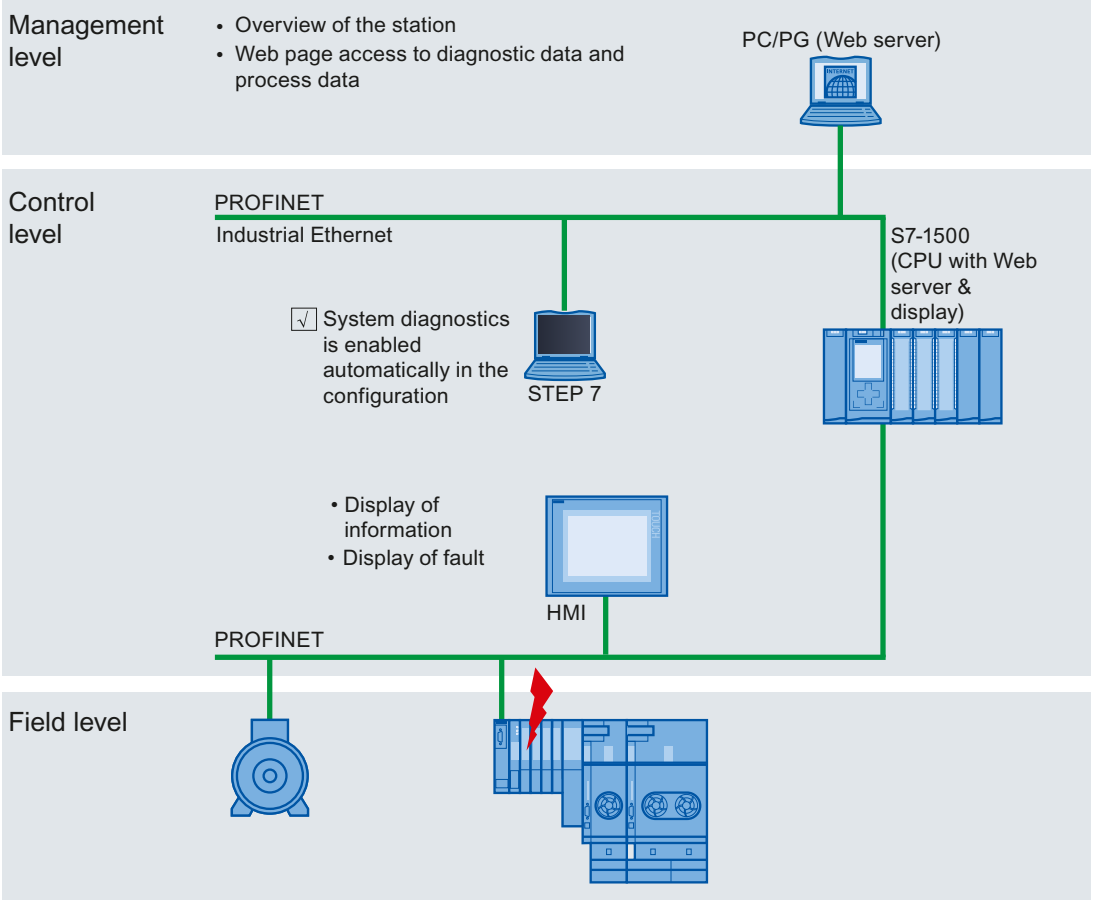


Figure 3-1 Overview of system diagnostics in a plant

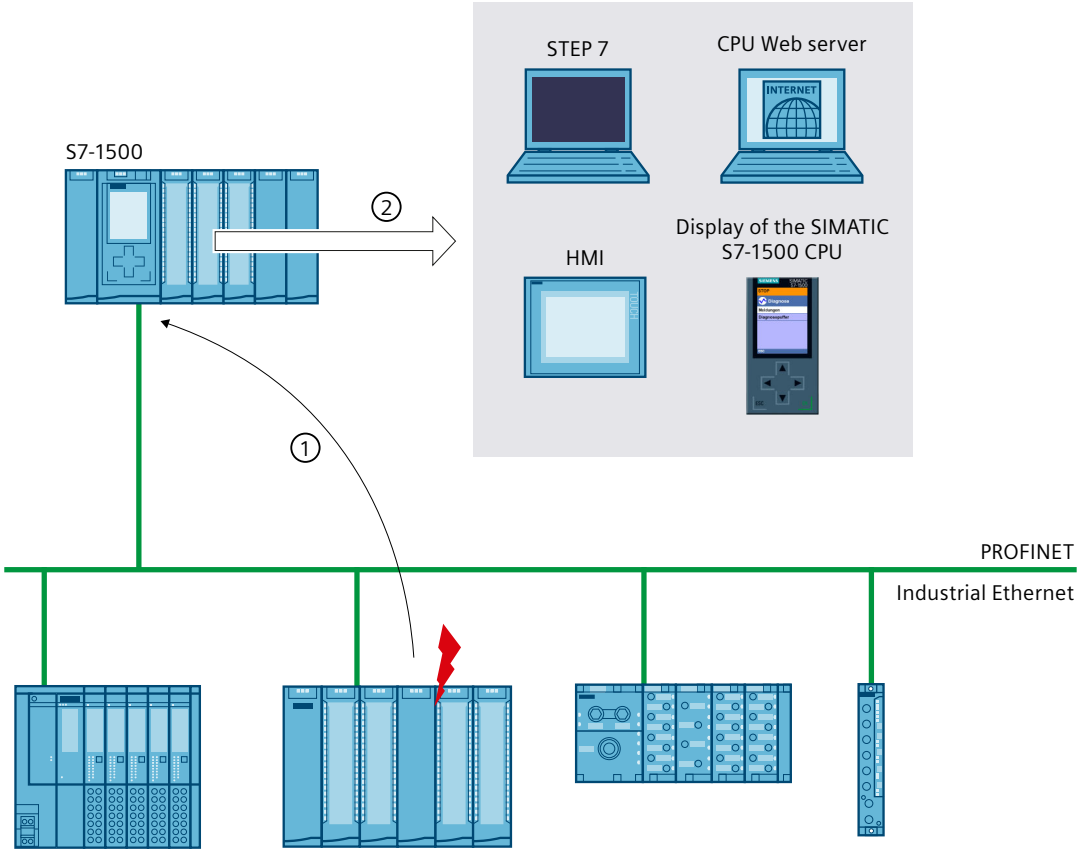
3.2 Benefits of innovative system diagnostics

System diagnostics is also possible in STOP

The system diagnostics is integrated in the firmware of the CPU and works independently of the cyclic user program. This means it is also available in the STOP CPU operating mode. Faults are detected immediately and signaled to the higher-level HMI devices, the Web server and the display of the SIMATIC S7-1500 CPU, even in STOP mode. This makes system diagnostics consistent with the actual plant state at all times.

Uniform display concept

All clients of a system are provided with diagnostics information by a uniform mechanism. The same system diagnostics information is used regardless of the display medium.



Step	Description
①	The device detects an error and sends diagnostics data to the assigned CPU.
②	The CPU informs the connected display media. The display of the system diagnostics is updated.

Figure 3-2 Sequence of the system diagnostics

Quick start

4

Introduction

The following chapters of this documentation describe the different options for establishing system diagnostics. All described options can be used independently of one another.

This chapter gives you an overview of the basic procedure to get initial diagnostics information fast.

NOTE

System diagnostics is generally available for the devices of the SIMATIC series.

4.1 Using the display of the CPU

The display of the SIMATIC S7-1500 CPU offers a fast and direct option to get diagnostics information. You can call up status information in different menus on the display.

Requirements

- A project has been created.
- The project has been downloaded to the CPU.

Determining diagnostics information using the display of the SIMATIC S7-1500 CPU

To determine diagnostics information using the display, follow these steps:

1. Select the "Diagnostics" menu on the display.
2. Select the "Diagnostics buffer" command from the "Diagnostics" menu.



Figure 3-3 Display of SIMATIC S7-1500 CPU

Result

The diagnostics events are displayed in the diagnostics buffer in the sequence in which they occur.

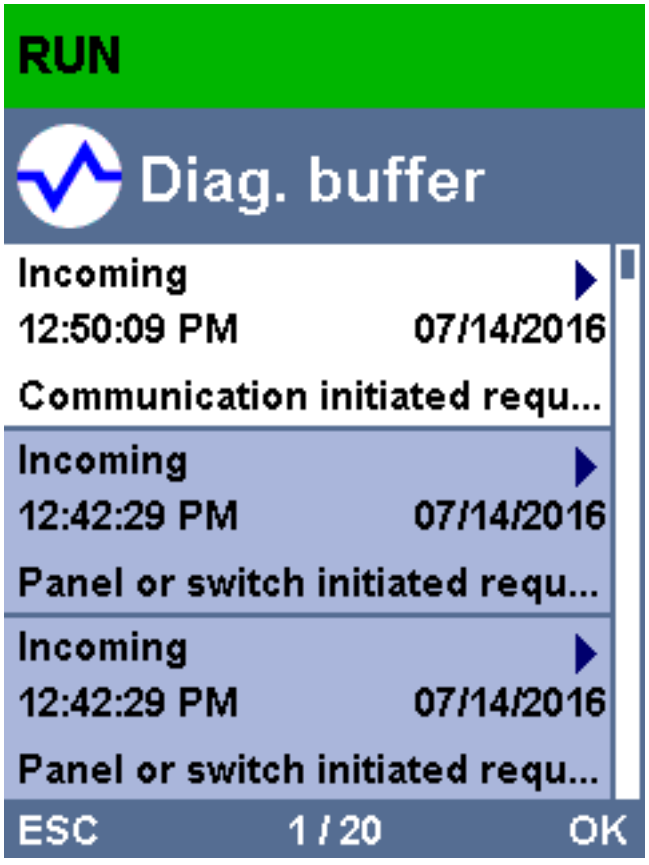


Figure 3-4 Display of the diagnostics buffer in the display of the SIMATIC S7-1500 CPU

NOTE

Automatic updating of diagnostics information
You set automatic updating of the diagnostics information under: "Display" > "DiagnosticRefresh".

Additional information

You can find information about the configuration of alarms in the section Configuring alarms for system diagnostics in the project (Page 27).

4.2 Using STEP 7

Getting started with STEP 7 gives you fast access to detailed diagnostics information.

Requirements

- A project has been created.
- The project has been downloaded to the CPU.
- An error has occurred.
- The programming device must be able to establish a connection to the CPU via an interface.

Determining diagnostics information using STEP 7

To determine diagnostics information using STEP 7, follow these steps:

1. Open the respective project in STEP 7.
2. Open the portal view of STEP 7.
3. Select the "Online & Diagnostics" portal.
4. Select the "Online status" action.
   The "Select device" dialog opens. The dialog is an image of the configured devices in the project.

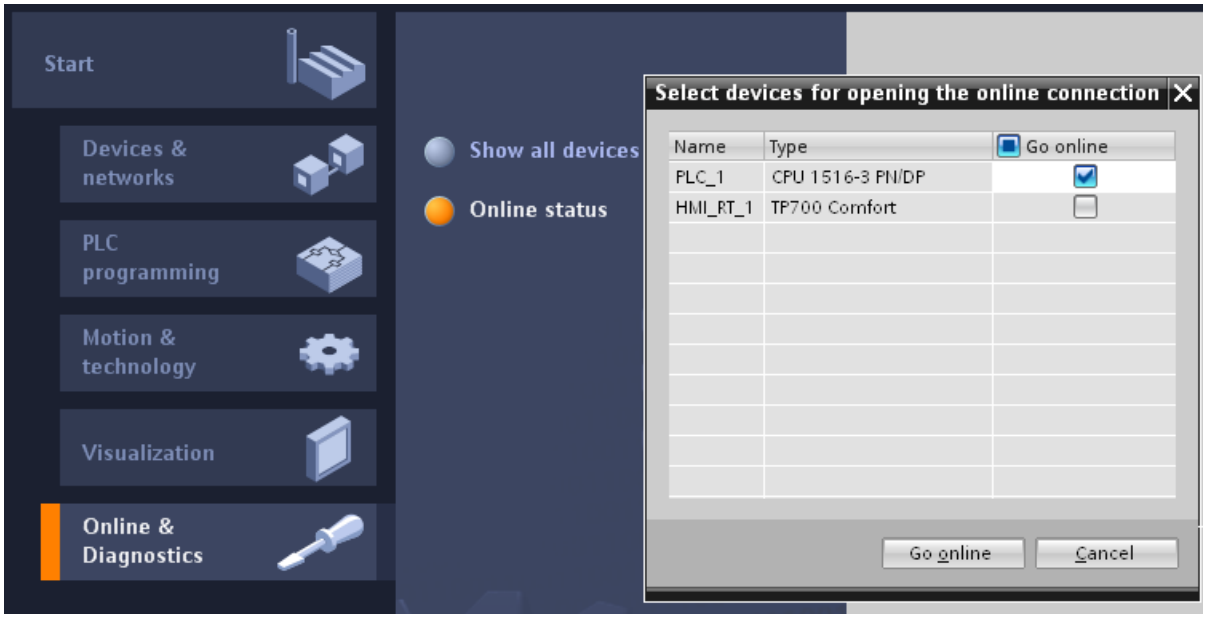


Figure 3-5 Device selection for online connection in the portal view

5. Activate the "Go online" option button for the device that you want to use to establish an online connection.
6. Click on the "Go online" button.

7. The "Go online" dialog opens.

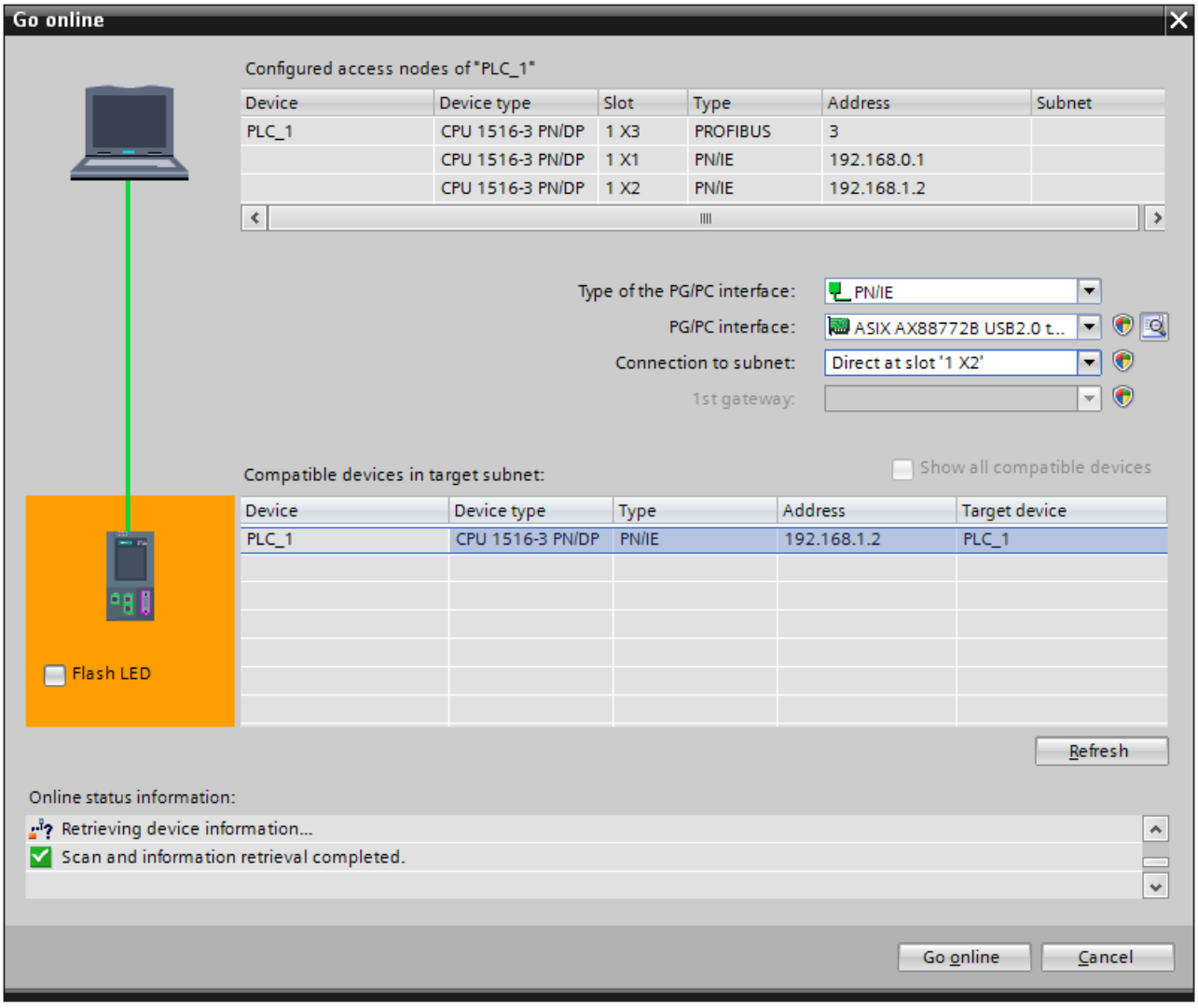


Figure 3-6 Establishing an online connection

8. Make the settings for the interface.

9. Click on the "Go online" button.
   The project view of STEP 7 opens. The network view is opened in the work area.
   The symbols in the project tree provide initial information about the faulty modules.

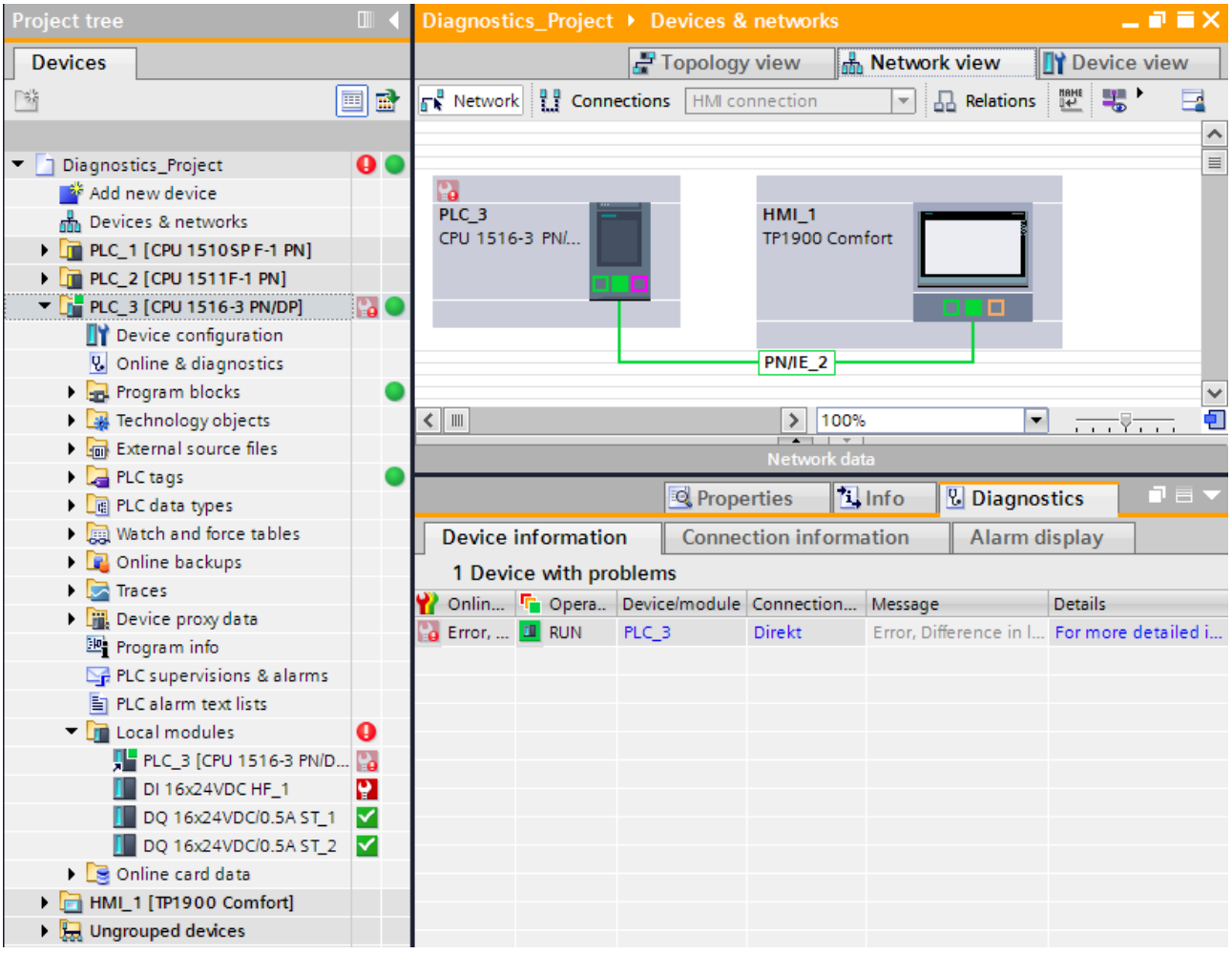


Figure 3-7 Display of the fault in the network view

10. Double-click the device which displays an alarm message to access the faulty module directly. This is the CPU in the example.

    The device view of the CPU is opened in the work area. In this view you can see directly in which module the error has occurred.

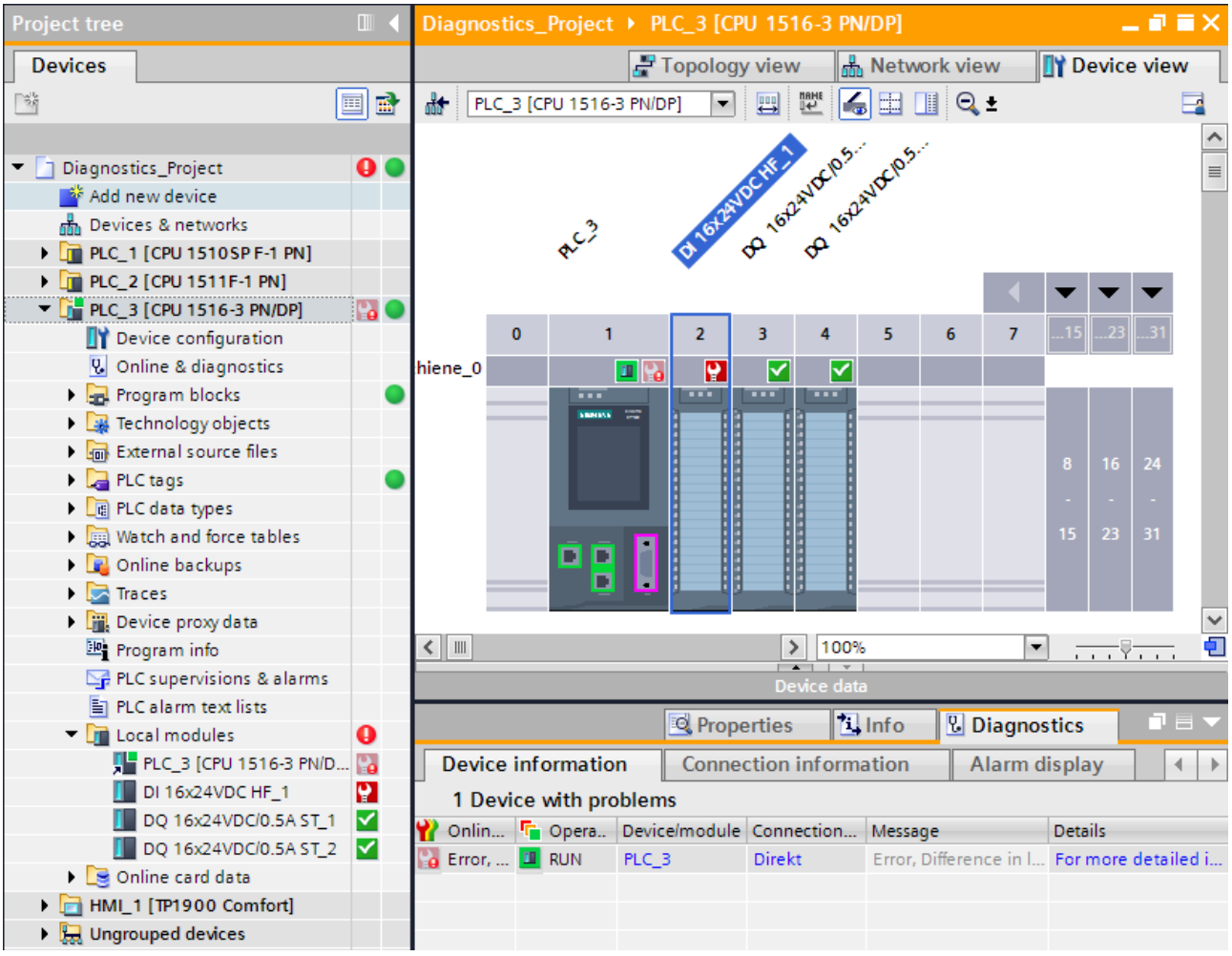


Figure 3-8 Display of the faulty module in the device view

11. Open the "Diagnostics" tab and the subordinate "Device information" tab in the Inspector window for a more detailed error description.

Result

The link in the "Details" table column takes you to the online and diagnostics view of the device and to the diagnostics buffer there, for example. This includes more information on all diagnostics events in the order in which they occurred.

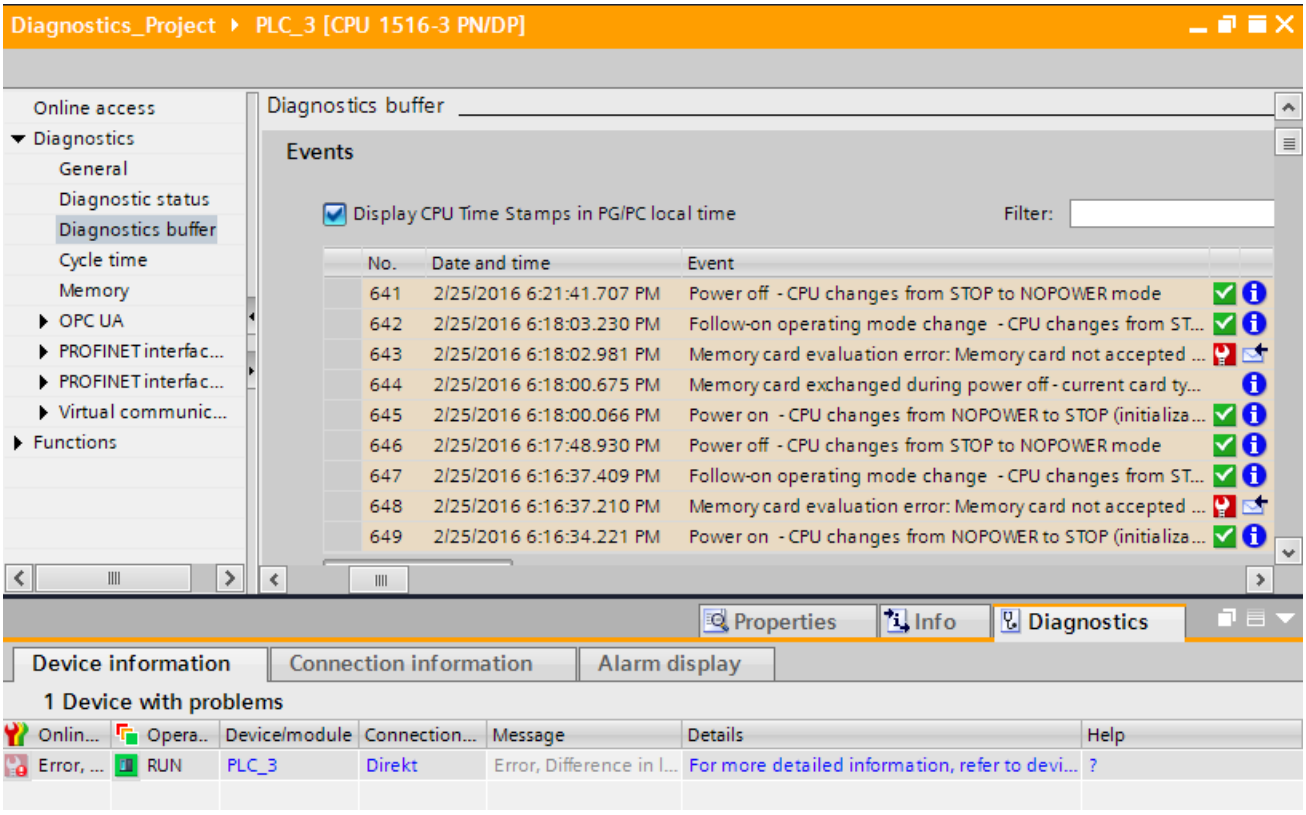


Figure 3-9 Diagnostics buffer with detailed error description

NOTE

Symbols and their meaning

You can find a legend with the meaning of each symbol in Explanation of diagnostics symbols (Page 31) and in the online help for STEP 7.

Configuring and determining system diagnostics 5

Introduction

System diagnostics is the recording, evaluation and reporting of an error within the automation system. The generated alarms contain a textual error description and the error location.

For SIMATIC CPUs, system diagnostics is enabled by default and cannot be disabled. For each individual CPU in your project, you can specify which diagnostic alarms you want or do not want to receive on your display device. The settings in the CPU properties act like a filter. Only the system diagnostics alarms you need are forwarded to the display devices. You can use the following devices to display alarms:

- Display of the CPU (only for S7-1500 CPUs)
- CPU Web server
- HMI device

In the system diagnostics settings in the project tree, you can make the following settings for the entire project:

- The alarm categories for which an alarm is issued
- Whether or not the alarms issued require acknowledgment

To learn how to set system diagnostics in CPU properties and in the project, see the following sections.

5.1 Configuring system diagnostics in the CPU properties

Requirements

- A project is open
- STEP 7 displays the network view

Procedure

To configure the system diagnostics in the CPU properties, proceed as follows:

1. Select the required CPU in the network view of STEP 7.
2. In the Inspector window, go to "Properties > System diagnostics".
3. Select the events for which the CPU should or should not issue an alarm.
   Depending on the firmware version of the CPU used, the following options are available:

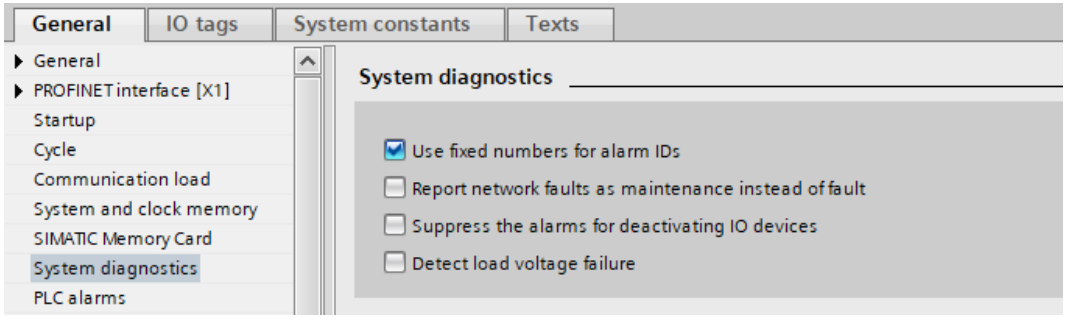


Figure 3-10 System diagnostics in the CPU properties

- Use fixed numbers for alarm IDs:
  This option is available on all CPUs and is activated in the basic settings.
  The system diagnostic alarms receive fixed alarm numbers from 1 to 512. If, for example, the user changes the order of the alarm types, the alarm numbers remain the same.

- Report network faults as maintenance instead of fault:
  This option is available on all CPUs as of FW version V2.5 and is deactivated in the basic settings.
  If you activate this option, the CPU will report any network errors as "Maintenance demanded".

- Suppress the alarms for deactivating IO devices:
  This option is available on all CPUs as of FW version V3.0 and is deactivated in the basic settings.
  If you activate this option, the CPU does not output any alarms for inactive but configured IO devices on the PROFINET IO system.
- Detect load voltage failure:
  This option is available on all CPUs as of FW version V3.1 and is deactivated in the basic settings.
  If you activate this option, the CPU reports a failure of the load voltage supply to central or distributed I/O in the user program.

Result: You have configured the alarm settings for system diagnostics in the CPU properties.

5.2 Configuring alarms for system diagnostics in the project

Predefined alarm texts are available for establishing the system diagnostics.

Requirements

- STEP 7 is open.
- A project is open.

Procedure

To configure alarm settings for system diagnostics of the project in STEP 7, proceed as follows:

1. Open the "Common data" folder in the project tree.
2. Double-click on the "System diagnostics settings" entry.
   STEP 7 displays the following configuration options.

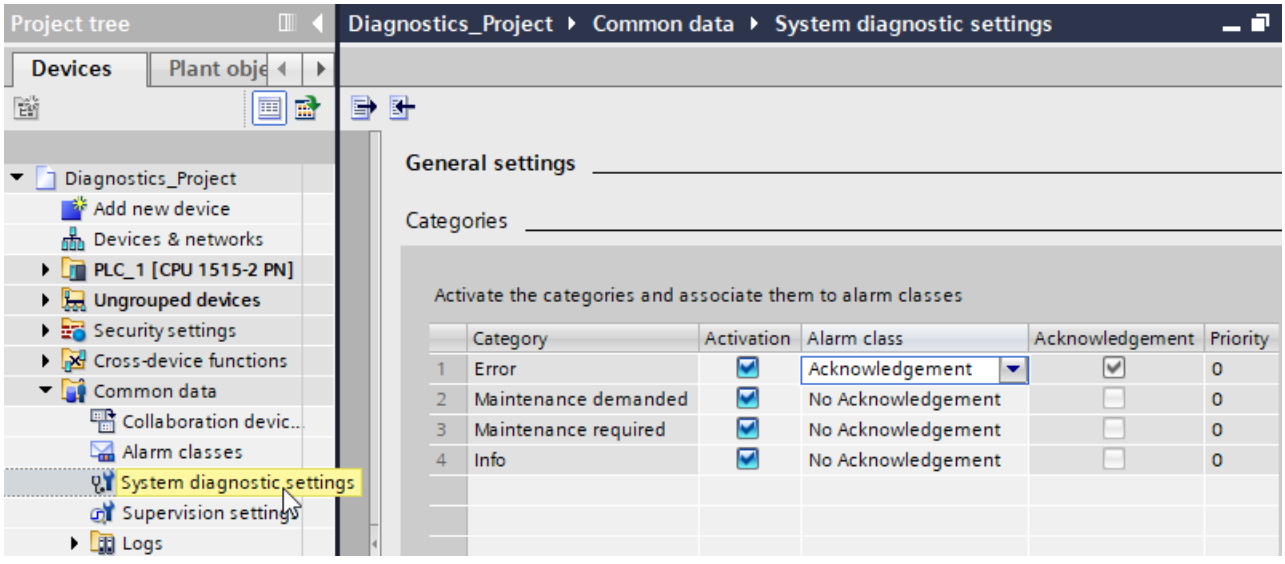


Figure 3-11 Properties of system diagnostics and alarm settings

3. Select the alarm categories for which you need an alarm in the "Activation" column.
   Alarms are activated for all categories in the basic settings. When you disable all check boxes, the status of the HMI system diagnostics view is still updated with the "Info Report" functionality.

4. Select one of the following options in the respective drop-down list of the "Alarm class" column:
   - No Acknowledgement (default):
     Alarms in this category do not have to be acknowledged.
     The corresponding option in the "Acknowledgement" column is not activated.
   - Acknowledgement:
     Alarms in this category must be acknowledged.
     The corresponding option in the "Acknowledgement" column is automatically activated.

Result: You have configured the alarms for system diagnostics of the project in STEP 7. The set priority of the respective alarm class is displayed in the "Priority" column.

The settings are saved with the project and become effective after the compiling and downloading of the hardware configuration to the involved components.

Maintenance events (maintenance demanded, maintenance required) are entered in the alarm buffer of the CPU just like any other event.

5.3 Options for displaying system diagnostics

Example

This section includes a diagnostics example to show how system diagnostics is established with the help of different display options. The example includes a CPU from the SIMATIC S7-1500 product series that is connected to an ET 200S distributed I/O system and an HMI Comfort Panel via PROFINET.

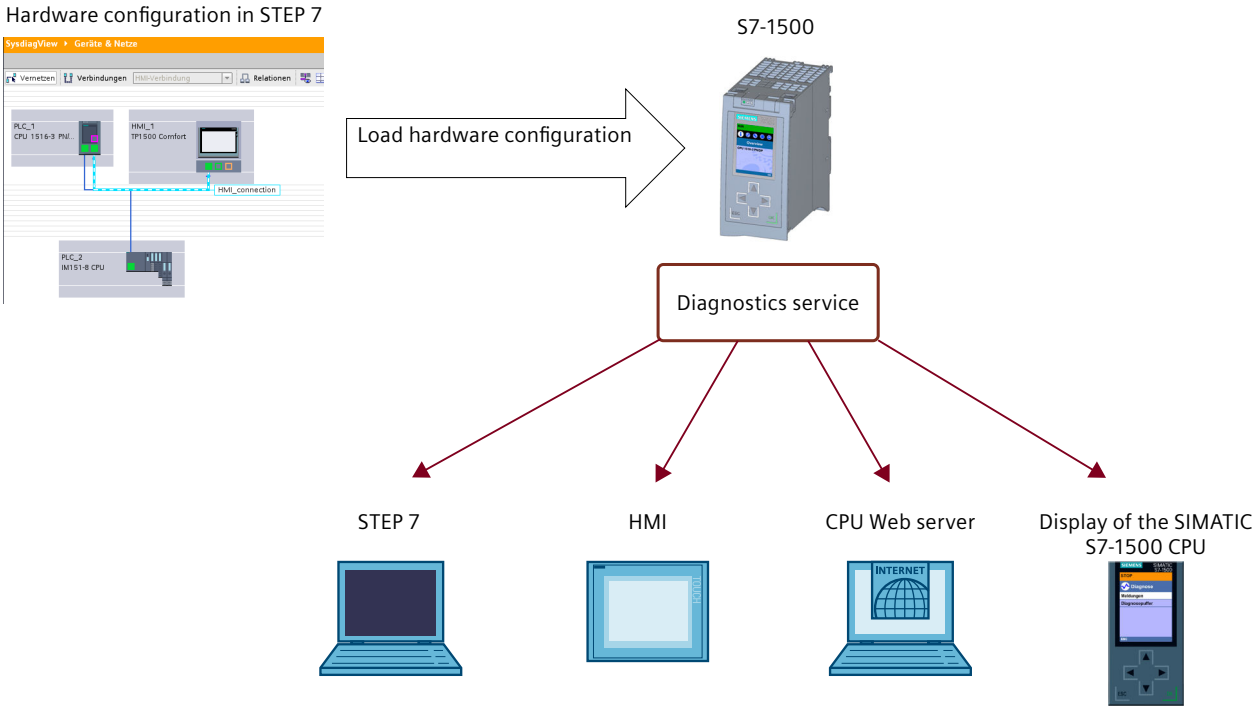


Figure 3-12 System diagnostics display options

The following sections include figures that illustrate how diagnostics information is displayed with the help of different display options.

- Using the LEDs on the hardware (Page 29)
- Local error analysis via the display of the CPU (Page 30)
- Using STEP 7 as of V12 (Page 31)
- Remote diagnostics using the Web server (Page 49)
- Stationary system diagnostics using the HMI diagnostics view (Page 59)

5.3.1 Diagnostics information at the devices

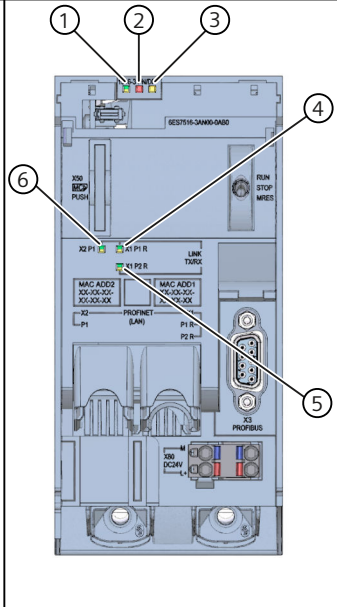
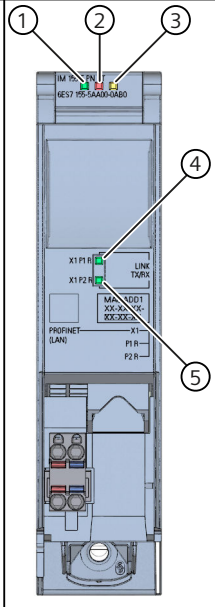
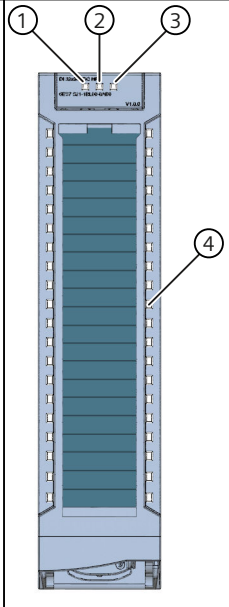
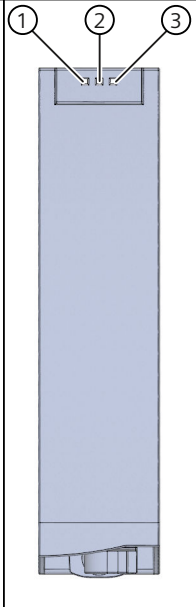
5.3.1.1 LEDs

Overview

All hardware components, such as CPUs, interface modules and modules, provide information about their operating mode as well as internal and external errors through their LEDs. Diagnostics by means of LEDs is an initial tool for error localization.

The graphics below include examples for the arrangement of LEDs on some modules.

Table 3-1 LED displays on the modules

	CPU 1516-3 PN/DP	IM 155-5 PN ST	DI 32x24VDC HF	PS 25W 24VDC
				
①	RUN/STOP LED (two-colored LED: green/yellow)	RUN LED (two-colored LED: green/yellow)	RUN LED (single-colored LED: green)	RUN LED (single-colored LED: green)
②	ERROR LED (single-colored LED: red)	ERROR LED (single-colored LED: red)	ERROR LED (single-colored LED: red)	ERROR LED (single-colored LED: red)
③	MAINT LED (single-colored LED: yellow)	MAINT LED (single-colored LED: yellow)	without function	MAINT LED (single-colored LED: yellow)

	CPU 1516-3 PN/DP	IM 155-5 PN ST	DI 32x24VDC HF	PS 25W 24VDC
④	X1 P1 (two-colored LED: green/yellow)	X1 P1 (single-colored LED: green)	LED CHx (two-colored LED: green/red)	
⑤	X1 P2 (two-colored LED: green/yellow)	X1 P2 (single-colored LED: green)		
⑥	X2 P1 (two-colored LED: green/yellow)			

Additional information

The meaning of the individual LED displays, their different combinations and the remedial measures resulting from them in case of errors are device-specific. The explanation can be found in the manuals of the modules.

5.3.1.2 Display of the CPU

Introduction

Each CPU in the S7-1500 automation system has a front cover with a display and operating keys. You can display status information in various menus on the display of the CPU. You use the operating keys to navigate through the menus.



Figure 3-13 Display - diagnostics screen

Display options

The display of the SIMATIC S7-1500 CPU shows the following diagnostics information:

- CPU operating state

"Diagnostics" menu

- Error and alarm texts (system diagnostics alarms)
- Information entered in the diagnostics buffer
- Watch tables
- Information on the cycle times of the user program
- Utilization of the CPU memory

"Modules" menu

- Information on modules and the network
- Detailed device view with diagnostics symbols
- Order number, CPU version and central I/O modules
- Module status for central and distributed modules
- Information about the currently installed firmware

Additional information

For additional information on the topic "Functions and operation of the display of the SIMATIC S7-1500 CPU", see the documentation for the S7-1500 automation system (http://support.automation.siemens.com/WW/view/en/59191792).

You can find detailed information on the individual options, a training course and a simulation of the available menu commands of the display for the CPU in the SIMATIC S7-1500 Display Simulator (http://www.automation.siemens.com/salesmaterial-as/interactive-manuals/getting-started_simatic-s7-1500/disp_tool/start_en.html).

5.3.2 Diagnostics information in STEP 7

5.3.2.1 Explanation of diagnostics symbols

Diagnostics symbols for modules and devices

When the online connection to a device is established in STEP 7, the diagnostics status of the device and its lower-level components and, if applicable, the device operating mode are also determined. The following table shows the possible symbols and their meaning.

Table 3-2 Diagnostics symbols for modules and devices

Symbol	Meaning
	The connection with a CPU is being established.
	The CPU is not reachable at the set address.
	The configured CPU and the CPU actually present are of incompatible types. Example: An existing CPU 315-2 DP is incompatible with a configured CPU 1516-3 PN/DP.

Symbol	Meaning
	On establishment of the online connection to a protected CPU, the password dialog was terminated without specification of the correct password.
	No fault
	Maintenance required
	Maintenance demanded
	Error
	The module or device is deactivated.
	The module or the device cannot be reached from the CPU (valid for modules and devices below a CPU).
	Diagnostics data is not available because the current online configuration data differ from the offline configuration data.
	The configured module or device and the module or device actually present are incompatible (valid for modules or devices under a CPU).
	The configured module does not support display of the diagnostics status (valid for modules under a CPU).
	The connection is established, but the module status has not yet been determined or is unknown.
	Hardware error in lower-level component: A hardware fault has occurred in at least one lower-level hardware component (occurs as a separate symbol only in the project tree).

Symbols for the comparison status

The diagnostics symbols can be combined at the bottom right with additional smaller symbols that indicate the result of the online/offline comparison. The following table shows the possible comparison symbols and their meaning.

Table 3-3 Symbols for the comparison status

Symbol	Meaning
	Hardware error in lower-level component: The online and offline versions differ (only in the project tree) in at least one lower-level hardware component.
	Software error in lower-level component: The online and offline versions differ (only in the project tree) in at least one lower-level software component.
	Online and offline versions of the object are different
	Object only exists online
	Object only exists offline
	Online and offline versions of the object are the same

Operating mode symbols for CPUs and CPs

The following table shows the possible symbols and their respective operating states.

Table 3-4 Operating mode symbols for CPUs and CPs

Symbol	Operating mode
	RUN
	STOP
	STARTUP
	DEFECTIVE
	Unknown operating mode
	The configured module does not support display of the operating mode.

Event table

The following information is displayed in the table for each diagnostics event:

- Sequential number of the entry
  The first entry contains the latest event.
- Date and time of the diagnostics event
  If no date and time are shown, the module has no integrated clock.
- Short designation of the event and, if applicable, the reaction of the CPU
- Symbol for information on incoming/outgoing status

The following table shows the possible symbols and their meaning.

Table 3-5 Symbols in the event table

Symbol	Meaning
	Incoming event
	Outgoing event
	Incoming event for which there is no independent outgoing event
	User-defined diagnostics event

Additional information

For additional information on the individual symbols, please refer to the online help for STEP 7.

5.3.2.2 Accessible devices (without project)

Accessible devices

Accessible devices are all devices that are connected to a PG/PC either directly by an interface or by means of a subnet and that are switched on. These devices can display diagnostic information even without an offline project.

Requirements

- STEP 7 is open.
- The portal view or project view is open.

Procedure

To display diagnostic information for specific devices even without an offline project, follow these steps:

1. Establish a connection to the respective CPU.
2. Select the command "Accessible devices" from the "Online" menu.
   The "Accessible devices" dialog opens.

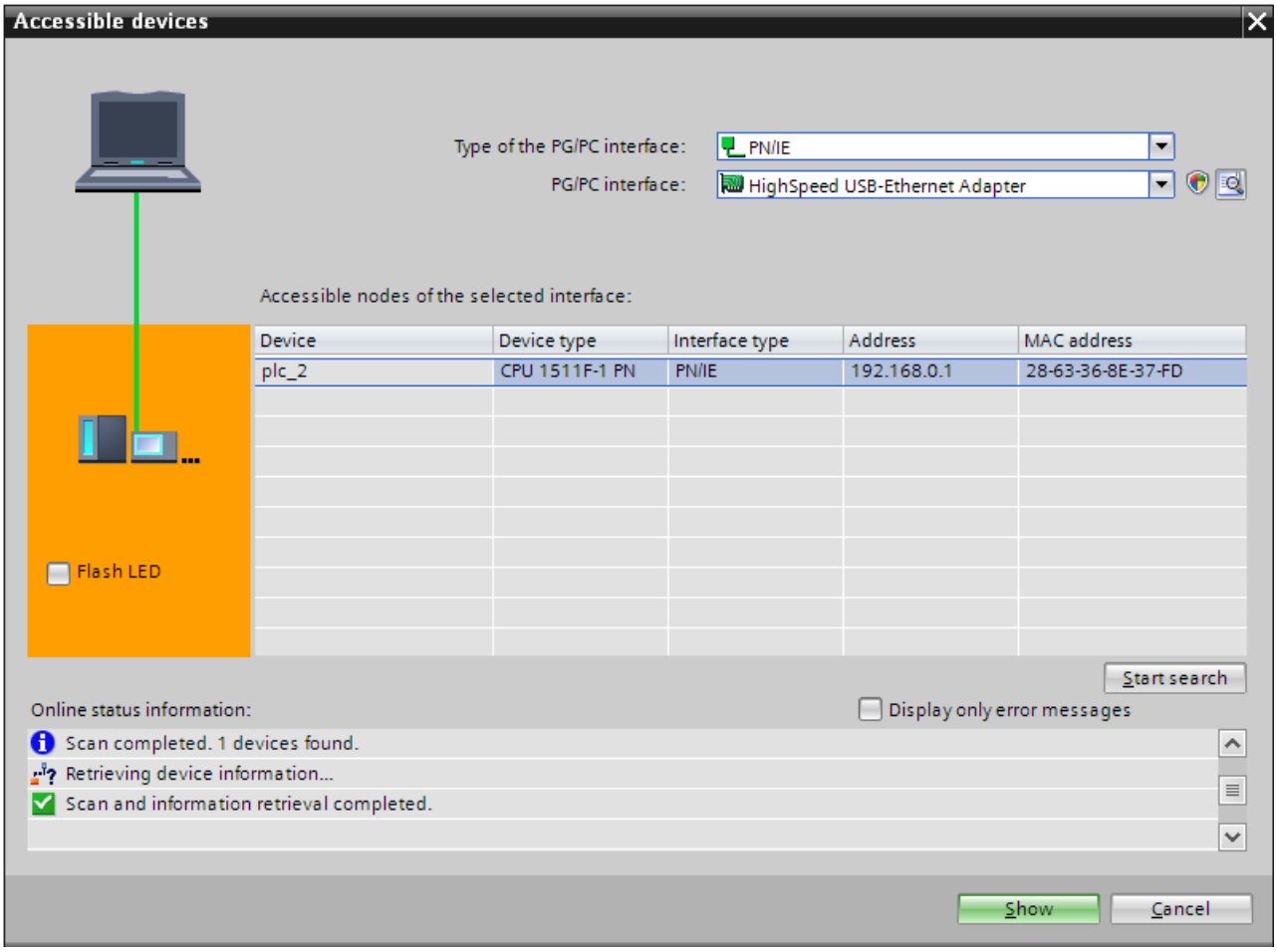


Figure 3-14 "Accessible devices" dialog

3. Make the settings for the interface.
4. Select the respective device under "Accessible nodes of the selected interface".
5. Confirm the dialog with the "Display" button.

Result

The device is displayed in the project tree. You open the diagnostic information in the work area with a double-click on "Online & Diagnostics".

Information is available on the diagnostic status, cycle times, memory usage and the diagnostics buffer.

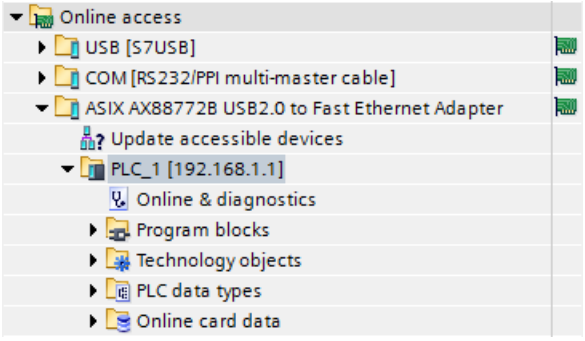


Figure 3-15 Device in the project tree

5.3.2.3 Devices & networks

Devices & networks - Go online

You can get an overview of the current state of your automation system in the device view or network view.

You implement the following tasks in the device view:

- Device configuration and parameter assignment
- Module configuration and parameter assignment

You implement the following tasks in the network view:

- Device configuration and parameter assignment
- Networking devices

Requirements

- STEP 7 is open.
- A project is open.
- The project view is open.

Procedure

To get an overview of the current state of your automation system, follow these steps:

1. Open the "Network view" in the working area.
2. Select the CPU.
3. Click the "Go online" Go online button in the toolbar.
   The "Go online" dialog opens.

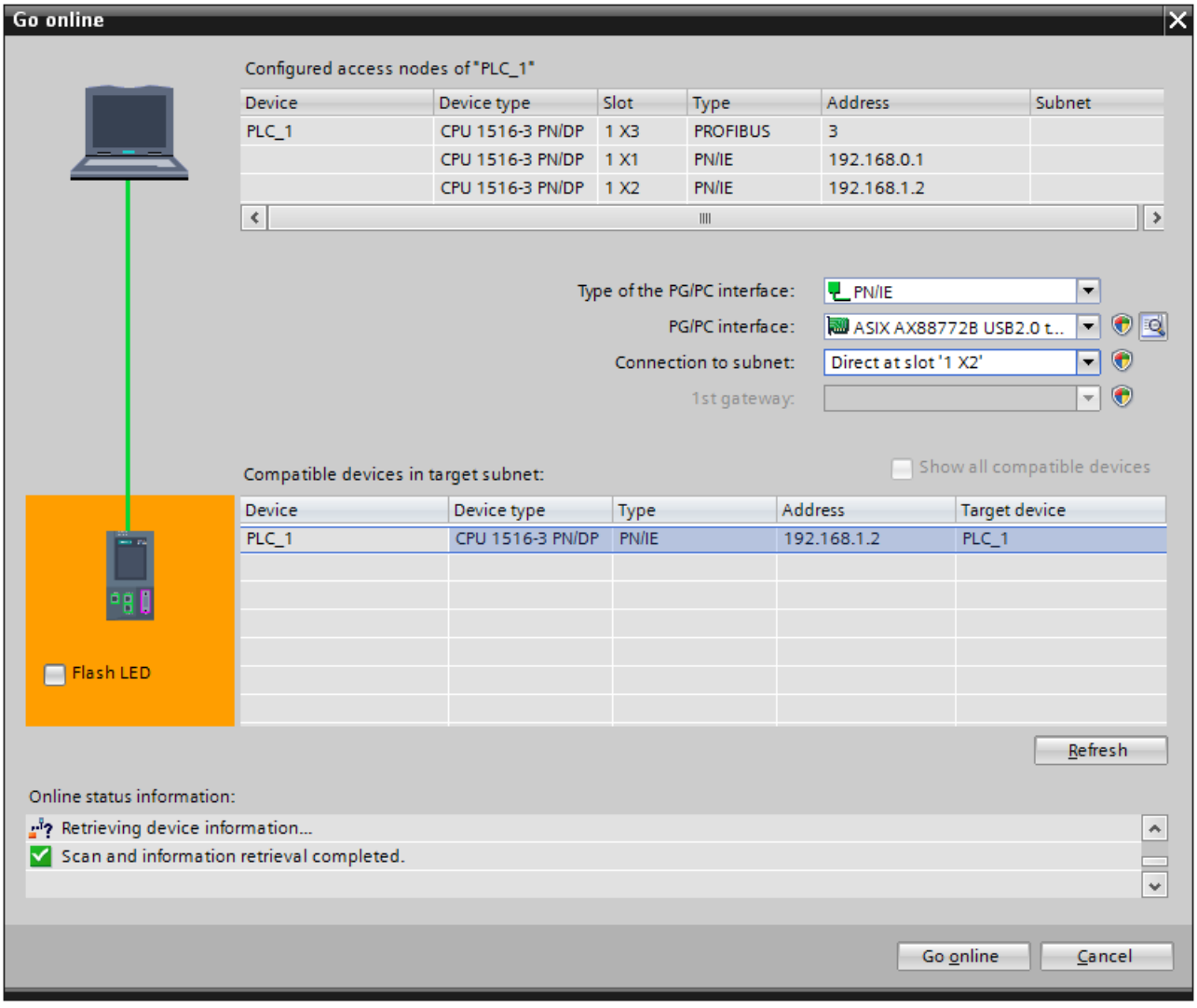


Figure 3-16 Go online

4. Make the settings for the interface.
5. Select the respective device under "Compatible devices in the target subnet".
6. Confirm the dialog with the "Connect" button.
   The online mode is started.

Result

The connected devices are now displayed with diagnostic information in the network view in the working area. Here you get an overview of the current state of your automation device.

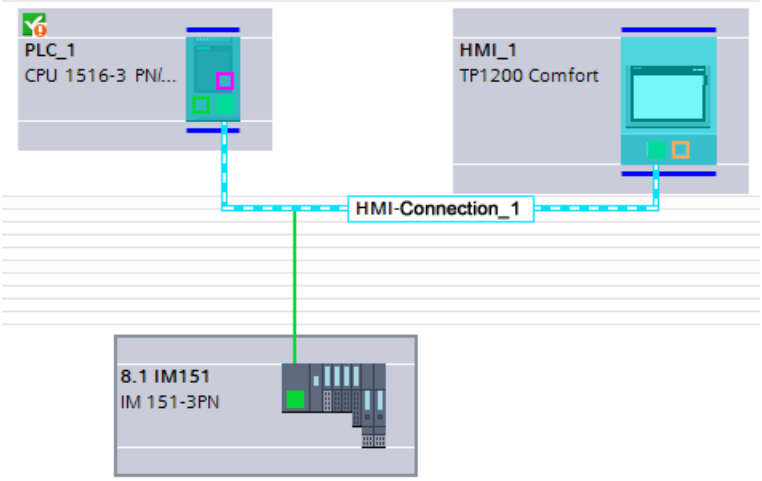


Figure 3-17 CPU with diagnostic information

You get to the "Device view" with a double-click on the device. The diagnostic information for the individual modules is displayed in this view.

NOTE

Symbols and their meaning
You will find a legend with the meaning of each symbol in Explanation of diagnostics symbols (Page 31) and in the online help for STEP 7.

5.3.2.4 Online & diagnostics

Online mode

In online mode there is an online connection between your PG/PC and one or several devices. Depending on the properties of a device, you are offered specific diagnostics options and certain functions in online mode.

- Diagnostics
  - General module information
  - Diagnostics status
  - Cycle time
  - Memory
  - Diagnostics buffer
  - Display
  - Interface information (e.g. IP parameter, port information)

- Functions
  - Assign IP address
  - Set time and date of the CPU
  - Firmware update (e.g. for PLC, display)
  - Assign device name
  - Reset to factory settings
  - Format memory card
  - Save service data

To establish an online connection at least one PG/PC interface must be installed that is physically connected with a device, for example, with an Ethernet cable. The current online status of a device is indicated by a symbol to the right of the device in the project tree.

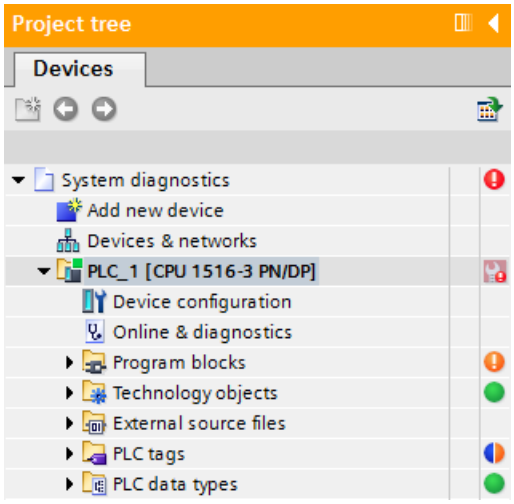


Figure 3-18 Partial view of network view

Requirements

- STEP 7 is open.
- A project is open.
- The project view is open.

Procedure

To display an overview of the faulty devices, follow these steps:

1. Select the affected device folder in the project tree.
2. Select the shortcut menu command "Online & Diagnostics".
   The online and diagnostics view of the module to be diagnosed is started.

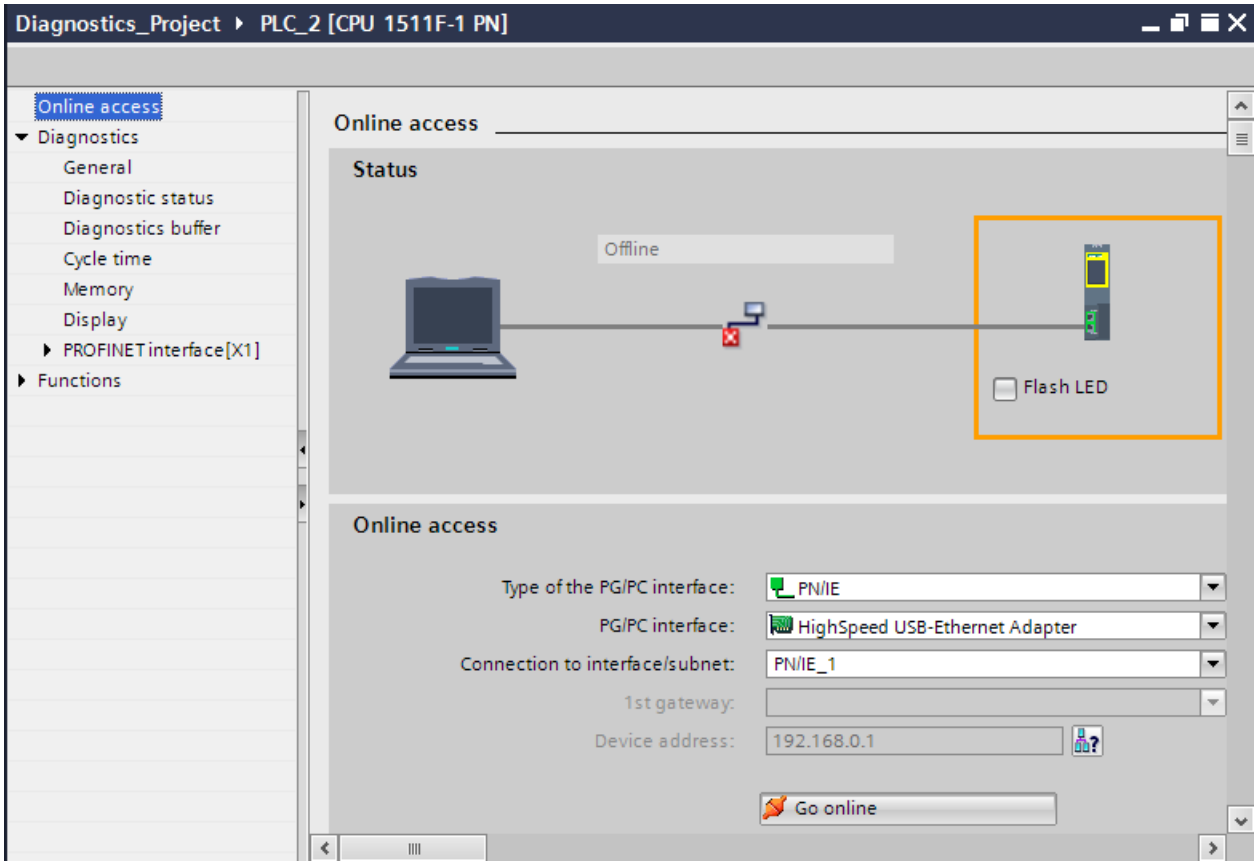


Figure 3-19 Setting online access

3. Make the settings for the interface.
   Here you can change an interface access that has already been set for an online connection that was successfully established previously.
4. Click on the "Go online" button.
   The online connection is established.

Result

You can find detailed diagnostics information on each device in the Inspector window, in the "Diagnostics" section of the area navigation on the "Properties" tab.

5.3.2.5 "Diagnostics" tab in the Inspector window

"Diagnostics" tab in the Inspector window

The "Diagnostics" tab of the Inspector window includes information on diagnostics events and configured alarm events.

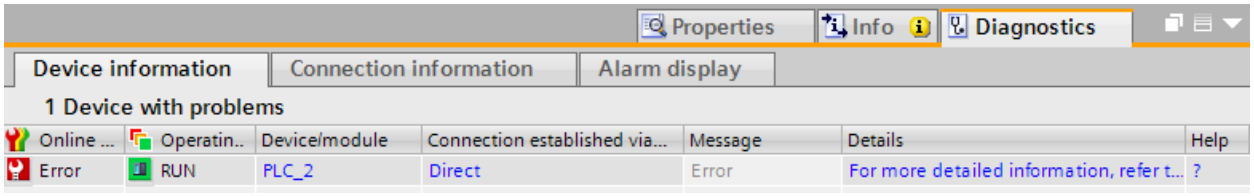


Figure 3-20 Diagnostics in the Inspector window, "Device information" tab

NOTE

Symbols and their meaning

You can find a legend with the meaning of each symbol in Explanation of diagnostics symbols (Page 31) and in the online help for STEP 7.

Subordinate "Device information" tab

This tab gives you an overview of faulty devices to which an online connection exists or has existed. The table provides the following diagnostics information on the faulty devices:

- Online status: Includes the online status as diagnostics symbol and in words
- Operating mode: Includes the operating mode as symbol and in words
- Device/module: Name of the affected device or the affected module
- Connection established via ...: Specifies the path used to establish the connection to the failed device.
- Alarm: This explains the entry in the previous columns and displays an alarm, if necessary
- Details: The link opens the online and diagnostics view associated with the device or puts it in the foreground.
  If the device cannot be reached, the link opens the "Go online" dialog.
- Help: The link provides additional information on the fault.

NOTE

Communication and access errors

Errors that occur in the user program (e.g., communication errors, access errors) are not reported in the "Diagnostics" tab of the device information. You must read out the diagnostics buffer of the CPU in the online and diagnostics view to get this information. The link in the "Details" column opens the diagnostics buffer.

Subordinate "Connection information" tab

The "Connection information" tab displays detailed diagnostics information for connections.

There will only be information on the "Connection information" tab if there is an active online connection to at least one end point of the relevant connection.

If a connection has been selected (connection table), the tab contains the following groups:

- Connection details
- Address details of the connection

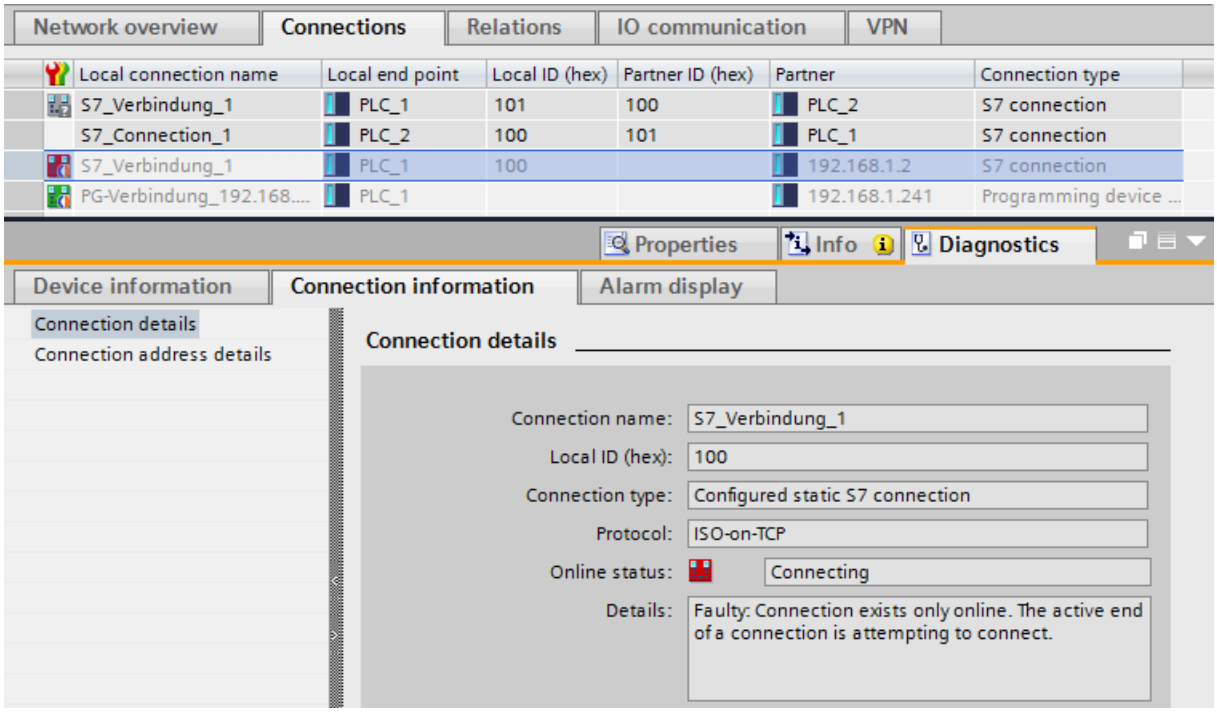


Figure 3-21 "Connection information" tab and open connection overview

If a module has been selected (network view), the tab contains the following group:

- Connection resources

Subordinate "Alarm display" tab

System diagnostics alarms are output in the "Alarm display" tab.

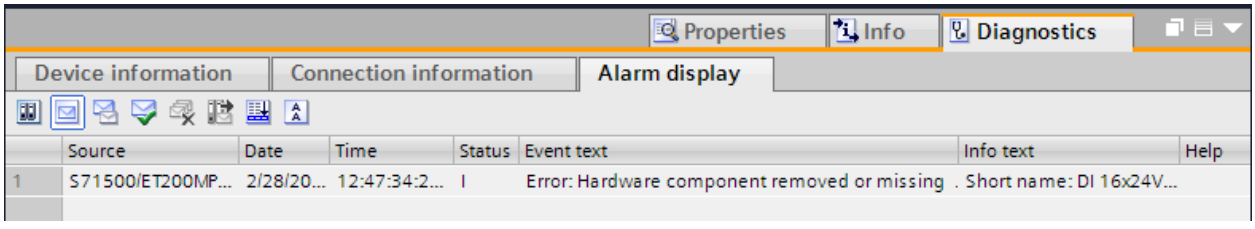


Figure 3-22 "Alarm display" tab

To receive alarms in STEP 7, follow these steps:

1. Open the project view.
2. Select the required CPU in the project tree.
3. To connect online with the respective CPU, select the shortcut menu command "Go online".
4. Select the required CPU once again in the project tree and select the shortcut menu command "Receive alarms".

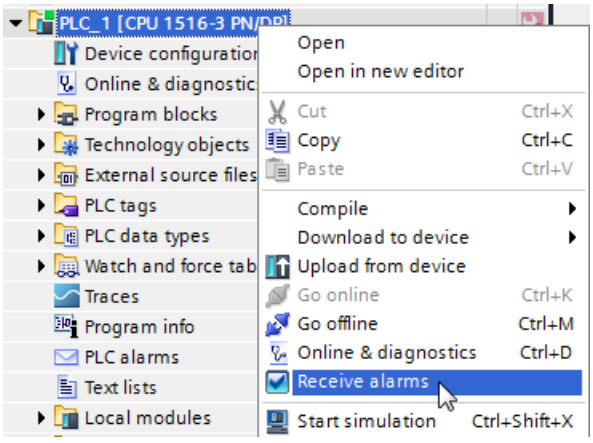


Figure 3-23 Receive alarms

5. Alarms are now displayed in the alarm display. "Archive view" is enabled by default.
6. To display the latest alarms, click the "Active alarms" icon .

5.3.2.6 CPU diagnostics buffer

Definition

Each CPU and some other modules have their own diagnostics buffer, in which detailed information on all diagnostic events is entered in the order in which they occurred.

The CPU diagnostics buffer can be displayed on all display media (STEP 7, SIMATIC HMI devices, SIMATIC S7-1500 Web server and display of the CPU).

Diagnostic events

The entries available in the diagnostics buffer include:

- Internal and external errors on a module
- System errors in the CPU
- Operating mode transitions (e.g., from RUN to STOP)
- Errors in the user program
- Removal/insertion of modules
- Security events

The contents of the diagnostics buffer are stored in the retentive memory in case of a memory reset of the CPU. Errors or events can be evaluated even after a longer period of time

thanks to the diagnostics buffer to determine the cause of a STOP or to trace the occurrence of a single diagnostic event and to be able to assign it.

Procedure

To display the diagnostics buffer of a CPU in STEP 7, follow these steps:

1. Select the respective CPU.
2. Select the shortcut menu command "Online & Diagnostics".
   The "Online access" view is opened in the work area.

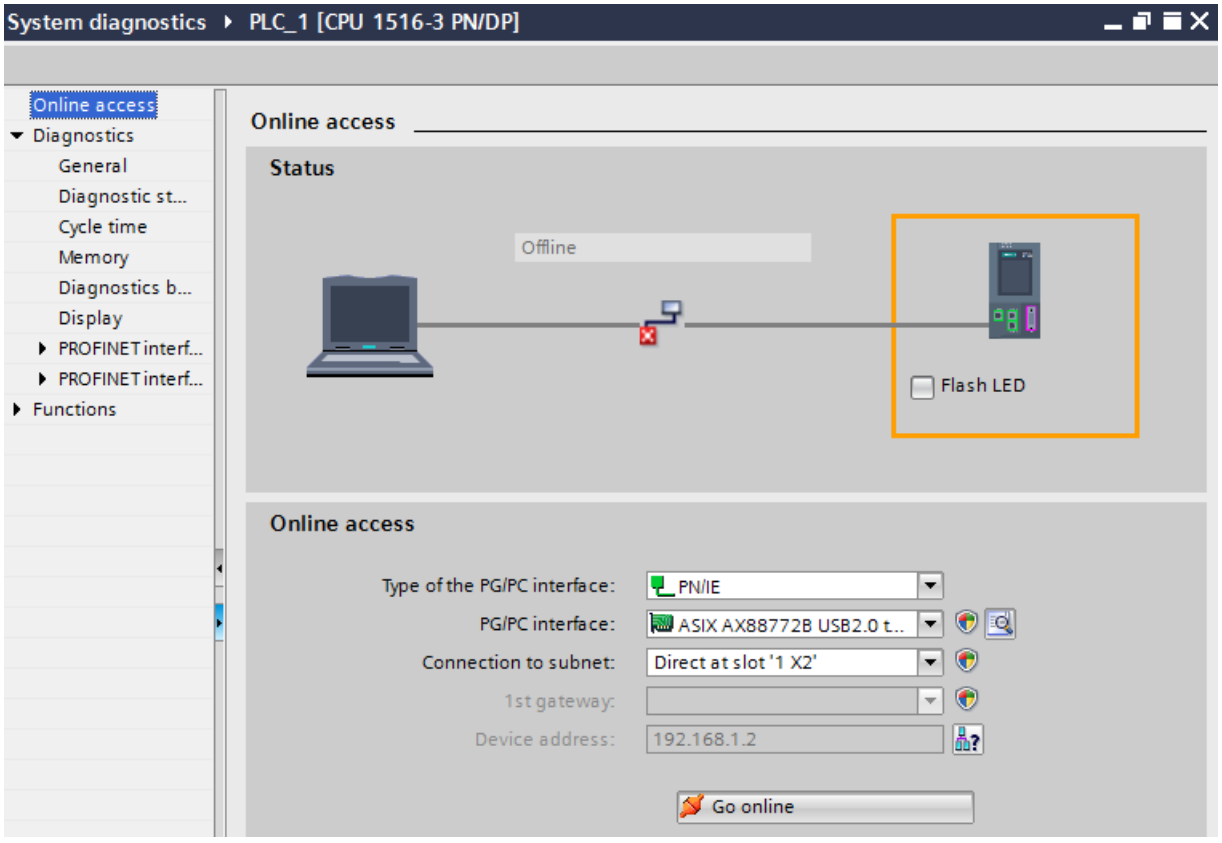


Figure 3-24 Setting up online access

3. Set the interface.
4. Click Go online.

5. Select the area "Diagnostics buffer".

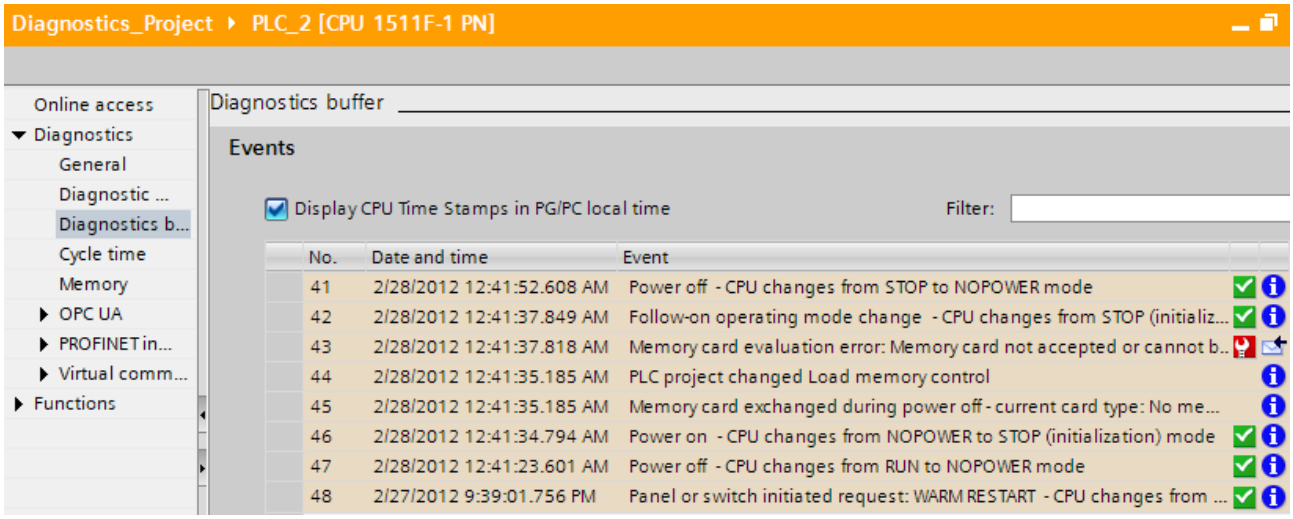


Figure 3-25 Diagnostics buffer in STEP 7

NOTE

Filtering events

You can filter the entries in the diagnostics buffer in the settings of the "Diagnostics buffer" area to only display specific types of events. This means that specific events, such as "CPU and configuration-internal events" or "Connection diagnostics events", can be displayed separately.

Security events

The following security events (event types) result in an entry in the diagnostics buffer.

- Going online with the correct or incorrect password
- Manipulated communications data detected
- Manipulated data detected on memory card
- Manipulated firmware update file detected
- Changed protection level (access protection) downloaded to the CPU
- Password legitimization restricted or enabled (by instruction or CPU display)
- Online access denied due to the possible number of simultaneous access attempts being exceeded
- Timeout when an existing online connection is inactive
- Logging on to the Web server with the correct or incorrect password
- Creating a backup of the CPU
- Restoring the CPU configuration (Restore)

To prevent the diagnostics buffer being "swamped" by large numbers of identical security events, you can set parameters so that these events are entered in the diagnostics buffer as a group alarm. For every interval (monitoring time), the CPU then only generates one group alarm per event type.

Configuring a group alarm for security events
To configure group alarms for security events, follow these steps:

1. Click on the CPU icon in the network view.
   The properties of the CPU are displayed in the Inspector window.
2. Navigate to the "Protection" > "Security event" area.
3. Click "Security event".
4. Select the option "Summarize security events in case of high message volume" to enable group alarms for security events.
5. Set the duration of an interval (monitoring period); the default is 20 seconds.

5.3.2.7 "Online tools" task card

Online view in the "Online tools" task card

The following requirements must be met to display the online view of the "Online tools" task card in STEP 7:

- An online connection to the CPU is available.
- You have selected the CPU in the topology view, network view or device view.

The "Online tools" task card provides an overview of the CPU state, the cycle time and the memory usage.

- The "CPU operator panel" pane displays the current state of some LEDs and the mode selector of a CPU.
- The "Cycle time" pane displays the cycle time diagram and below it the measured cycle times as absolute values.

- The "Memory" pane contains the current memory usage of the associated CPU. The free memory is shown both as a bar graph and as a numerical value (percentage).
  The display for "Load memory" contains, in addition to the online project data (program code, data blocks, hardware configuration etc.), all other data that may be on the SIMATIC memory card, such as recipes, data logs, HMI backups or non-SIMATIC files that have been copied to the memory card via the Web server of the CPU or offline in Explorer (for example, PDF files).

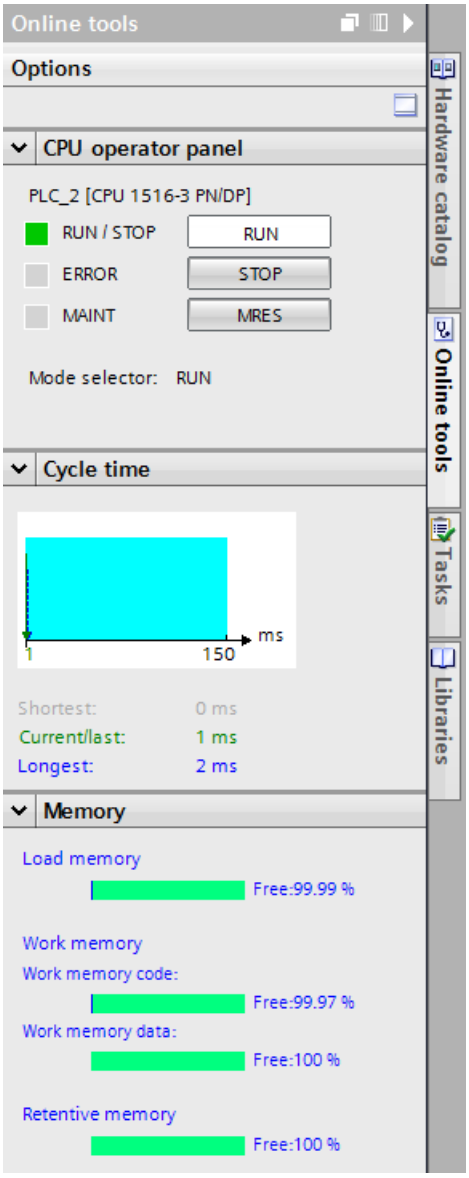


Figure 3-26 "Online tools" task card

5.3.2.8 Configuring the settings for I/O modules in STEP 7

You can also make settings for system diagnostics in STEP 7 for I/O modules. The parameters you have to configure depend on the I/O module.

The settings are optional.

Requirements

- STEP 7 is open.
- A project is open.
- The project view is open.
- A design with I/O modules has been configured.

Procedure

To make settings for system diagnostics of I/O modules in STEP 7, follow these steps:

1. Select the respective I/O module in the device view.
2. Open the "Properties" tab in the Inspector window.
3. Select the area "Inputs", for example.

   You have access to the settings for system diagnostics of the I/O module. If you select "Wire break", for example, a possible wire break for the channel is signaled during operation.

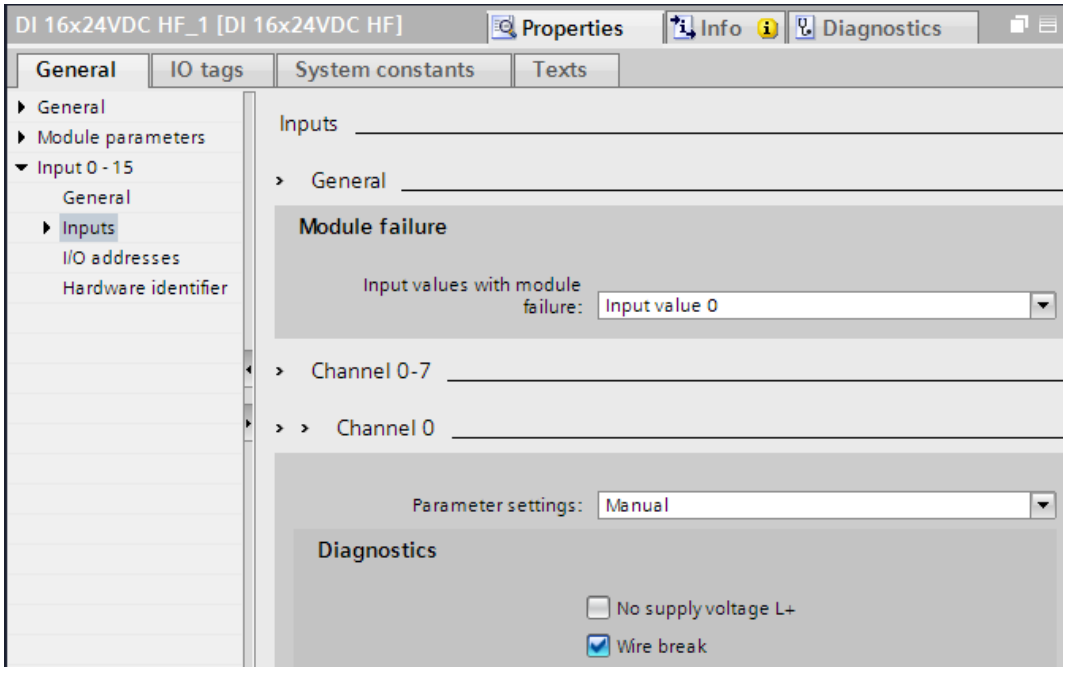


Figure 3-27 I/O setting with a digital input module

4. Save the hardware configuration.
5. Download the new hardware configuration to the CPU.

Additional information

The documentation for the respective module includes additional information on parameter assignment of I/O modules.

5.3.3 Diagnostics information using the web server

System diagnostics using the CPU Web server

The CPUs of the SIMATIC series have an integrated Web server and let you display the system diagnostics information by means of PROFINET. Any terminal devices, such as PCs or smartphones, can thus access module data, user program data and diagnostics data of a CPU by using an Internet browser. This means access to CPUs is possible without installed STEP 7.

In addition to normal websites, the Web server provides so-called basic websites with reduced content that are adapted to the requirements of small screens with low resolution.

Using CPU 1516-3 PN/DP as an example, the following figure shows the start page of the Web server:



Figure 3-28 Web server, Start page

The following diagnostics options are available with the integrated Web server:

- Start page with general CPU information
- Information on diagnostics
- Contents of the diagnostics buffer
- Module information
- Alarms
- Information about communication
- PROFINET topology
- Motion Control diagnostics
- Trace

Configuring the Web server in STEP 7

Proceed as follows to activate the Web server:

Requirements

- You have opened STEP 7.
- You have added a CPU to the project.
- You have opened the project view.

Procedure

1. Open the network view.
2. Select the CPU.
3. Open the "Properties" tab in the Inspector window.
4. Select the entry "Web server" in the "General" area navigation.

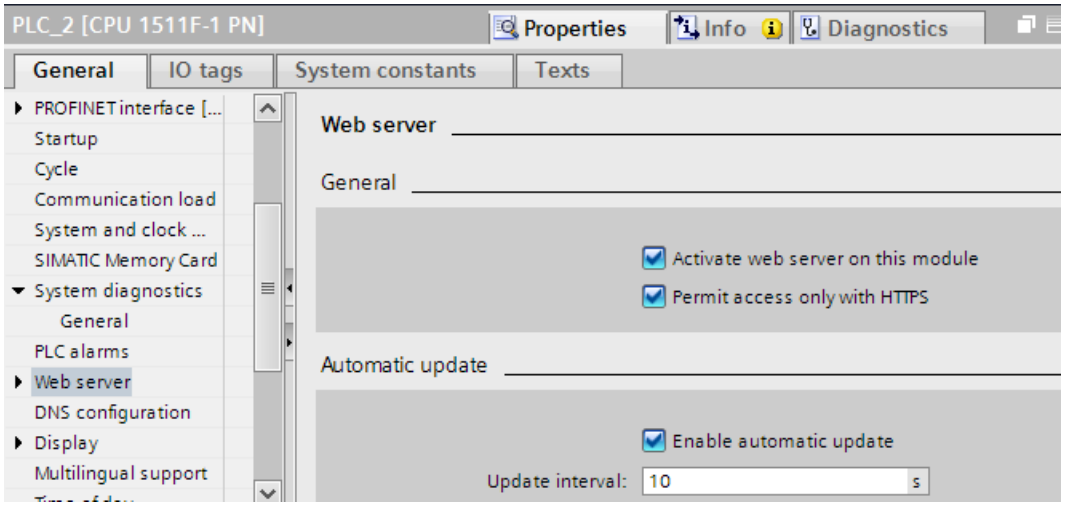


Figure 3-29 Activate the Web server

5. Select the "Activate web server on this module" check box.

6. "Permit access only with HTTPS": The activation of the Web server using the secure transmission protocol "HTTPS" requires a valid Web server certificate in the CPU.

NOTICE
Utilizing the full functionality of the Web server A valid CA-signed Web server certificate in the CPU is a requirement for: – User management with password-protected users – Saving and downloading diagnostic information in csv files – Using the following safety-related functions: – Backing up and restoring the CPU configuration To use the full functionality of the Web server, we recommend that you create a CA-signed server certificate and assign it to the CPU. To create a CA-signed Web server certificate, you must enable the Certificate Manager in the global security settings of STEP 7 and assign a CA-signed server certificate to the Web server in the properties of the CPU. You can find additional information on handling Web server certificates in the "Configuring the Web server" section of the Web server function manual (http://support.automation.siemens.com/WW/view/en/59193560). Detailed information on Certification Authority (CA) certificates, device certificates (End Entity certificate), "Public Key Infrastructure" (PKI) and certificate management can be found in the Communication function manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) and in the online help for STEP 7, keyword "Secure communication".

7. Automatic updating is activated in the default setting of a configured CPU.
8. Activate the Web server also for each interface via which you want to access the Web server.
   To do this, open the "Properties" tab in the Inspector window and select the "Web server" entry in the "General" area navigation. In the "Overview of interfaces" area, select the "Enabled web server access" check box for the corresponding interface.
9. Compile and load the configuration into the CPU.

Accessing the Web server

To access the Web server, proceed as follows:

1. Connect the display device (PG/PC, HMI, mobile terminal device) with the CPU or a communication module using a PROFINET interface.
   If you are working with WLAN, activate the WLAN on the display device and establish a connection to the access point (e.g. SCALANCE W788-1RR or SCALANCE W784-1), which is in turn connected to the CPU.
2. Open the web browser on the display device.
3. Enter the IP address of the interface of the CPU which is connected to the client in the "Address" field of the web browser in the following format: http://a.b.c.d or https://a.b.c.d (example input: https://192.168.3.141).
   The intro page of the CPU opens.

4. You need to perform the installation of the CA certificate again for each display device you want to use. A valid CA certificate is available for download from the "Intro" web page under "Download certificate". You can find instructions for installing the certificate in the help system of your Web browser and in the FAQ with the entry ID 103528224 at the Service&Support (https://support.industry.siemens.com/cs/ww/en/view/103528224) website.
5. Click the NEXT link to go to the Web server pages.

NOTE

Managing access rights
In STEP 7, you can create users, define access rights and assign passwords under "Web server > User management". Users only have access to the options that are permanently linked to the access rights.
You can find additional information on managing access rights in the "Configuring the Web server" section of the Web server function manual (http://support.automation.siemens.com/WW/view/en/59193560).

"Diagnostics" option

The "Diagnostics" web page provides more information about the tabs:

- Identification
  This tab contains the characteristics of the CPU (serial number, article number, hardware and firmware version, etc.).
- Program protection
  This tab provides information on whether the PLC program contains know-how protection or copy protection.
- Memory
  This tab contains current values on the memory currently in use.
- Runtime information
  Current information on program/communication load and cycle time can be found in this tab.
- Fail-safe (only with an F CPU)
  The safety program of an F-CPU consists of one or two F-runtime groups. You can find their cycle time (F-monitoring time) and runtime in this tab.

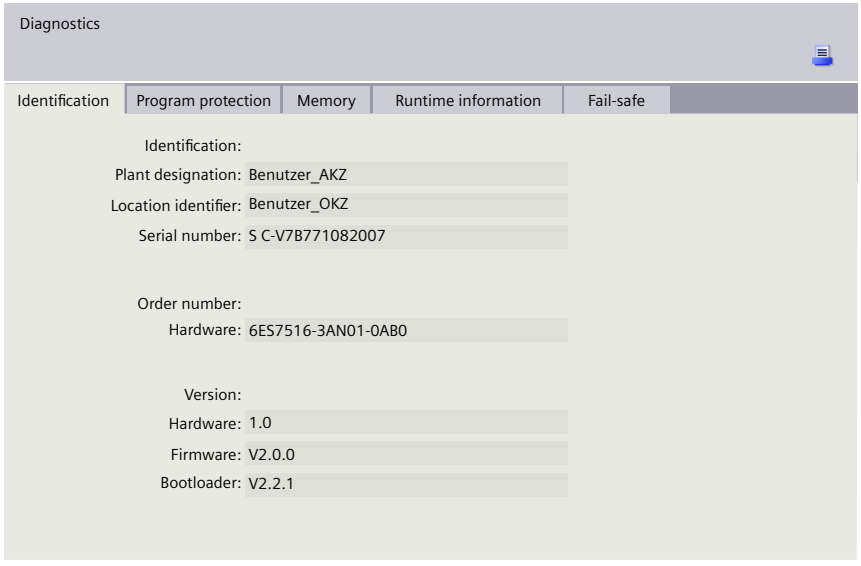


Figure 3-30 Web server, "Diagnostics" Web page

Diagnostics option "Diagnostics buffer"

The browser displays the content of the diagnostics buffer on the "Diagnostics buffer" Web page.

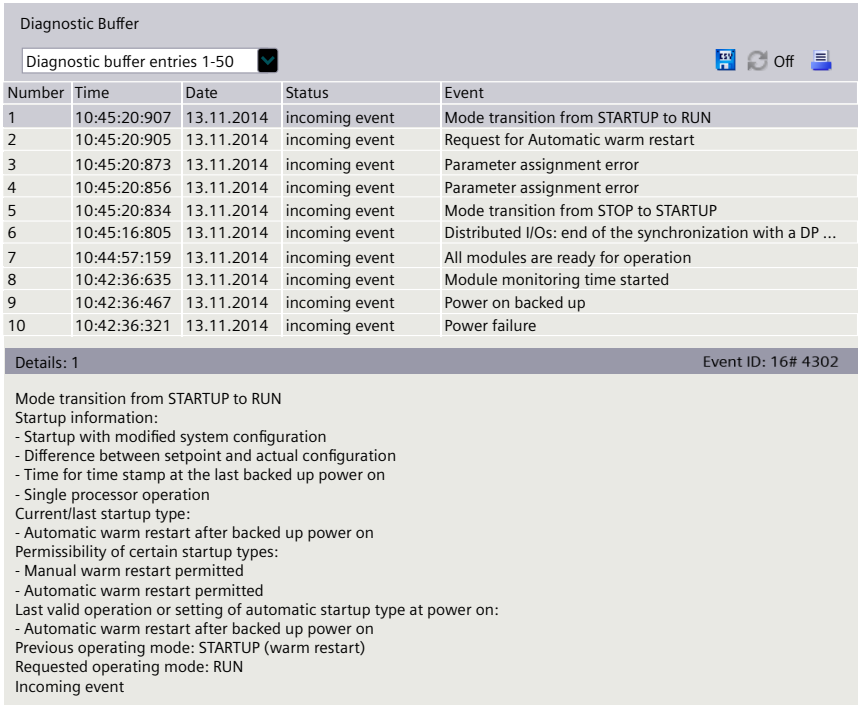


Figure 3-31 Web server, "Diagnostics buffer" Web page

Diagnostics option "Module information"

The status of a device is indicated by the Web browser with symbols and comments on the "Module information" Web page.

Modules are displayed on the "Module information" Web page in the "Name" column with a link. You can thus get to the faulty module in hierarchical order.

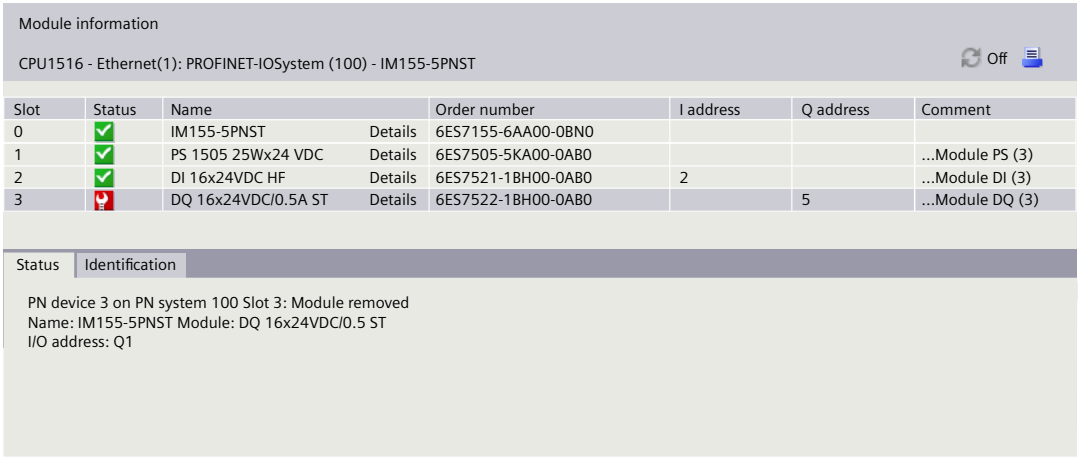


Figure 3-32 Web server, "Module information" Web page

Diagnostics option "Messages"

The Web browser displays the content of the message buffer on the "Messages" Web page. The messages can be acknowledged via the Web server if you have the appropriate user rights.

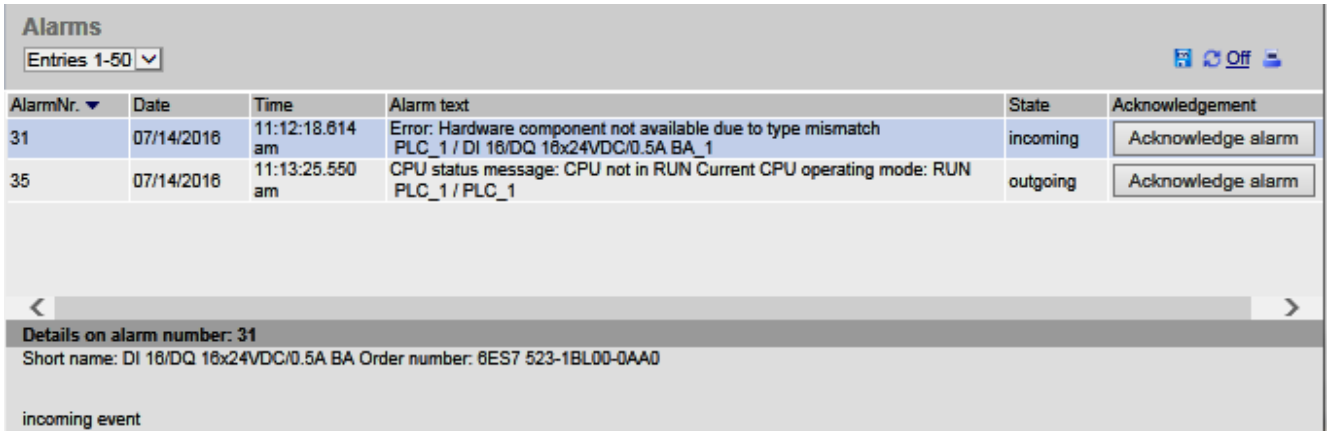


Figure 3-33 Web server, "Messages" Web page

Diagnostics option "Communication"

The "Communication" web page provides detailed information about the following tabs:

- Parameter
  A summary of the information on the PROFINET and Ethernet interfaces of the selected CPU is available in this tab.
- Statistics
  You will find information on data transmission in this tab.
- Resources
  Information about the resource consumption of the connections is available in this tab.
- Connections
  Information about the status of the communication connections is available in this tab.

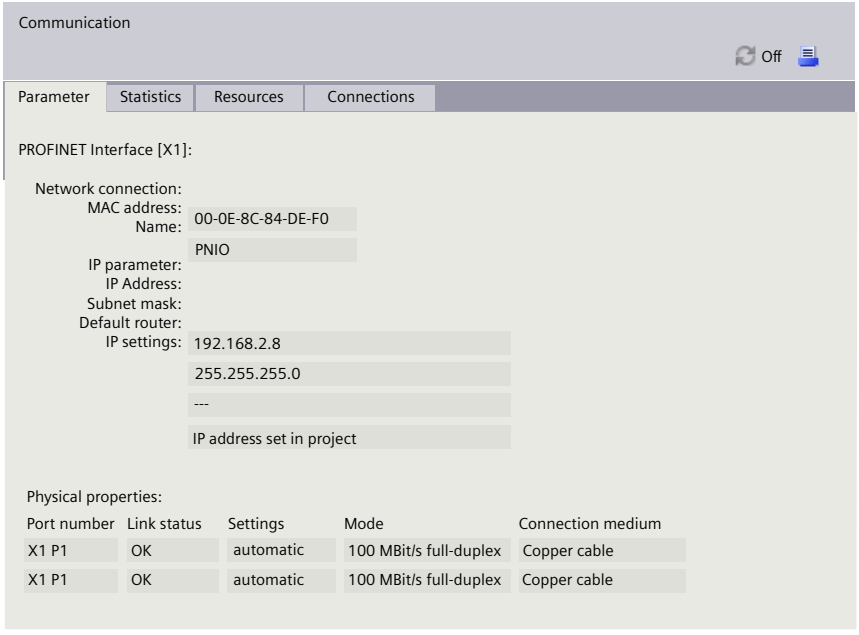
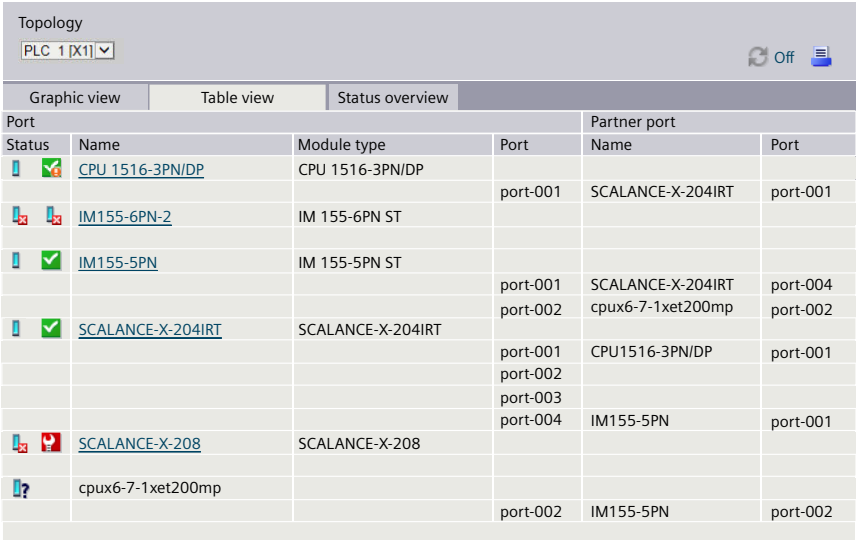


Figure 3-34 Web server, "Communication" Web page

"Topology" diagnostics option

The "Topology" Web page provides information on the topological configuration and status of the PROFINET devices in your PROFINET IO system.



Port				Partner port	
Status	Name	Module type	Port	Name	Port
	CPU 1516-3PN/DP	CPU 1516-3PN/DP			
			port-001	SCALANCE-X-204IRT	port-001
	IM155-6PN-2	IM 155-6PN ST			
	IM155-5PN	IM 155-5PN ST			
			port-001	SCALANCE-X-204IRT	port-004
			port-002	cpux6-7-1xet200mp	port-002
	SCALANCE-X-204IRT	SCALANCE-X-204IRT			
			port-001	CPU1516-3PN/DP	port-001
			port-002		
			port-003		
			port-004	IM155-5PN	port-001
	SCALANCE-X-208	SCALANCE-X-208			
	cpux6-7-1xet200mp				
			port-002	IM155-5PN	port-002

Figure 3-35 Web server, "Topology" Web page

"Motion Control Diagnostics" diagnostic option

The Web server displays statuses, errors, technology alarms and the current values of the configured technology objects (TOs).

The "Motion Control Diagnostics" web page provides detailed information on the configured technology objects in the following views:

- Diagnostics

  This view provides an overview list of configured technology objects, the status and error messages of a selected technology object, as well as values and limits of the movement status for a selected axis.
- Service overview

  This view contains diagnostic information for multiple technology objects and a filter option for selecting the displayed technology objects.

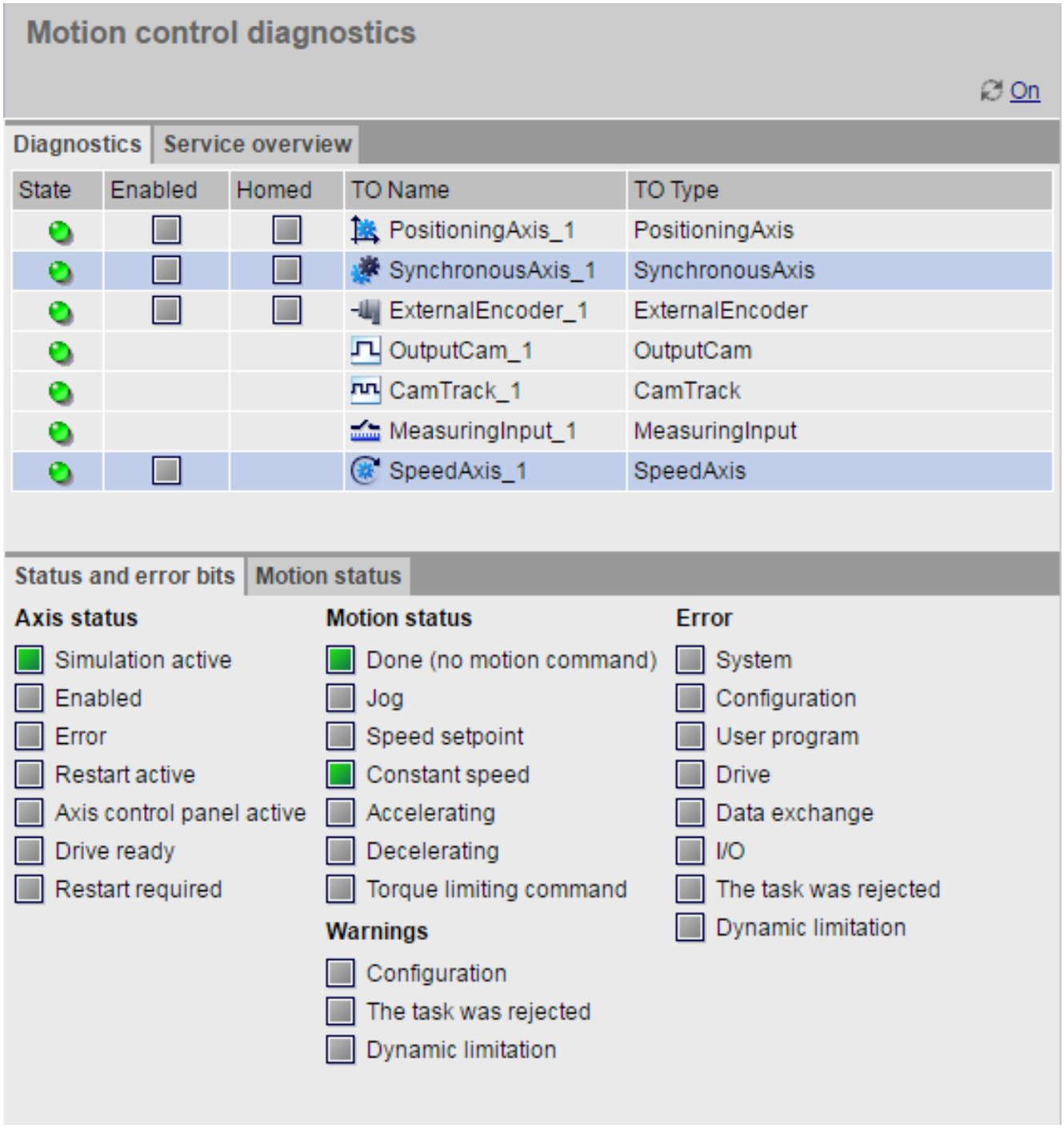


Figure 3-36 Web server, "Motion Control diagnostics" webpage

"Trace" diagnostic options

You can read, view and save the trace recordings via the Web server and thus obtain plant and project information for diagnostics and maintenance.

The web page of the trace and logic analyzer function consists of several areas. The example in the figure below shows how the Web server user interface is divided when the "Trace" web page is first called.

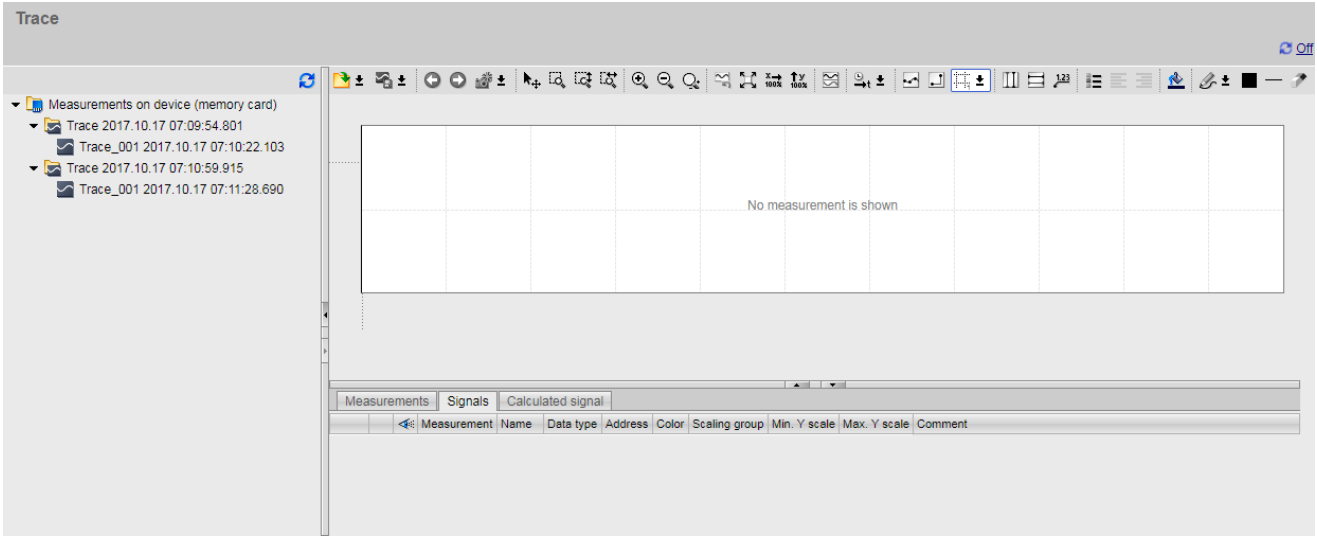


Figure 3-37 Web server, "Trace" home page (without measurement)

Additional information

Additional information on the topic is available in the Web server function manual (http://support.automation.siemens.com/WW/view/en/59193560).

You can find additional information on the trace function in the Using the trace and logic analyzer function (https://support.industry.siemens.com/cs/ww/en/view/64897128) function manual.

5.3.4 Showing diagnostic information on an HMI device

Components and objects for system diagnostics

You can use the functionality of system diagnostics via HMI devices with the following components:

- SIMATIC components:
  - Basic Panels
  - Comfort Panels
  - Mobile Panels
  - WinCC RT Advanced
- SIMATIC Unified components:
  - Unified Basic Panels
  - Unified Comfort Panels
  - WinCC Unified PC

The following table provides an overview of the SIMATIC components with their supported diagnostics objects in WinCC.

Table 3-6 SIMATIC components and system diagnostics objects in WinCC

Component	System diagnostics indicator	System diagnostics view	System diagnostics window
Basic Panel	-	X[1)]	-
Comfort Panel	X	X	X
Mobile Panel	X	X	X
WinCC RT Advanced	X	X	X

1) Only diagnostics buffer view possible

The following sections and paragraphs describe the objects and procedures for WinCC devices and WinCC software.

You can find information on objects and procedures in WinCC Unified devices and WinCC Unified software in the section System diagnostics in WinCC Unified (Page 69).

System diagnostics indicator

The system diagnostics indicator shows the overall status of your plant in one of two states as follows:

- Green with white checkmark: No error
- Red with white wrench: Error

If at least one CPU indicates an error, the overall status also indicates an error.

System diagnostics view

The system diagnostics view reflects the current status of all accessible devices in your plant. You navigate directly to the cause of the error and the associated device. You have access to all diagnostics-capable devices that you have configured in the STEP 7 hardware and network editor.

System diagnostics window

The system diagnostics window is an operating element and display object.

The functions of the system diagnostics window are the same as for the system diagnostics view. Because the system diagnostics window is configured in the "Global screen", you can also specify, for example, whether the object can be closed in WinCC Runtime.

5.3.4.1 Configuring system diagnostics

Introduction

You can add a system diagnostics view or a system diagnostics window to your project to get a diagnostics overview of all devices available in your plant.

The system diagnostics window behaves like the system diagnostics view but is only available in the global screen.

Requirements

- At least one CPU has been set up in the project.
- An HMI device (e.g. Comfort Panel) has been set up in the project.
- The CPU and the HMI device are connected with each other by an HMI connection.
- You have created a screen (for the system diagnostics view).
- The global screen is open (for the system diagnostics window).
- The "Toolbox" task card is open.

Procedure

Proceed as follows to configure the system diagnostics view:

1. Insert a system diagnostics view in your project:
   - To insert in the global screen: Double-click the "System diagnostics window" object in the "Toolbox" task card in the "Controls" pane. The object is added to the global screen.
   - To insert in any screen: Double-click the "System diagnostics view" object in the "Toolbox" task card in the "Controls" pane. The object is added to the opened screen.

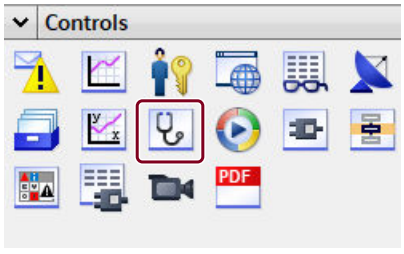


Figure 3-38 Adding a system diagnostics view

2. Select the "Properties" tab in the Inspector window.
3. Select the area "Columns".

4. Enable the columns that you require in the device view for WinCC Runtime, for example:
   - Operating mode
   - Slot
   - Type
   - Article number
   - Address

   The "Status" and "Name" columns are enabled by default and cannot be deselected.
5. Change the default values under "Device view column width" if necessary. You can also adapt the column widths during runtime.
6. Enable the columns that you require in the details view for WinCC Runtime, for example:
   - Operating mode
   - Rack
   - Slot
   - Address
   - Plant designation
   - Error description
7. Change the headers for the columns under "Column header", if required.
8. To close the system diagnostics window in WinCC Runtime, select the "Close button:" option in the "Header" area under "Properties > Window" in the "Properties" tab of the Inspector window.

Result: Any screen result

The system diagnostics view has been added to the screen. The diagnostics status of the entire plant is displayed in the system diagnostics view in WinCC Runtime.

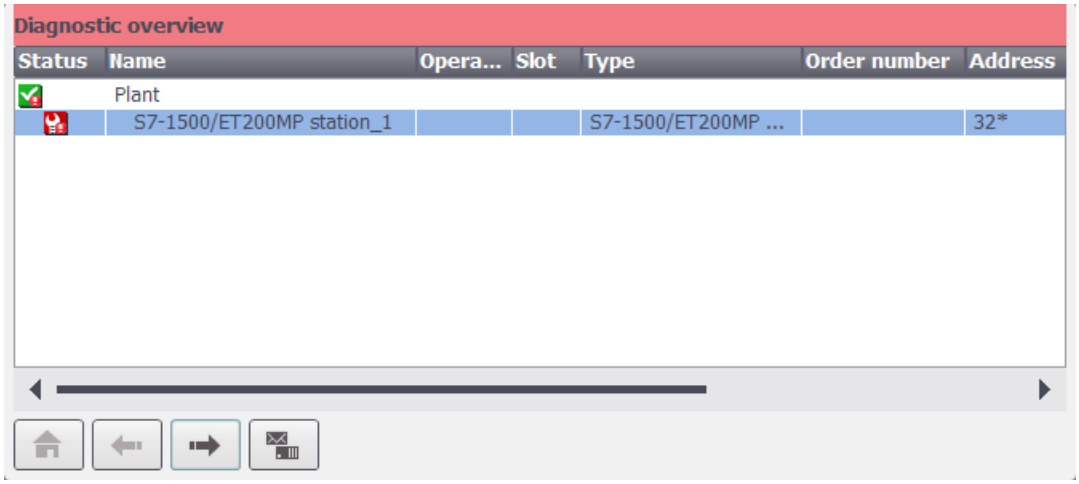


Figure 3-39 System diagnostics view in the screen

Result: Global screen result

The system diagnostics window has been added to the global screen. If there is an error message in the plant, the system diagnostics window responds and displays the affected device.

5.3.4.2 Different views of the system diagnostics view

Introduction

The following views are available in the system diagnostics view and the system diagnostics window in WinCC Runtime:

- Diagnostic overview
- Device view
- Details view
- Distributed I/O view (only for PROFIBUS and PROFINET- systems)
- Diagnostics buffer view

Diagnostic overview

The "Diagnostic overview" screen is the start screen of the system diagnostics view in WinCC Runtime. In this view, you can select the station for which you want to display additional diagnostic information.

The "Status" column shows the status of the overall plant and the associated stations using symbols.

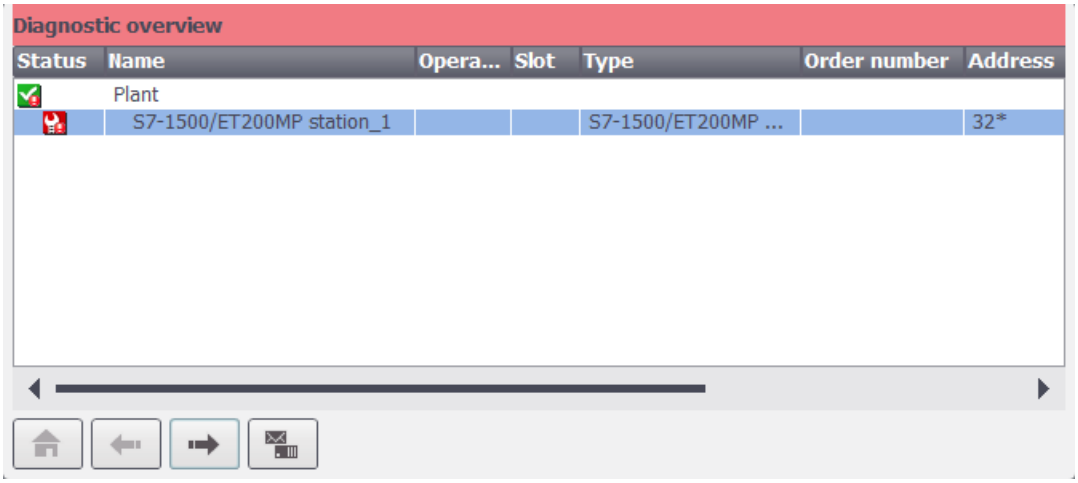


Figure 3-40 Diagnostic overview

Device view

The device view shows all the available devices of a layer in a table. Double-clicking on a device opens either the lower-level devices or the details view. The symbols in the first column provide information about the current state of the device.

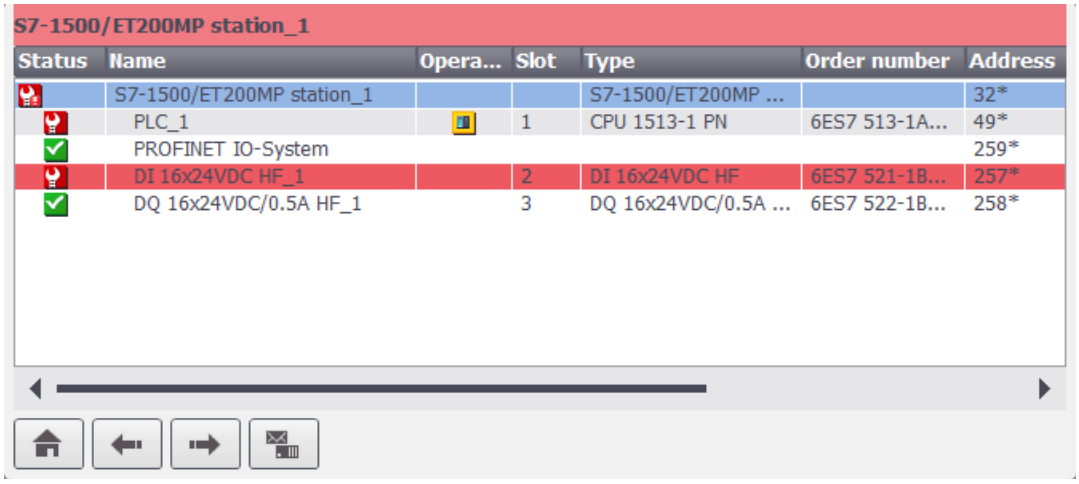


Figure 3-41 Device view

Details view

The details view gives detailed information about the selected device. Check whether the data is correct in the details view.

The error text shows a detailed description of the pending errors and suggestions on resolving the errors.

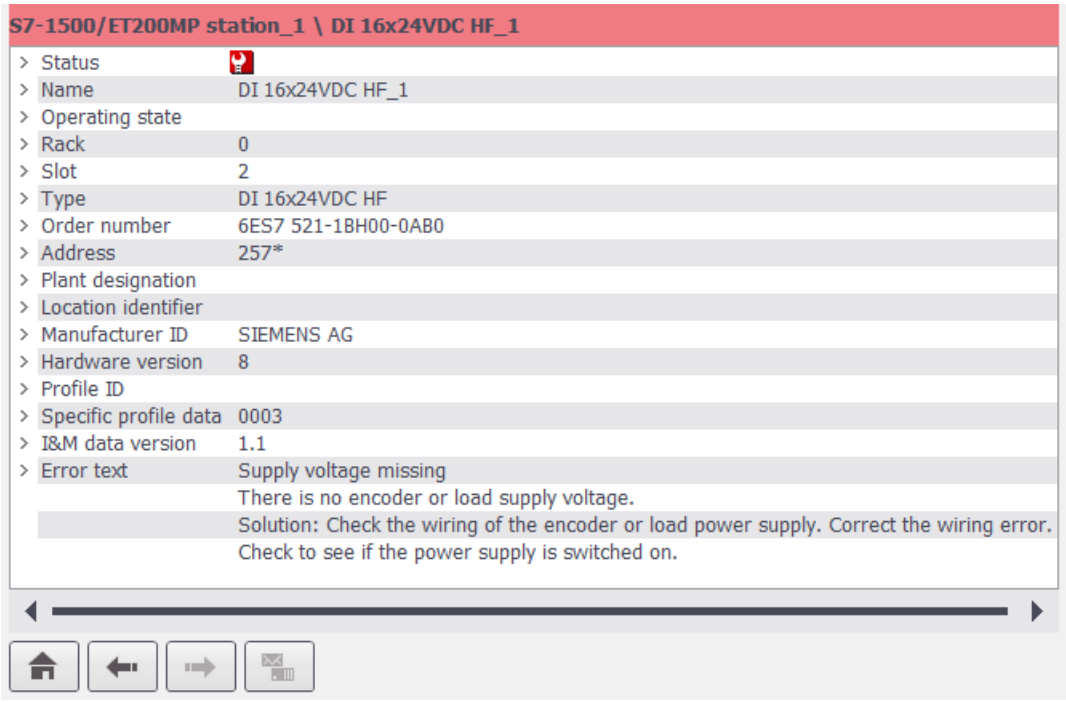


Figure 3-42 Details view

Distributed I/O view

The distributed I/O view is only available for distributed I/O systems. The distributed I/O view shows the status of the devices of the PROFIBUS/PROFINET-subnet.

Each element in the view shows the following information:

- Device name
- Device type
- The IP- or PROFIBUS address.

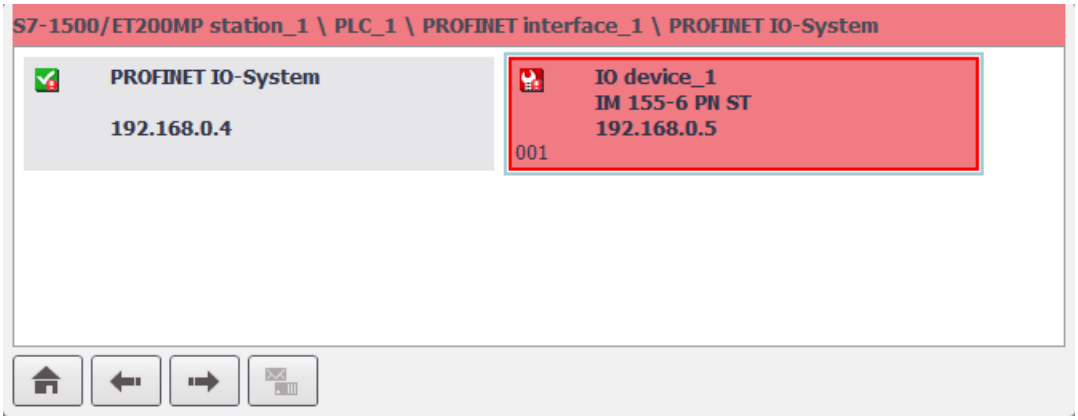


Figure 3-43 Distributed I/O view

Diagnostics buffer view

The diagnostics buffer view shows the current data from the diagnostic buffer of a station, e.g. a CPU. You can obtain detailed information on the event by double-clicking on the corresponding entry.

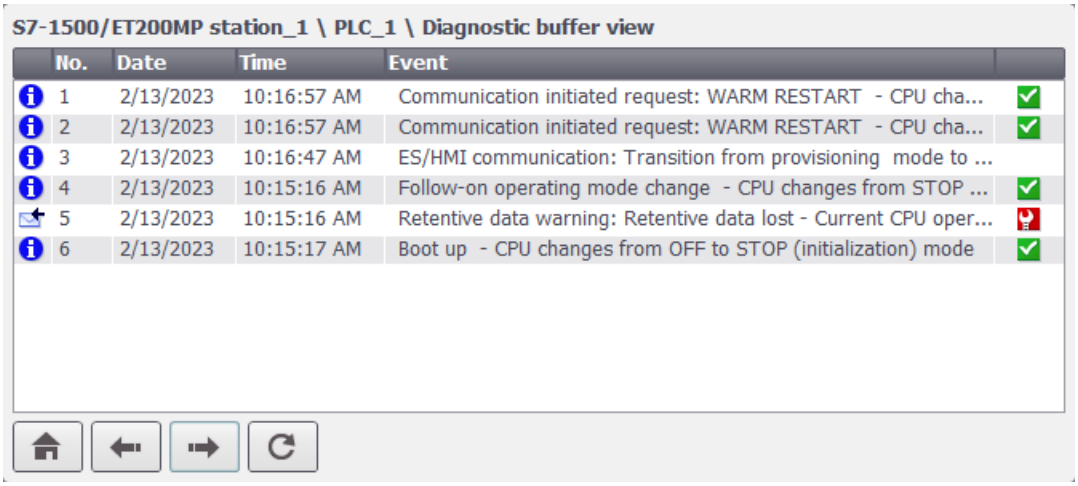


Figure 3-44 Diagnostics buffer view

Navigation buttons

Button	Function
	Opens the diagnostic overview.
	Opens the higher-level device, or the device view if there is no higher-level device.

Button	Function
	Opens the lower-level devices, or the details view if there are no lower-level devices.
	Opens the diagnostics buffer view. Can only be selected if a station is selected.
	Updates the diagnostics buffer view. Can only be selected in the diagnostic buffer view.

5.3.4.3 Inserting system diagnostics indicator

Introduction

The system diagnostics indicator is a predefined graphic library object which alerts you to errors in your plant.

The library object shows the overall status of your plant in one of two states as follows:

- Green with white checkmark: No error
- Red with white wrench: Error

If at least one CPU indicates an error, the overall status also indicates an error.

Requirements

- At least one CPU has been set up in the project.
- An HMI- device (e.g. Comfort Panel) has been set up in the project.
- The CPU and the HMI device are connected with each other via an HMI connection.
- The "Libraries" task card is opened.
- The global library "Buttons-and-Switches > Master copies > DiagnosticsButtons" is open.
- A screen is open.
- The system diagnostics window has been set up in the global screen.

Procedure

1. Select the "DiagnosticsIndicator" object in the global library.
2. Drag-and-drop the library object to the position in the open screen where you want to insert the object.
   The library object is added.
3. Open the "Events" tab in the Inspector window.
   The "ShowSystemDiagnosticsWindow" function is preset for the "Click" event.

4. Next to "Object name", select the system diagnostics window in the global screen.

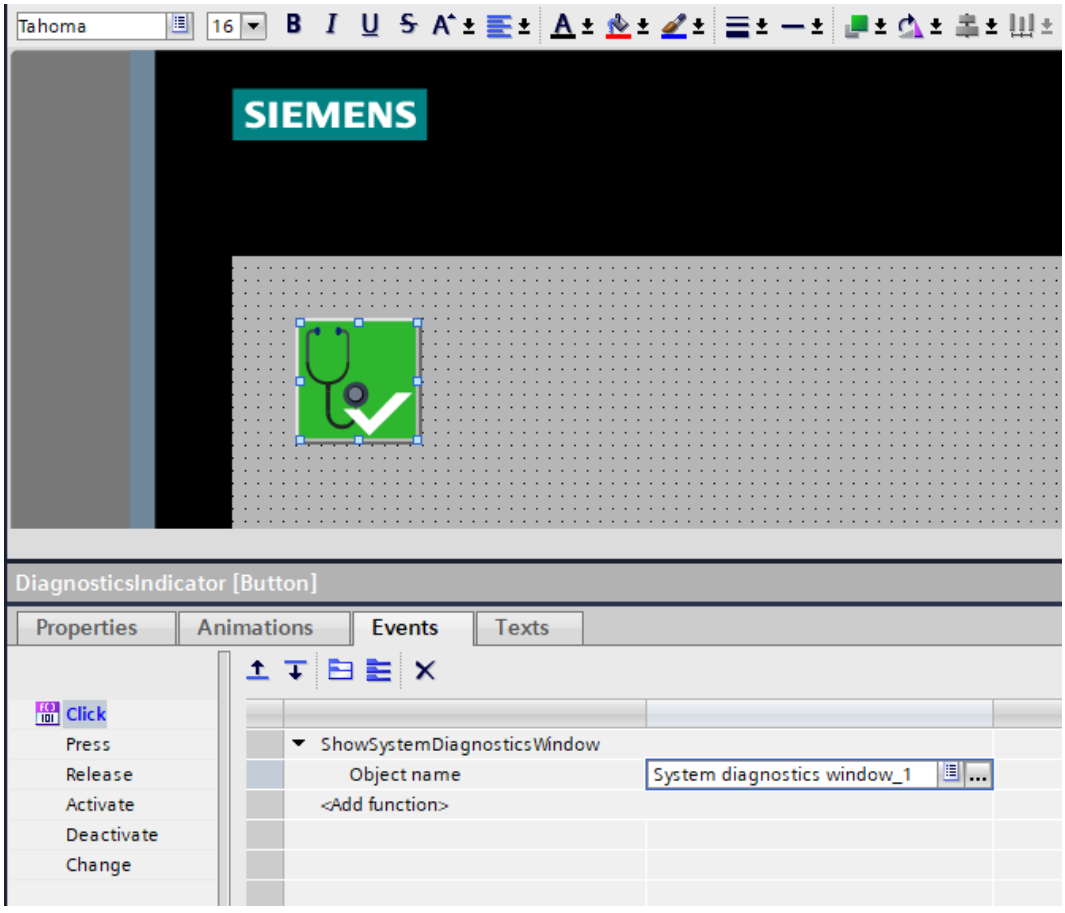


Figure 3-45 Inserting library object in the work area

Result

The system diagnostics indicator has been added to the project and connected with the system diagnostics window.

The system diagnostics indicator changes its appearance if an error message is output in WinCC Runtime. The system diagnostics window opens when you click on the system diagnostics indicator. The system diagnostics window shows the details view of the affected device.

Configuring access protection for the system diagnostics window

Configure access protection for the system diagnostics indicator to prevent unauthorized access to the system diagnostics window.

1. Select the "DiagnosticsIndicator" object in the screen.
2. Open the "Properties" tab in the Inspector window.
3. Navigate to "Security".
4. Select an authorization in the "Security in Runtime" area.

A logon dialog opens when you click on the system diagnostics indicator in WinCC Runtime. The system diagnostics window does not open unless you have the required authorization.

5.3.4.4 Configuring button as system diagnostics indicator

Introduction

Instead of using the "DiagnosticsIndicator" object from the library, you can configure a button in "Graphics" mode, for example, to indicate errors in your plant.

Requirements

- At least one CPU has been created.
- An HMI device (e.g. Comfort Panel) has been set up in the project.
- The CPU and the HMI device are connected with each other via an HMI connection.
- A screen is open.
- The "Toolbox" task card is open.
- A graphics list has been created with two different graphics for the states "Error" and "No error".
- You have created a system diagnostics view.

Procedure

Follow these steps to configure a button as system diagnostics indicator:

1. Double-click the "Button" object in the "Toolbox" task card. A button is added to the screen.
2. Select the "Properties" tab in the Inspector window.
3. Select the "Graphics" option in the "General > Mode" area.
4. Select the "Graphics list" option in the "General > Graphics" area.
5. Select the created graphics list as the graphics list.
6. Select the "@DiagnosticsIndicatorTag" under "Tag" in the "General > Process" area.
7. To assign a function to the button, select the "Events" tab in the Inspector window.
8. Select the "Click" event.
9. Click on "Add function" in the table.
10. Select "EnableSystemDiagnosticsView".
11. Add the settings as follows:
    - Next to "Screen name", select the screen in which the system diagnostics view was created.
    - Select the system diagnostics view next to "Screen object".
12. Correct the height and width of the button as required.

Result

You have configured an interface that reacts to error events from the CPU. The button changes when an error event occurs in Runtime.

The button has two states.

- Error

  The system diagnostics view opens when you click on the button. The system diagnostics view shows the details view of the affected device.
- No error

  The system diagnostics view opens when you click on the button. The system diagnostics view shows the diagnostic overview.

More information

You can find detailed information and procedures for visualization in the TIA Portal online help under "Visualizing processes (Basic Panels, Panels, Comfort Panels, RT Advanced, RT Professional) > Using diagnostics functions".

5.3.4.5 System diagnostics in WinCC Unified

Objects for system diagnostics in WinCC Unified

The following diagnostics objects are available to display system diagnostics on WinCC Unified components:

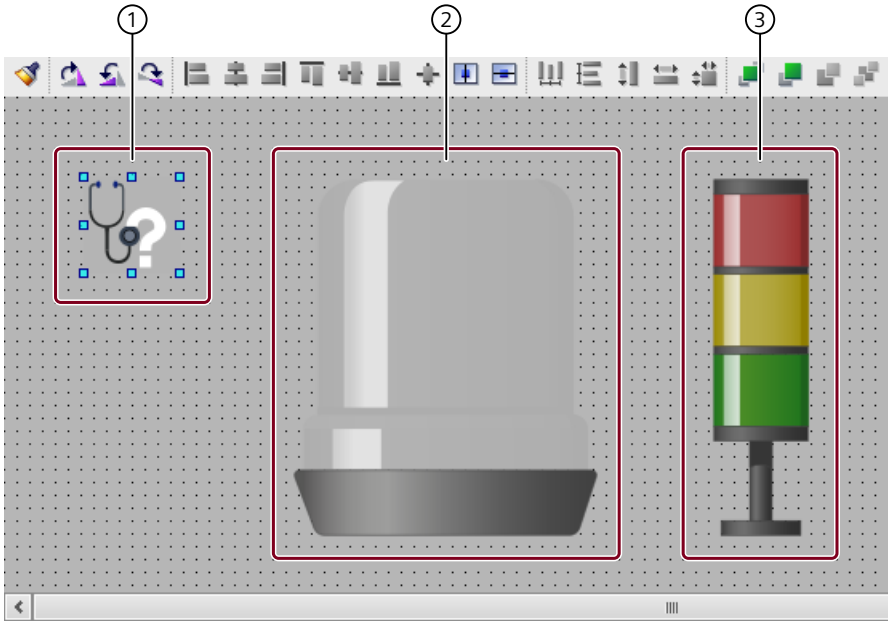
- Diagnostics indicator
- System diagnostics view

You can use each of the diagnostics objects on all WinCC Unified components.

Configuring a diagnostics indicator

A diagnostics indicator shows the overall status of your plant. If at least one CPU indicates an error, the overall status also indicates an error.

In WinCC Unified, you can configure a diagnostics indicator using dynamically scalable vector graphics (DynamicSVGs). The following figure shows the pre-programmed objects provided by WinCC Unified:



① Diagnostics indicator
② Signal lamp
③ Signal tower

To configure a diagnostics indicator in an open screen, follow these steps:

1. Open the "Toolbox" task card.
2. Select the "IndustryGraphicLibrary > SIMATIC > SystemDiagnostic" folder in the "Dynamic widgets" pane.
   You see the pre-programmed objects below.

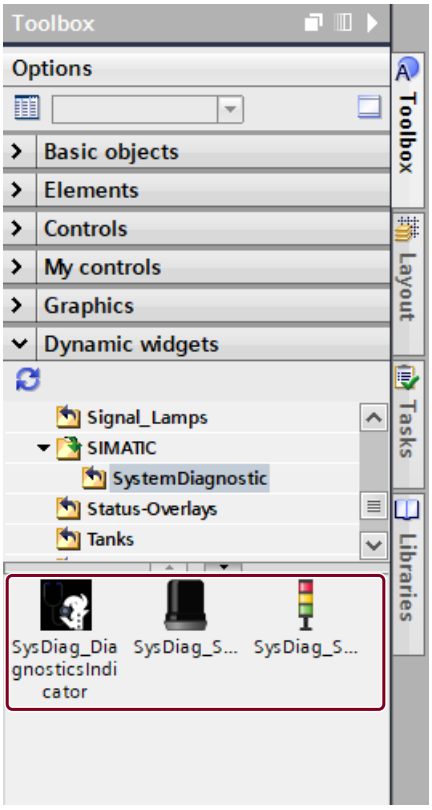


Figure 3-46 "Dynamic widgets" pane

3. Drag-and-drop the desired object onto an open screen.
4. Open the "Properties" tab in the Inspector window.
5. For the "State" parameter, configure dynamization by means of a variable.

6. Select the "@DiagnosticsIndicatorTag" in the "Process" area.

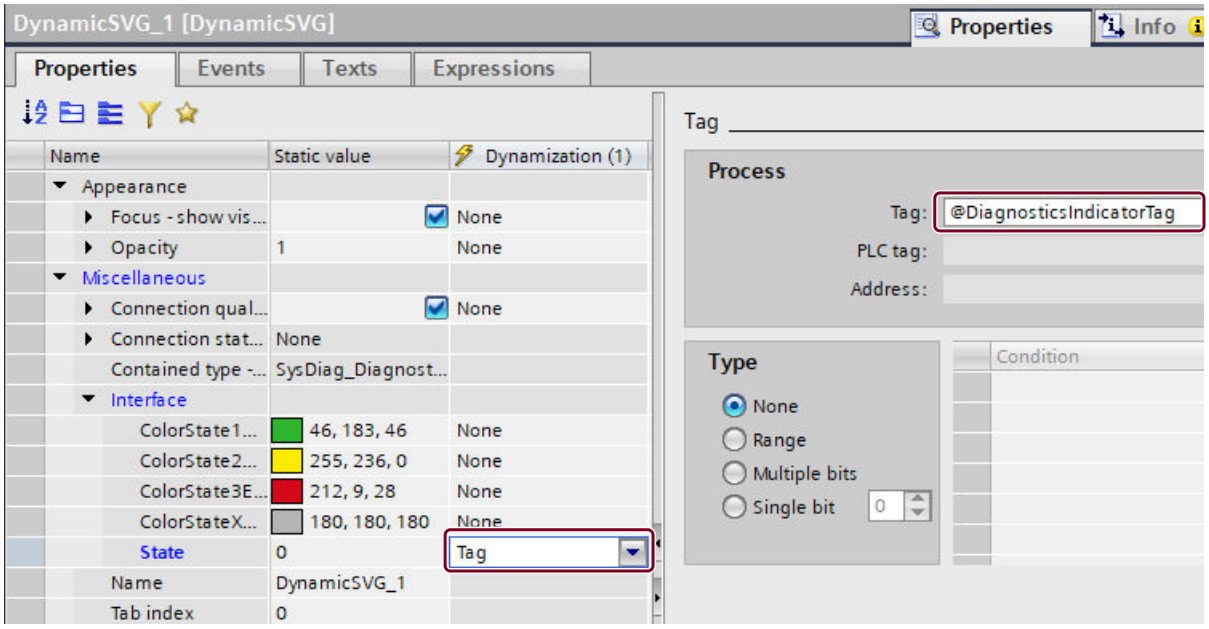


Figure 3-47 Configuring a diagnostics indicator

Result: You have configured a diagnostics indicator and dynamized the status using a tag. The colors of the dynamized SVGs change according to the defined tag values in Runtime.

Table 3-7 Possible diagnostic values

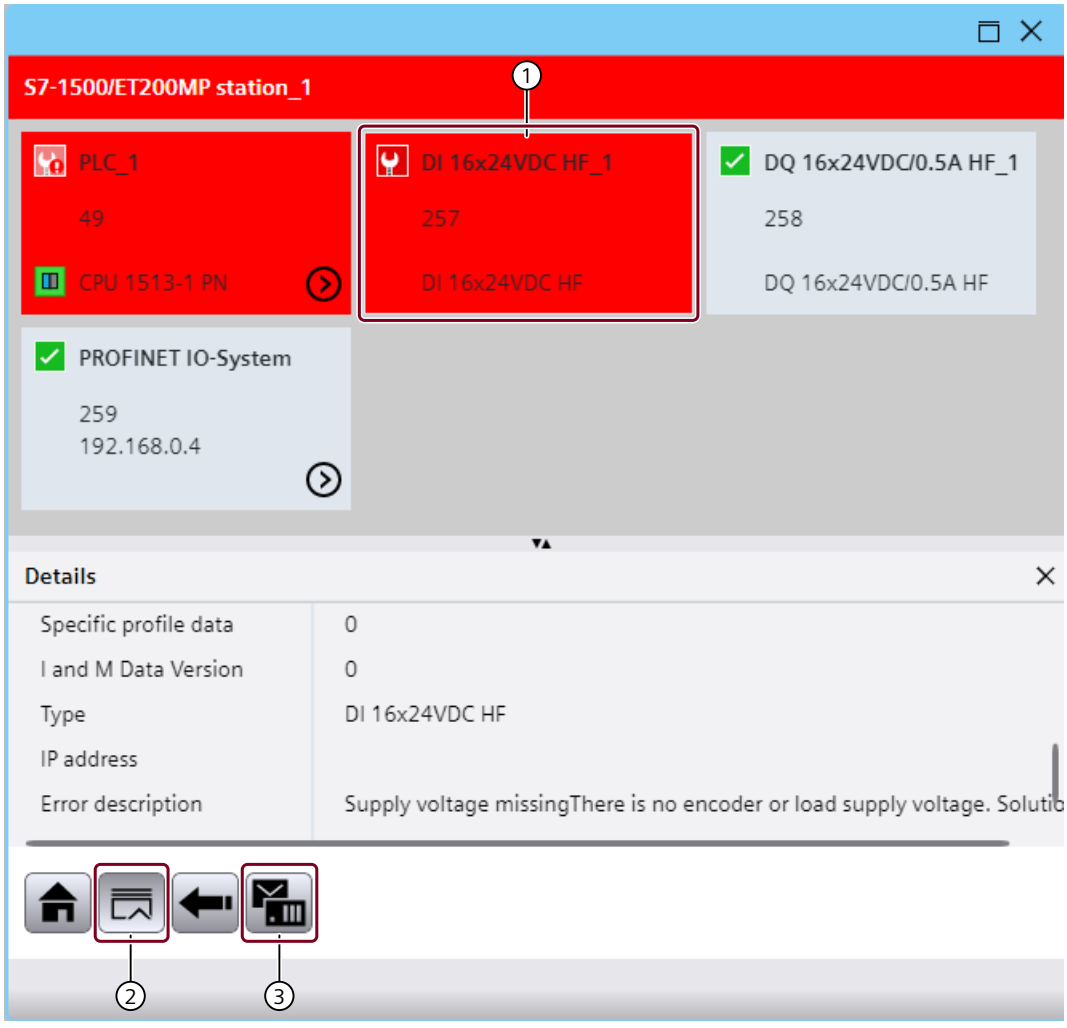
Status	Diagnostic value	Color
Indeterminate	0	Gray
Good	1	Green
Maintenance	2	Yellow
Error	3	Red

Configuring the system diagnostics view

You configure the system diagnostics view in WinCC Unified in the same way as in WinCC.

However, while system diagnostics in WinCC shows each view in table form, WinCC Unified has a matrix view. In the matrix view, you see an overview of your devices and the associated details view in the same window during runtime.

The matrix view shows stations and devices as tiles. When you click on a tile of a device, the lower part of the view shows detailed information about the device. To show detailed information about the higher-level station, click the "Enable/disable details view" button.



① Tile of a faulty device
② "Enable/disable details view" button
③ "Show diagnostics buffer" button

Figure 3-48 Matrix view during runtime

NOTE

System diagnostics in WinCC Unified for S7-1500R/H systems

For S7-1500R/H systems, system diagnostics in WinCC Unified is available as of TIA Portal V20.

In the matrix view, you can switch to the diagnostics view with the "Show diagnostics buffer" button.

The diagnostics view shows the diagnostics buffer with the diagnostic events of the selected CPU. In WinCC Unified, unlike in WinCC, the diagnostic alarms are loaded from the diagnostics buffer of the selected CPU and displayed during runtime. Errors in the diagnostics view due to non-updated text lists on the HMI devices are prevented in this way.

When you click on the "Enable/disable details view" button, the lower part of the diagnostics view shows detailed information about the selected event.

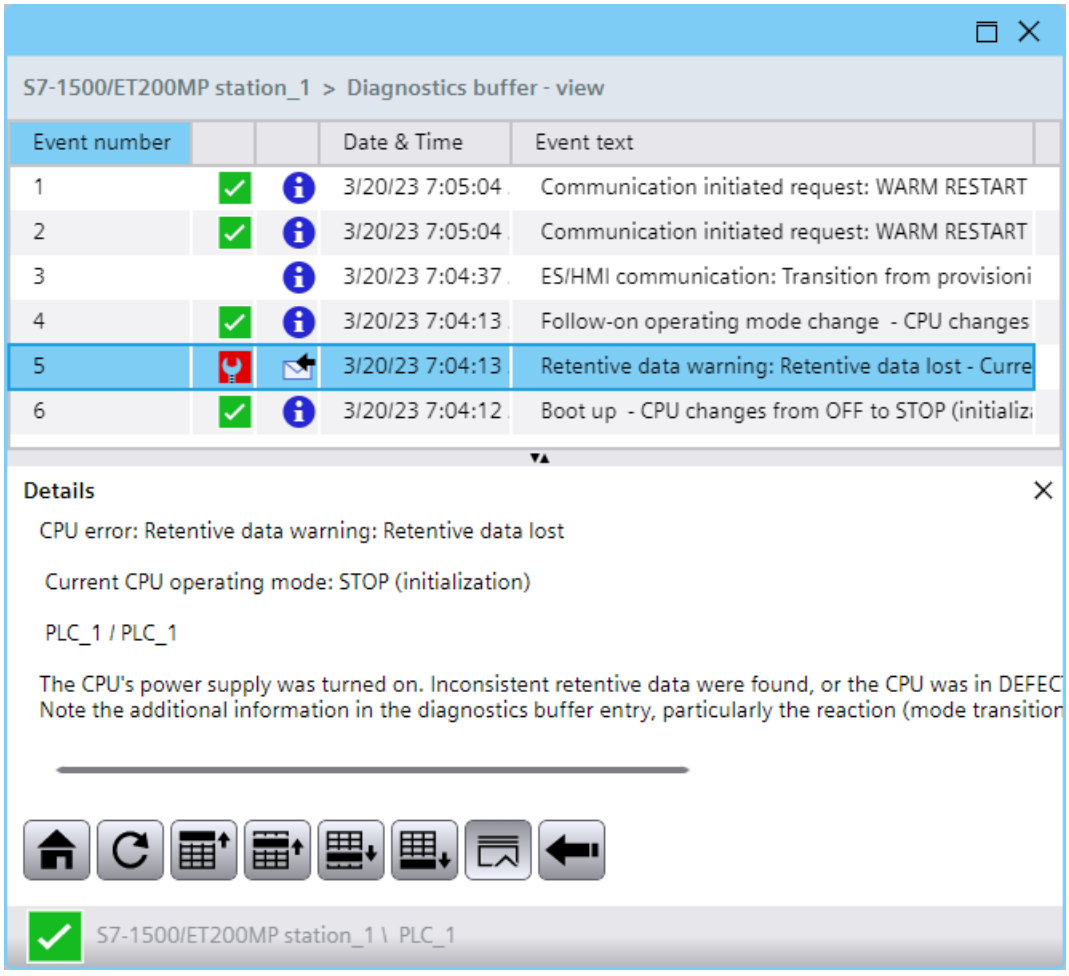


Figure 3-49 Diagnostics buffer view

In the Runtime settings, you can select the languages you need for your display. A CPU supports three languages that you configure in the engineering. If the Runtime language and the configured language of the CPU do not match, the diagnostic alarms are displayed in the configured substitute language of the CPU.

More information

You can find detailed information and procedures for visualization in the TIA Portal online help under "Visualizing processes (RT Unified)> Using diagnostics functions".

System diagnostics by means of the user program 6

6.1 Options of system diagnostics in the user program

Introduction

You can configure responses to diagnostics alarms in the user program. You can, for example, specify that your plant is stopped in case of specific diagnostics alarms.

Instructions

A vendor-independent structure of data records with diagnostics information applies. The following instructions are available for determining the system diagnostics of a device:

Table 3-8 Instructions for determining the system diagnostics

Instruction	Description
RDREC	• Reads data records of a component (module or submodule) of a DP slave/IO device that may contain error information • Works asynchronously, which means processing takes place across several calls
DPNRM_DG	• Reads the current diagnostics data of a DP slave (DP standard diagnostics) • Works asynchronously, which means processing takes place across several calls
T_DIAG	• Provides diagnostic and status information on a connection • Works asynchronously, which means processing takes place across several calls
Get_IM_Data	• Reads the identification and maintenance data of the CPU • Works asynchronously, which means processing takes place across several calls
GetStationInfo	• Reads address information of a PROFINET IO device • IO device may also be located in a lower-level IO system (connection via CP/CM) (except in S7-1500R/H systems). • Works asynchronously, which means processing takes place across several calls
GetChecksum	• Reads the checksum of a group of objects • Works asynchronously, which means processing takes place across several calls
GetSMCinfo	• Reads information about the inserted SIMATIC Memory Card • Works asynchronously, which means processing takes place across several calls
RALRM	• Reads the start information of the OB when calling the diagnostics interrupt OB (OB 82) • Provides information on cause and location of error
GEN_DIAG	• Generates diagnostics information • To generate diagnostics information, the module or submodule is identified with its logical address
Gen_UsrMsg	• Generates an alarm that is entered in the diagnostics buffer
GET_DIAG	• Provides diagnostics information • To provide diagnostics information, the module or submodule is selected
GET_Name	• Reads the name of an IO device
RD_SINFO	• Reads the start information of the OB called last that has not been processed completely and the startup OB started last • Provides general error information
LED	• Reads the status of the module LED
DeviceStates	• Outputs the state of all devices of an IO system

Instruction	Description
ModuleStates	• Outputs the state of all modules of a device
RT_INFO	• Provides statistics on the runtime of certain organization blocks of the communication or the user program
GetClockStatus	• Reads information about the internal CPU clock

Additional information

Online help
In the online help for STEP 7, you can find:

- Additional information on instructions for system diagnostics
- Information about further options for evaluating diagnostic information in the user program (e.g. with the "RDREC", "RALRM", "GET_DIAG" instructions)
- Information on SIMATIC ProDiag. This functionality enables targeted and fast machine and plant diagnostics for SIMATIC S7-1500 and SIMATIC HMI:
  - Standardized diagnostics concept for different SIMATIC components
  - No additional configuration work for diagnostics functionality
  - Reduces the load on PLC memory and program run time

  You can find details in the online help under "Supervising machinery and plants with ProDiag".

Manuals
You can find additional information about evaluating diagnostic information in the user program in the following manuals:

- PROFINET function manual (http://support.automation.siemens.com/WW/view/en/49948856)
- From PROFIBUS DP to PROFINET IO (https://support.industry.siemens.com/cs/ww/en/view/19289930) programming manual
- Manual for the respective module

Application examples
You can find detailed application examples with further documentation and example projects on the Service&Support Website:

- Diagnostic overview for SIMATIC S7-1200 and S7-1500 (https://support.industry.siemens.com/cs/ww/en/view/109752283)

FAQ
For more information about how to realize channel diagnostics in the user program of the SIMATIC S7-1500, refer to the FAQ with entry ID 109480387 on the Service&Support Website (https://support.industry.siemens.com/cs/ww/en/view/109480387).

6.2 System diagnostics using process image inputs

Introduction

In addition to event-driven system diagnostics, the input and output modules of the SIMATIC series provide diagnostics information using the process image input.

The system diagnostics described in the preceding sections is made available asynchronously to the program processing. To ensure the correct processing of the input and output data in the case of faults while reading the input and output data, some modules offer the so-called value status (QI = Quality Information) for evaluation.

Requirement for evaluation of the value status

The diagnostics information about the process image input is transmitted synchronized with the user data. Select the "Value status" check box in the properties of the I/O module in STEP 7 if you want to evaluate the value status of the channel.

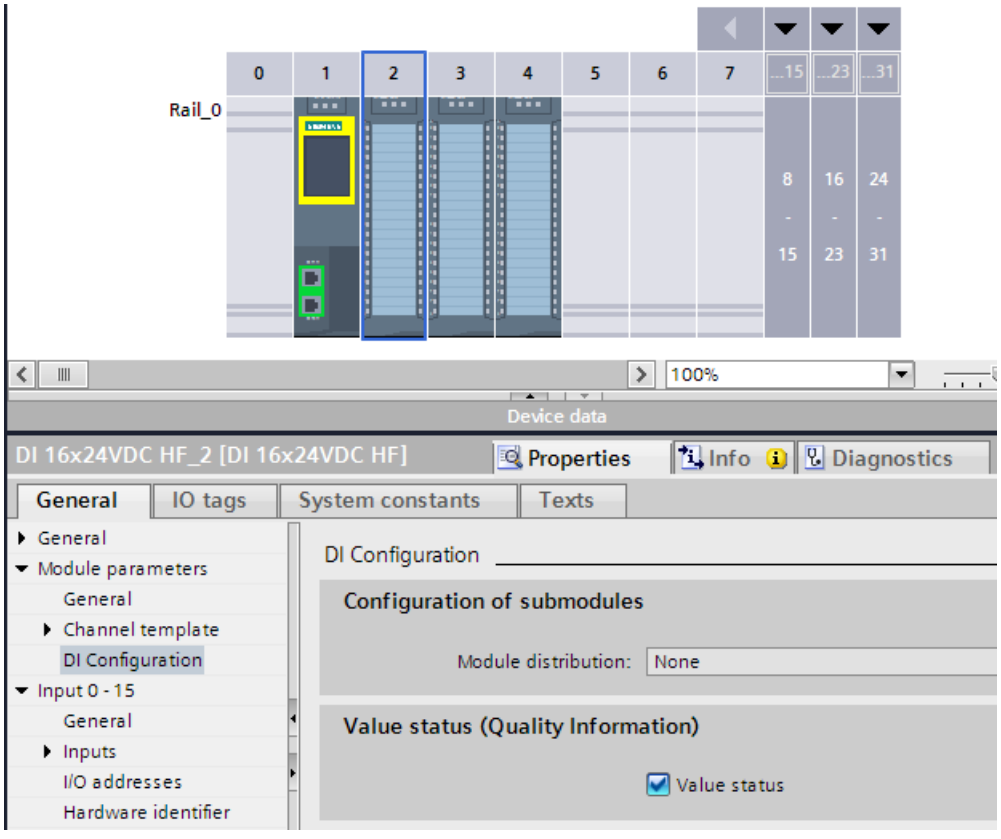


Figure 3-50 Enable value status

Evaluation of the value status

If you have enabled the value status for an I/O module, this module provides additional information on the value status in addition to the user data. This information is available directly in the process image input and can be retrieved with simple binary operations without having the evaluate the module diagnostics. Configured diagnostics in STEP 7 is not necessary for output of the value status.

Each channel is uniquely assigned one bit in the value status. The bit in the value status indicates the validity of the read-in value in the user data.

Table 3-9 Example for evaluation of the user datum in case of a wire break for a digital input module

	Bit in user datum	Bit in value status	Value in user datum
Faulty channel	Logical 0	0	Invalid
Fault-free channel	Logical 0 (actual value)	1	Valid

Influence of the value status

The value status of an active channel is "Invalid" when any **one** of the following factors is given:

- Channel diagnostics pending (regardless of whether diagnostics, for example wire break, is configured for this channel)
- For output channels: "Reaction to CPU STOP" feature is active (due to CPU STOP, interrupted connection)
- For output channels of the digital on-board I/O of compact CPUs: If a channel is used for technology functions, it returns the value status 0 ("Invalid"). It does not matter in this context whether the output value is incorrect or not.
- PROFIenergy is active, i.e. hibernation is enabled (except in "Continue working mode")

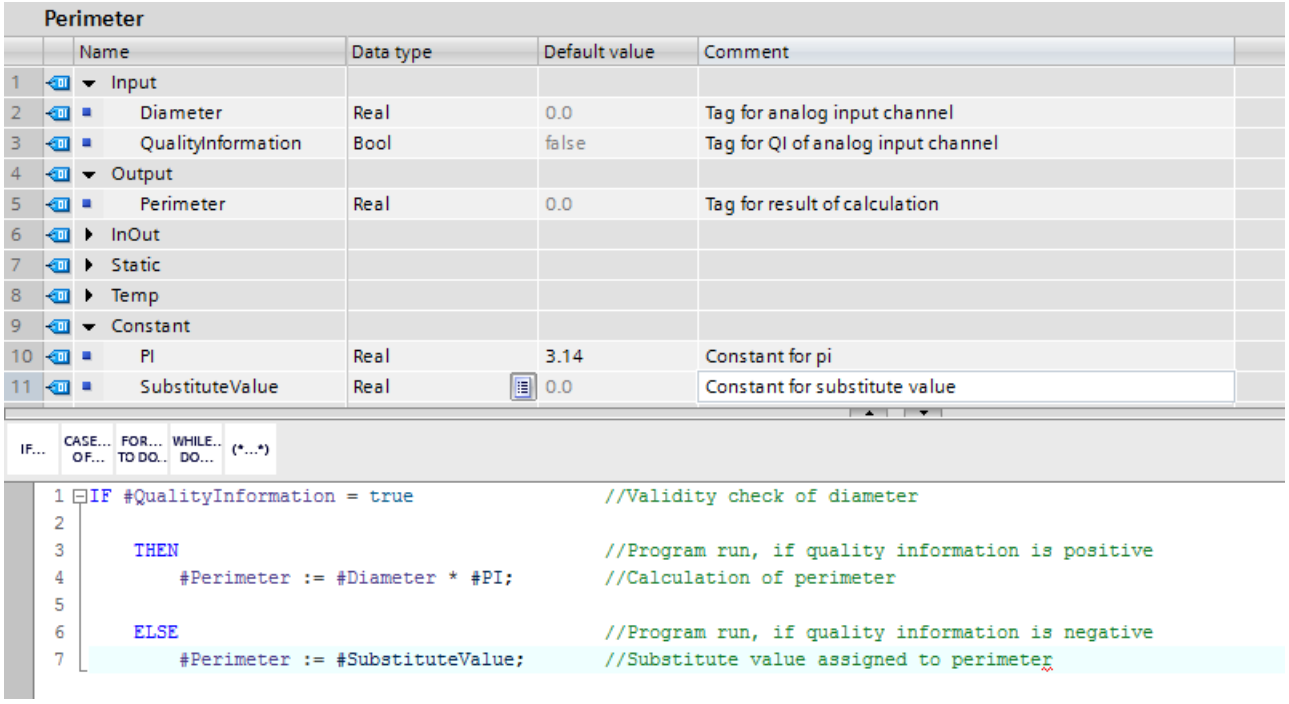
When working with non-fail-safe modules, note that an invalid active channel also sets the value status of all other active channels to "Invalid". We therefore recommend that you disable all unconnected or unused channels.

Example - Evaluation of the value status for the input channel of an analog input module

The example below shows the basic evaluation of the value status for the input channel of an analog input module in the user program. The diameter of a cylinder is measured by means of a channel and its circumference is calculated.

- If the value status indicates the channel is error-free, the circumference is to be calculated.
- If the value status indicates the channel is defective, the value "0" is to be output as substitute value for the circumference.

The figure below shows the evaluation of the value status in the user program.



Perimeter

	Name	Data type	Default value	Comment
1	Input			
2	Diameter	Real	0.0	Tag for analog input channel
3	QualityInformation	Bool	false	Tag for QI of analog input channel
4	Output			
5	Perimeter	Real	0.0	Tag for result of calculation
6	InOut			
7	Static			
8	Temp			
9	Constant			
10	PI	Real	3.14	Constant for pi
11	SubstituteValue	Real	0.0	Constant for substitute value

IF... CASE... OF... FOR... TO DO... WHILE... DO... (*...*)

```
1 IF #QualityInformation = true                //Validity check of diameter
2
3     THEN                                     //Program run, if quality information is positive
4         #Perimeter := #Diameter * #PI;       //Calculation of perimeter
5
6     ELSE                                     //Program run, if quality information is negative
7         #Perimeter := #SubstituteValue;      //Substitute value assigned to perimeter
```

Figure 3-51 Example - Evaluation of the value status in the user program

Additional information

Depending on the I/O module, the value status reserves different addresses in the process image input. The manual for the module used includes specific information on the assignment and arrangement.

Alarms

7

Introduction

Alarms allow you to display events from processing in the automation system and to quickly detect errors, to precisely localize them and to remove them. Downtimes are significantly reduced in a plant.

Before alarms can be output, they need to be configured.

You can create, edit and compile event-dependent alarms along with their alarm texts and alarm attributes and display them on display devices.

In STEP 7, you create program alarms in the user program with the "Program_Alarm" instruction. You edit the attributes and alarm texts in the alarm editor in STEP 7.

You can output the alarm status with the "Get_AlarmState" instruction.

Advantages of program alarms

Compared to other alarm methods, such as HMI discrete alarms, program alarms offer the following advantages:

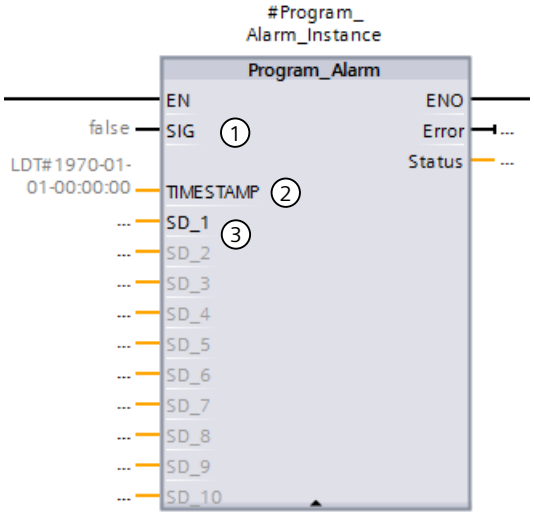
- Central engineering in STEP 7: You only configure a program alarm once for the CPU. The program alarm is automatically transferred from the CPU to all registered HMI devices.
- System-supported acknowledgment: The acknowledgment of a program alarm on an HMI device is automatically updated on other HMI devices by the CPU.
- Time stamping close to the event in the CPU
- Identical time stamps of the alarms on multiple HMI devices without time synchronization

7.1 Creating alarms with the "Program_Alarm" instruction

"Program_Alarm" instruction

You create a program alarm in STEP 7 with the "Program_Alarm" instruction.

The figure below shows the "Program_Alarm" instruction with the most important input tags.



① The "Program_Alarm" instruction monitors the signal at the SIG block input and generates a program alarm in case of a signal change at the SIG parameter. The instruction generates an incoming alarm when the signal changes from 0 to 1 and an outgoing program alarm if the signal changes from 1 to 0. The program alarm is triggered synchronously to program execution.

② The time stamp is automatically created when the alarm event occurs in the automation system and is passed along with the alarm.

③ You can append up to ten associated values to the program alarm at the parameters SD_i (1 ≤ i ≤10). The associated values are acquired at the time of the signal change at the SIG parameter and assigned to the program alarm.
Associated values are used to display dynamic contents in alarms.
Example: The temperature in the tank <associated value 1> is <associated value 2> °C.
You can find more information on associated values in the STEP 7 online help.

Figure 3-52 "Program_Alarm" instruction

NOTE

The "Program_Alarm" instruction can only be called in a function block.

A program alarm can be up to 256 bytes long in total (with associated values and texts from the text list).

The associated values can be a maximum of 512 bytes in length. Text lists are not affected by this.

The CPUs of the SIMATIC S7-1500 product series have the following memory for text lists:

- CPU 1510-x to CPU 1513-x: 4.5 MB
- CPU 1515-x to CPU 1516-x: 6.5 MB
- CPU 1517-x to CPU 1518-x: 50 MB

The number of configurable program alarms depends on the CPU used. With a CPU 1515-2 PN, for example, a maximum of 10,000 program alarms are possible. You can find this information in the Equipment Manual for the respective CPU under "Number of configurable alarms".

The number of simultaneously active "Program_Alarms" depends on the CPU used. With a CPU 1515-2 PN, for example, a maximum of 1,000 program alarms are possible. You can find this information in the Equipment Manual for the respective CPU under "Number of reserved user interrupts".

Sometimes, it is not possible for all program alarms that are active at the same time to be output within one cycle. Query the status of each "Program_Alarm" and activate the instruction again, if necessary. The cycle time is increased for a short time by simultaneously activating/sending multiple "Program_Alarms".

A maximum of 40,000 program alarms should be configured in a STEP 7 project on a 64-bit operating system.

More information

You can find more information on creating program alarms in the STEP 7 online help under "Creating and editing alarms".

7.2 Editing alarms in the alarm editor

Introduction

You can edit the created alarms in STEP 7 either in the program editor or in the alarm editor.

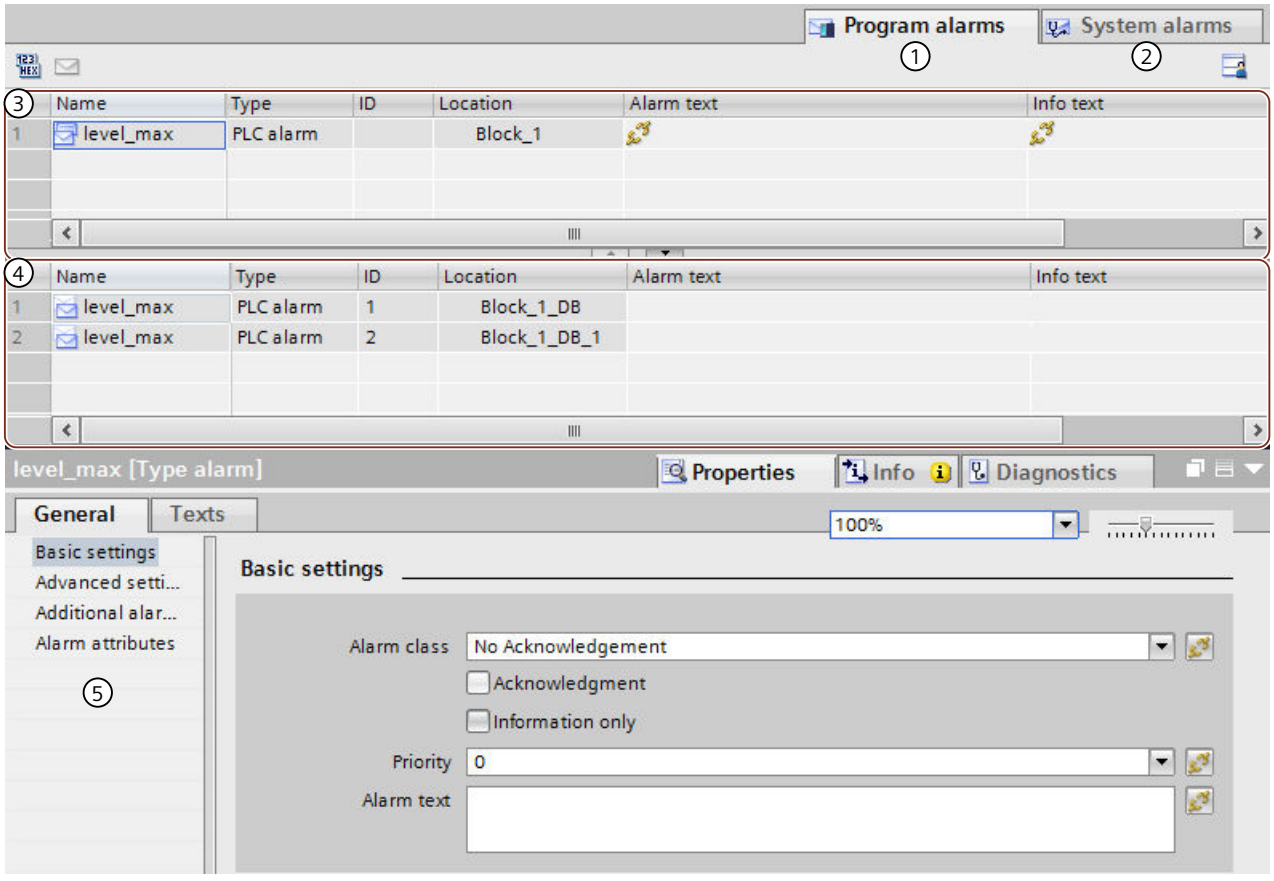
You can find additional information on editing alarms in the program editor in the STEP 7 online help under "Creating and editing alarms".

Editing alarms in the alarm editor

You can edit alarm texts in the alarm editor and specify attributes such as alarm class or priority for the alarms.

1. Double-click "PLC supervisions & alarms" in the project tree. Select the "Alarms" tab. The alarm editor opens.
2. Enter the required texts and attributes in the appropriate columns.

The figure below shows the layout of the alarm editor.



① "Program alarms" tab: You can edit program alarms here.

② "System alarms" tab: System alarms can only be viewed but not edited. To edit these alarms, you must navigate to the device view ("Go to device" menu command), where you can modify the system diagnostics alarms in the Inspector window.

③ "Type alarms" area:
This is where the type alarms created in a function block with the "Program_Alarm" instruction are displayed. Type alarms serves as templates for instance alarms (④).
All the inputs you make for the type alarm are automatically included in the instance alarms derived from it.
You can find more information on type alarms in the STEP 7 online help under "Alarm types and alarms".

④ "Instance alarms" area:
When you assign an instance DB to the message block (for example, call in an OB, FB, FC), instance alarms are automatically generated based on the template of the type alarm and alarm numbers are assigned.
You can modify the instance alarms for specific instances.
You can find more information on instance alarms in the STEP 7 online help under "Alarm types and alarms".

⑤ Properties of the selected type and instance alarm in the Inspector window

Figure 3-53 Layout of the alarm editor

You can enter or modify the necessary parameters, texts and attributes in the table or in the Inspector window.

Multilingual alarms

You can have program alarms displayed in multiple languages by assigning different project languages to the interface languages of the display devices.

NOTE

The project languages you want to assign must be activated and the corresponding texts (translations) must be available in the project. The project language selection can be found in the project tree under "Languages & Resources".

To create the texts of the program alarm as multilingual, follow these steps:

1. In the Inspector window of the alarm editor, open the "Properties" tab and the lower-level "Texts" tab.
2. Enter the text in the desired project language.
3. Open the "Properties" tab in the Inspector window of the CPU and select the "Display" command in the "General" area navigation. Under "Multilingual", assign one of the activated project languages to each interface language of the display devices. Overall, you can assign up to three different project languages to the user interface languages. All assigned project languages are loaded into the CPU.

More information

You can find additional information on texts and attributes in the STEP 7 online help under "Texts and attributes".

You can find more information on text lists in the STEP 7 online help under "Text lists for alarms".

7.3 Display of program alarms

Program alarms you create with the "Program_Alarm" instruction are automatically made available to the display devices.

You have the following options to display the alarms:

- STEP 7
- HMI
- Web server of the CPU
- Display of the CPU

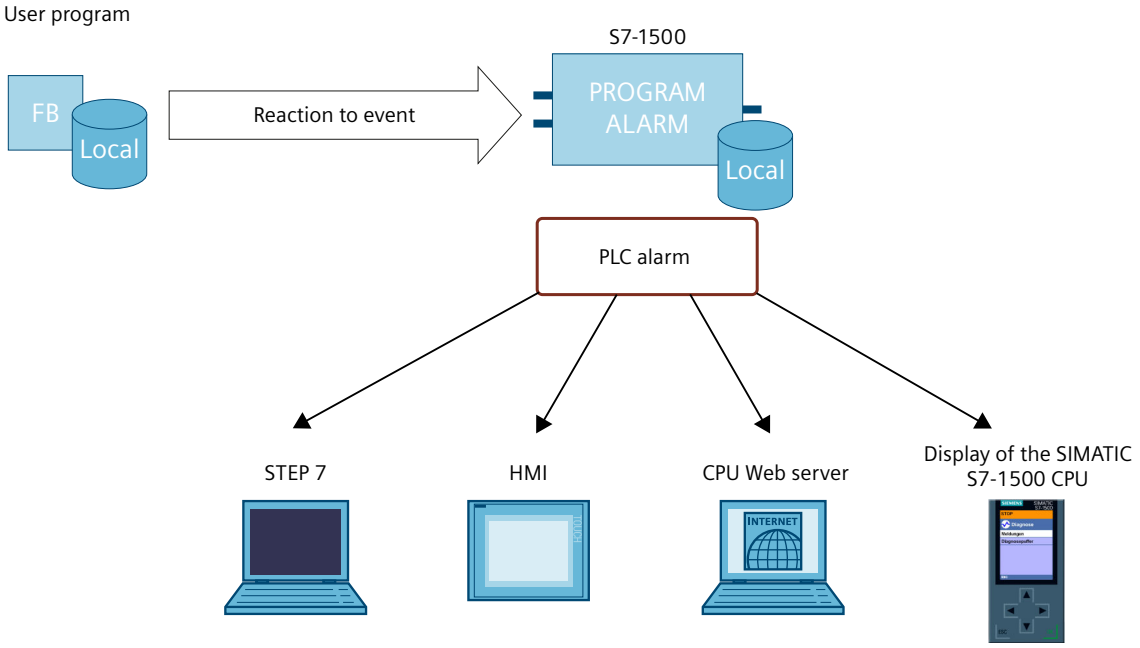


Figure 3-54 Display of program alarms

Multilingual alarms
You can have program alarms displayed in multiple languages by assigning different project languages to the interface languages. See section Editing alarms in the alarm editor (Page 82).

7.4 Output of the alarm state with the "Get_AlarmState" instruction

"Get_AlarmState" instruction

The "Get_AlarmState" instruction outputs the alarm state of a program alarm. The output of the alarm state always refers to a program alarm that was created using the "Program_Alarm" instruction.

The program alarm is selected with the "Alarm" input parameter. Specify the instance DB of the "Program_Alarm" instruction at the "Alarm" parameter.

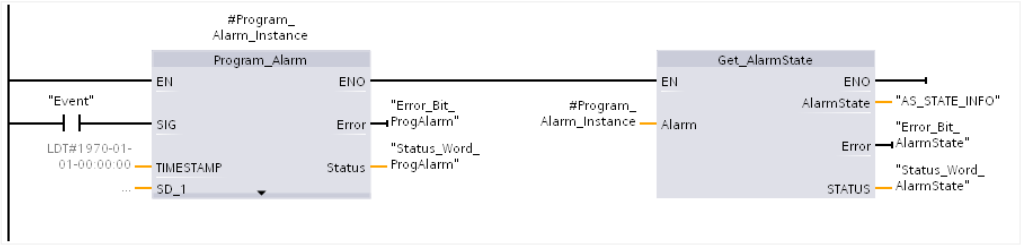


Figure 3-55 Call - Get_AlarmState

Additional information

You can find additional information on evaluation of the "Get_AlarmState" instruction in the STEP 7 online help.

7.5 Example program for program alarms

7.5.1 Task

Introduction

This section describes the basic configuration of program alarms with the "Program_Alarm" instruction based on two examples. The two examples solve the same problem but use a different approach. Example 1 does not use associated values. In example 2, an associated value is assigned to the program alarm to reference a text list.

Example - Minimum/maximum fill level of a tank

A tank is filled with a liquid. The fill level is monitored by two sensors.

If the liquid in the tank drops below a minimum fill level, an alarm is output for low fill level.

If the liquid in the tank exceeds a maximum fill level, an alarm is output for high fill level.

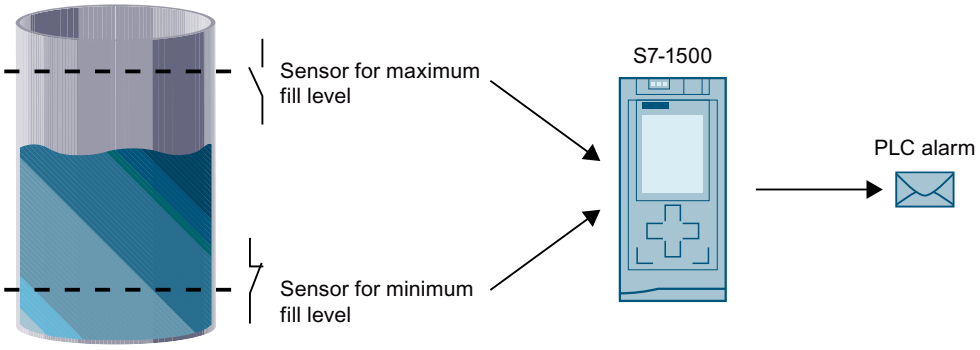


Figure 3-56 Example for fill level alarms

7.5.2 Example 1: Program alarm without associated values

Introduction

In this example, you create a program alarm for the maximum and the minimum fill level.

How the example works

When the maximum fill level is exceeded in the tank, a program alarm with the alarm text for the excessive fill level is output.

When the minimum fill level is undershot in the tank, a program alarm with the alarm text indicating that the fill level is too low is output.

Steps

The following steps are necessary for this example:

1. Define tags for signal acquisition
2. Create function block
3. Create program alarms
4. Call function block
5. Edit alarm text

Define tags for signal acquisition

The following table shows the tags that are used in this example. Define these tags in the standard tag table. The standard tag table is available in the project tree under "PLC tags".

Table 3-10 Tags for fill level alarms

Name	Data type	Description
max	BOOL	Tag for maximum fill level If "max" = 1, the maximum fill level is exceeded.
min	BOOL	Tag for minimum fill level If "min" = 1, the minimum fill level is undershot.

The figure below shows the standard tag table with the defined tags "max" and "min".

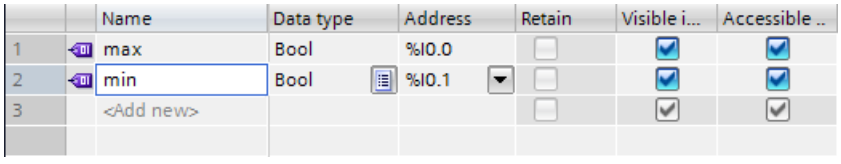


Figure 3-57 Define tags

Create function block

To create a function block, follow these steps:

1. Open the "Program blocks" folder in the project tree.
2. Double-click "Add new block".
   The "Add new block" dialog opens.
3. Select the button "Function block".

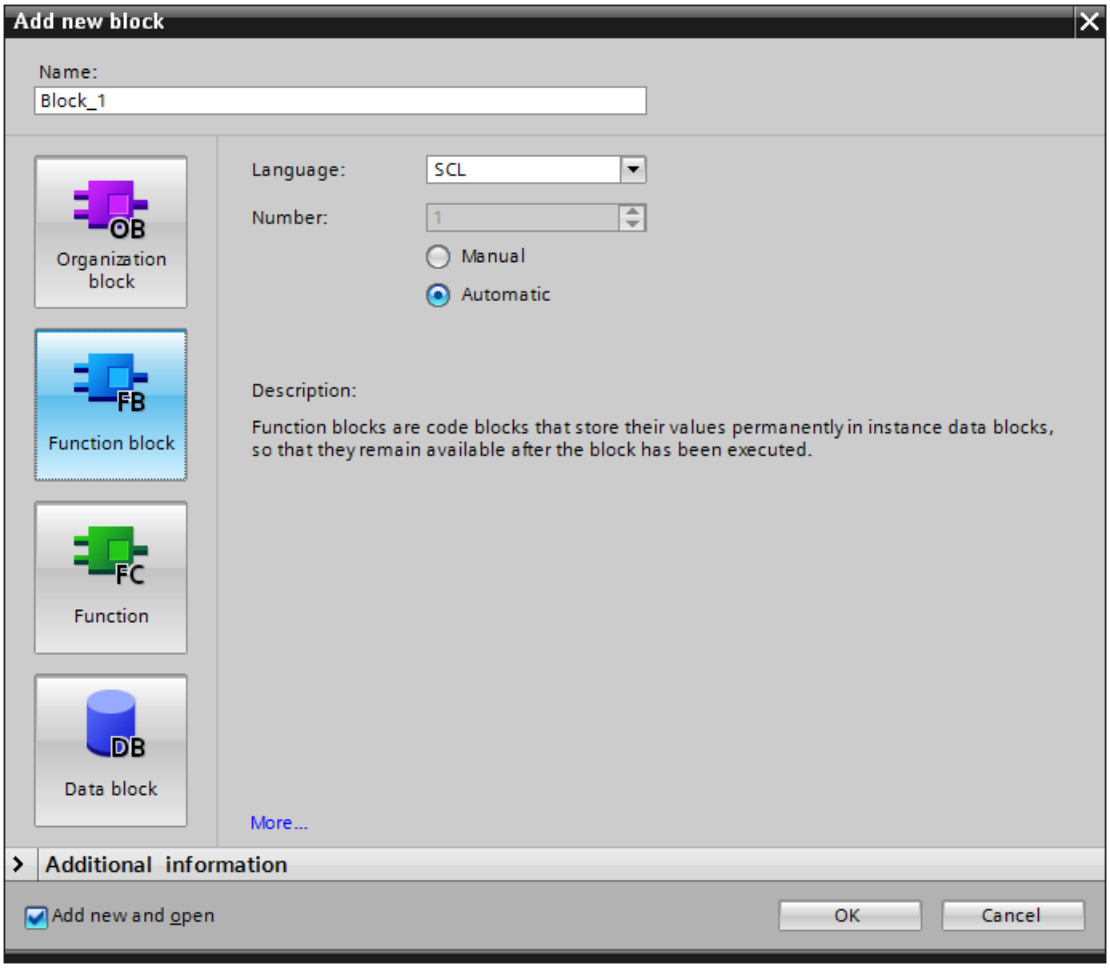


Figure 3-58 Create FB

4. Enter a name for the new block.
5. Select the language SCL.
6. Click on "OK" to confirm your input.

Result: You have created a function block.

Create program alarms

To create the program alarm for the example program, follow these steps:

1. Select the created function block (FB) in the "Program blocks" folder in the project tree and double-click the function block to open it.
2. Insert the call of the "Program_Alarm" instruction in the instruction part of the function block. The "Program_Alarm" instruction is available in the "Instructions" task card under "Extended instructions" > "Alarms".

   The "Call options" window opens.

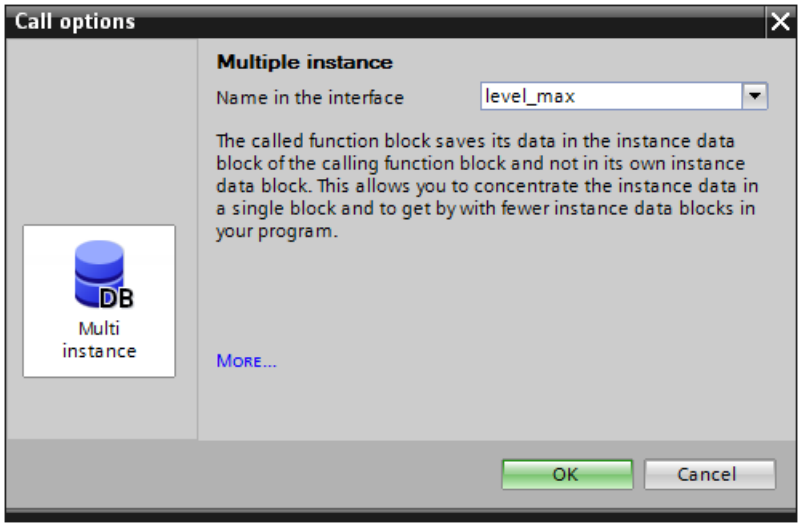


Figure 3-59 Call Program_Alarm

3. Enter "level_max" as the name and confirm the call options by clicking "OK".

   Result: The input tags of the "Program_Alarm" instruction are displayed in the instruction part.
4. Supply the SIG input tag of the "Program_Alarm" instruction with the tags for the maximum fill level.
   `#level_max(SIG:="max");`
   SIG: If a signal change occurs at the SIG input tag, the "Program_Alarm" instruction generates a program alarm.
5. Insert another call of the "Program_Alarm" instruction.
   The "Call options" window opens.
6. Enter "level_min" as the name and confirm the call options by clicking "OK".

   Result: The input tags of the "Program_Alarm" instruction are displayed in the instruction part.
7. Supply the SIG input tag of the "Program_Alarm" instruction with the tags for the minimum fill level.
   `#level_min(SIG:="min");`

Result: You have created two type alarms.

Call function block

To call the function block in the user program, follow these steps:

1. In the "Program blocks" folder, select the cycle OB (e.g., OB1) in which you want to call the function block and open the cycle OB with a double-click.
2. Select the function block you want to call in the "Program blocks" folder.
3. Drag the function block into the instruction part of the cycle OB.
   The "Call options" window opens.

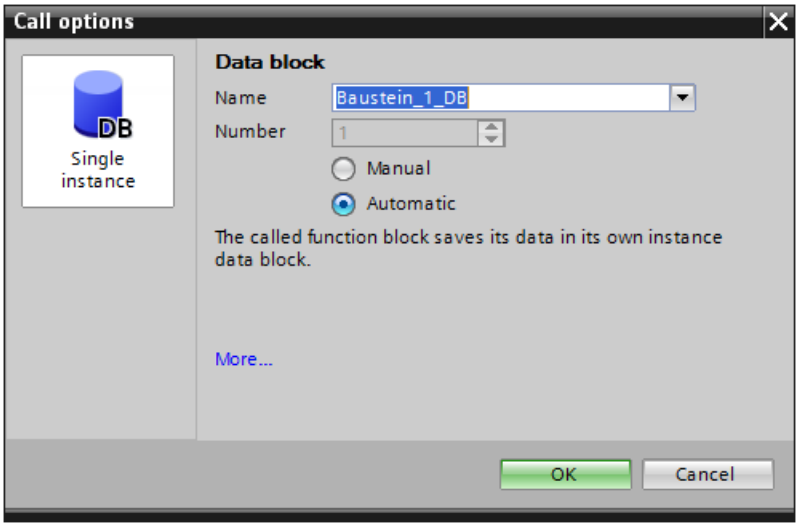


Figure 3-60 Call function block

4. Confirm the call options by clicking "OK".

Result: You have called the alarm block in the user program and created an instance alarm.

Edit alarm text

To edit the alarm text, follow these steps:

1. Double-click "PLC supervisions & alarms" in the project tree. Select the "Alarms" tab. The alarm editor opens.
2. Select the type alarm for the maximum fill level.
3. Enter the alarm text for the maximum fill level in the "Alarm text" column.
4. Select the type alarm for the minimum fill level.
5. Enter the alarm text for the minimum fill level in the "Alarm text" column.

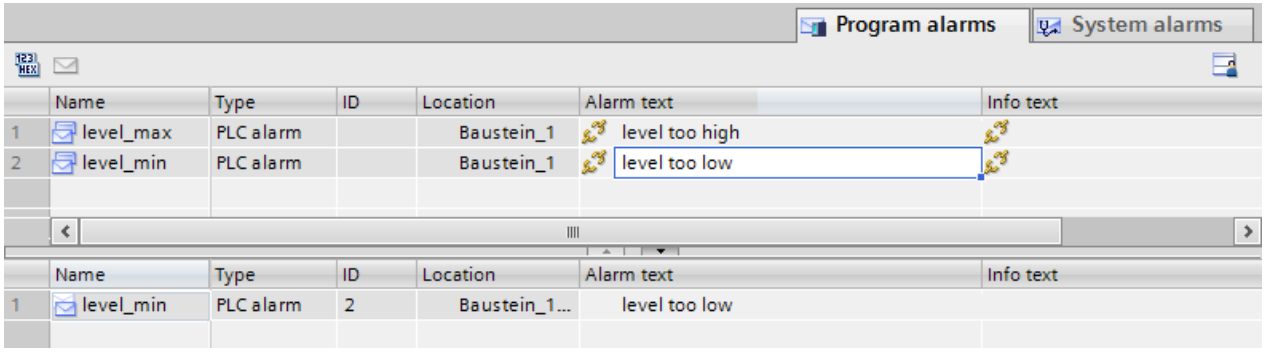


Figure 3-61 Edit alarm text

Result: You have created the alarm texts for both type alarms.

Additional information

You can learn how to create multilingual texts under "Multilingual alarms" in the section Editing alarms in the alarm editor (Page 82).

7.5.3 Example 2: Program alarm with associated value

Introduction

In this example, you create a shared program alarm for the maximum and the minimum fill level. The program alarm is given an associated value. The program alarm uses the associated value to access a text list entry and outputs a separate alarm text for the minimum and the maximum fill level.

How the example works

The program alarm is output if either the minimum fill level is undershot or the maximum fill level is exceeded.

The associated value 1 of the "Program_Alarm" instruction is assigned the tag for the maximum fill level. The associated value references a text list with the entries "0" and "1".

The following scenarios are possible for output of the alarm text:

- Associated value is "0": The entry "0" of the text list with the alarm text for the undershot fill level is output.
- Associated value is "1": The entry "1" of the text list with the alarm text for the excessive fill level is output.

Steps

The following steps are necessary for this example:

1. Define tags for signal acquisition
2. Create function block
3. Create program alarm
4. Call function block
5. Create a text list
6. Edit alarm text

Define tags for signal acquisition

The following table shows the tags that are used in this example. Define these tags in the standard tag table. The standard tag table is available in the project tree under "PLC tags".

Table 3-11 Tags for fill level alarms

Name	Data type	Description
max	BOOL	Tag for maximum fill level If "max" = 1, the maximum fill level is exceeded.
min	BOOL	Tag for minimum fill level If "min" = 1, the minimum fill level is undershot.

The figure below shows the standard tag table with the defined tags "max" and "min".

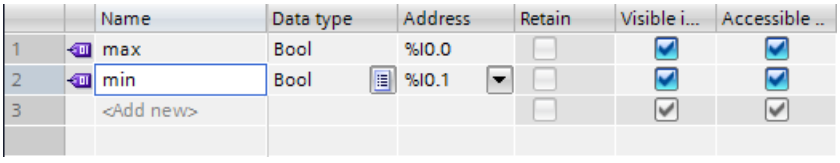


Figure 3-62 Define tags

Create function block

To create a function block, follow these steps:

1. Open the "Program blocks" folder in the project tree.
2. Double-click "Add new block".
   The "Add new block" dialog opens.

3. Select the button "Function block".

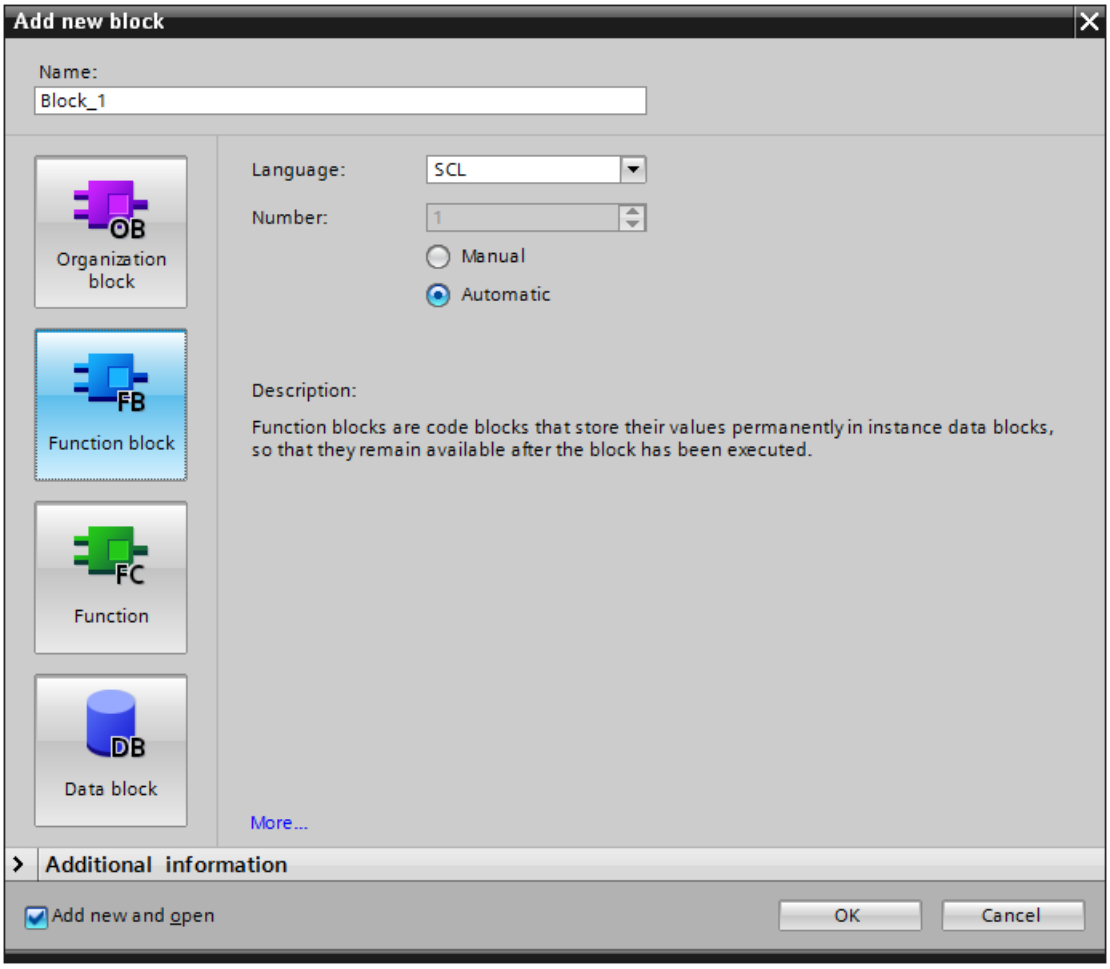


Figure 3-63 Create FB

4. Enter a name for the new block.
5. Select the language SCL.
6. Click on "OK" to confirm your input.

Result: You have created a function block.

Create program alarm

To create the program alarm for the example program, follow these steps:

1. Select the created function block (FB) in the "Program blocks" folder in the project tree.
2. Insert the call of the "Program_Alarm" instruction in the instruction part of the function block. The "Program_Alarm" instruction is available in the "Instructions" task card under "Extended instructions" > "Alarms".
   The "Call options" window opens.

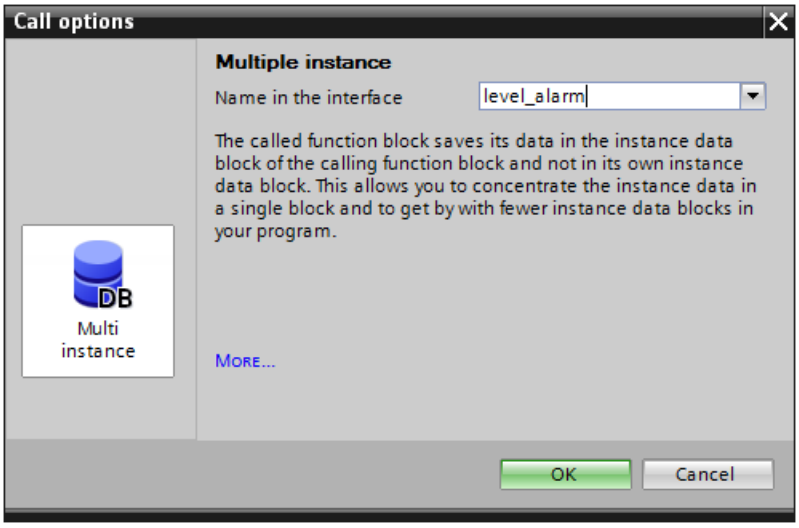


Figure 3-64 Call Program_Alarm

3. Enter "level_alarm" as the name and confirm the call options by clicking "OK".
   Result: The input tags of the "Program_Alarm" instruction are displayed in the instruction part.
4. Supply the SIG input tag of the "Program_Alarm" instruction with the XOR logic operation of the tags for minimum and maximum fill level and the input tag SD_1 with the tag for the maximum fill level.
   `#level_alarm(SIG:="min"XOR"max",SD_1:="max");`
   SIG: If a signal change occurs at the SIG input tag, the "Program_Alarm" instruction generates a program alarm.
   SD_1: The associated value is acquired at the time of the signal change at the input tag and assigned to the program alarm.

Result: You have created a type alarm.

Call function block

To call the function block in the user program, follow these steps:

1. In the "Program blocks" folder, select the cycle OB (e.g., OB1) in which you want to call the function block and open the cycle OB with a double-click.
2. Select the function block you want to call in the "Program blocks" folder.

3. Drag the function block into the instruction part of the cycle OB.
   The "Call options" window opens.

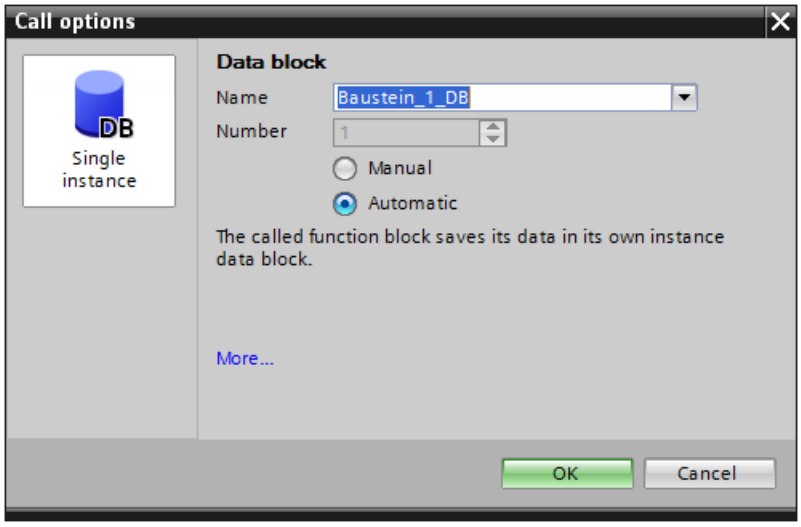


Figure 3-65 Call function block

4. Confirm the call options by clicking "OK".

Result: You have called the alarm block in the user program and created an instance alarm.

Creating a text list

To create the text list for the example program, follow these steps:

1. Double-click on the "Text lists" command in the program tree.
   The text list editor opens.
2. Double-click "<Add>" in the Text lists area.
   A new text list is added.
3. Name the text list "level_textlist".
4. Double-click "<Add>" in the Text list entries area of level_textlist.
   A new text list entry is added in the level_textlist text list.
5. Enter the alarm text for the maximum fill level in the "Entry" column.
6. Add another entry in the text list.
7. Enter the alarm text for the minimum fill level in the "Entry" column.

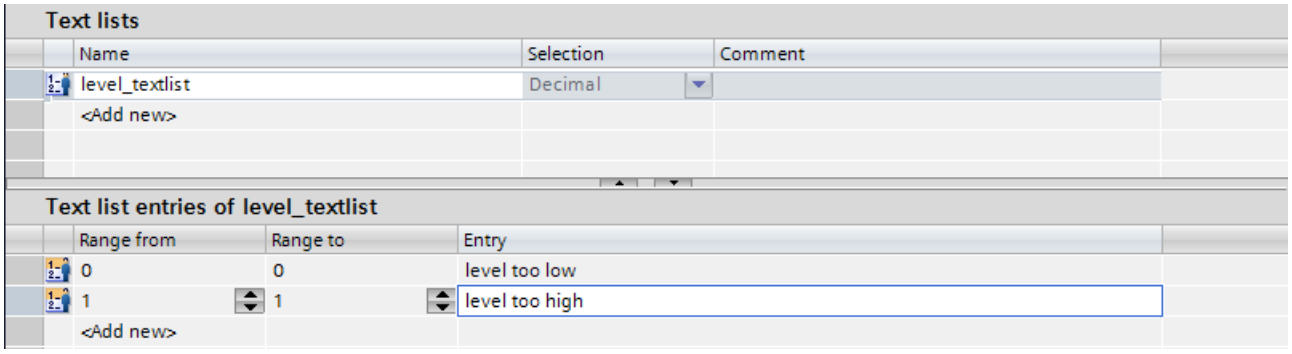


Figure 3-66 Creating a text list

Result: You have created the text list for the alarm text.

Edit alarm text

To edit the alarm text for the example program, follow these steps:

1. Double-click "PLC supervisions & alarms" in the project tree. Select the "Alarms" tab. The alarm editor opens.
2. Select the type alarm created for the example.
3. Click in the "Alarm text" column.
4. Open the shortcut menu and select the command "Insert a dynamic parameter (text list)".

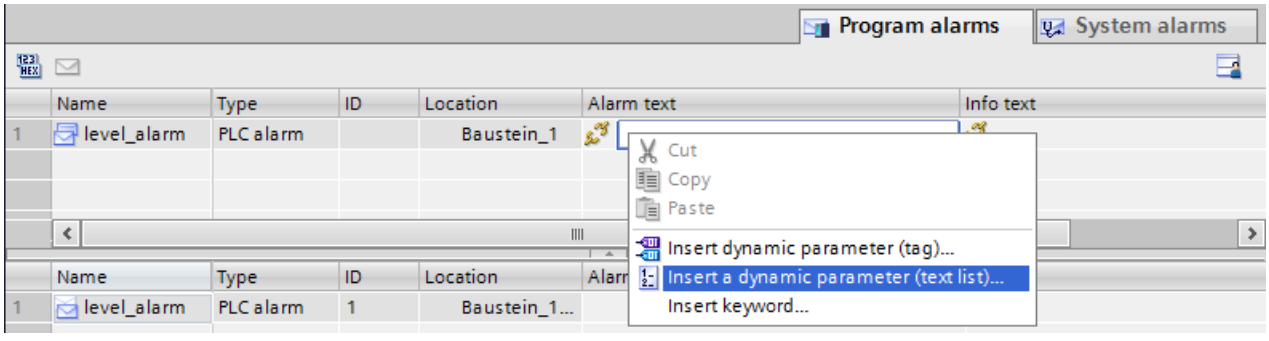


Figure 3-67 Edit alarm text

The window below opens.

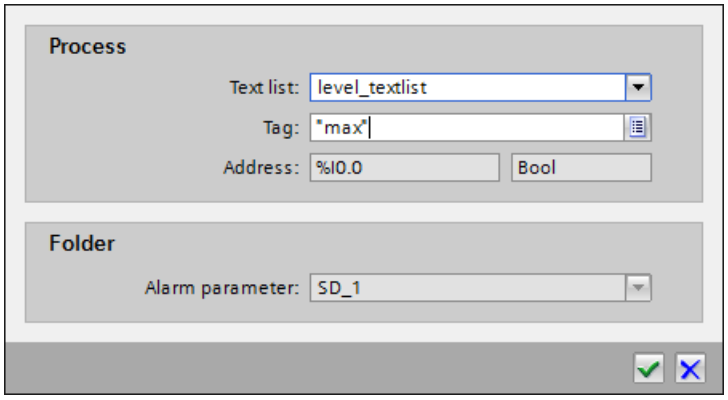


Figure 3-68 Insert a dynamic parameter (text list)

5. Select the text list "level_textlist" and the tag "max". Confirm your selection by clicking "OK".

Result: You have created the alarm text for the type alarms.
If the tag "max" (associated value 1) is 0, the alarm text "level too low" is output.
If the tag "max" (associated value 1) is 1, the alarm text "level too high" is output.

Additional information

You can learn how to create multilingual texts under "Multilingual alarms" in the section Editing alarms in the alarm editor (Page 82).

7.5.4 Displaying the alarm

Displaying the alarm in the Web server

The figure below shows the display of the alarm in the Web server for both examples.

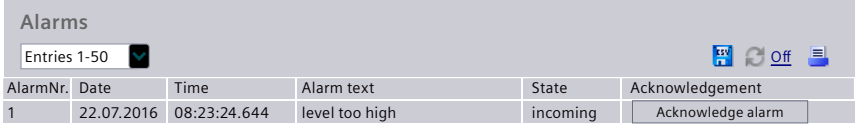


Figure 3-69 Displaying the alarm in the Web server

Displaying the alarm in STEP 7

NOTE

Displaying alarms in STEP 7
To display alarms in STEP 7, enable the option "Receive alarms" in the shortcut menu of the CPU.

The figure below shows the display of the alarm in STEP 7 for both examples.

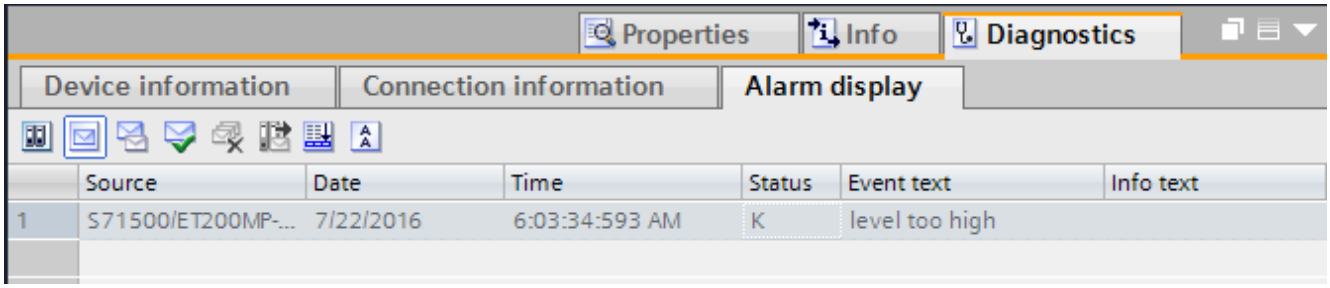


Figure 3-70 Display in STEP 7

Diagnostics of the S7-1500R/H redundant system 8

S7-1500R/H diagnostics

Diagnostics for a S7-1500R/H redundant system is basically the same as a standard S7-1500. You have the following display options:

- Via STEP 7
- Via HMI devices
- Via the display of the CPUs

The CPUs provide information about their operating states as well as internal and external errors through their LEDs.

The special features of the diagnostics of S7-1500R/H redundant systems are described below. In addition, the information of the current function manual and the STEP 7 online help also apply to S7-1500R/H redundant systems.

Diagnostics information in STEP 7

Hardware diagnostics can be performed as follows:

- Via the Online and Diagnostics view
- Via the "Online Tools" task card
- Via the "Diagnostics > Device Information" area of the Inspector window
- Via diagnostics icons, for example, in the device view and in the project tree

Diagnostics view in STEP 7 in dependence on the online connection and system states

The diagnostics view for S7-1500R/H redundant systems is partly dependent on:

- Which of the two CPUs the programming device / PC currently has a connection to
- The current system state in the redundant system

The table below provides an overview. The following sections illustrate the diagnostics view for S7-1500R/H using examples.

Table 3-12 Diagnostics view in dependence on the online connection and system states

Diagnostics view in STEP 7	An online connection is available to the	System state	Examples in section
Online data and diagnostics of the redundant system	Primary CPU or backup CPU	RUN-Redundant	Online and Diagnostics view (Page 100)
Online data and diagnostics of the primary CPU The following are not displayed: • Online data and diagnostics from the backup CPU	Primary CPU	RUN-Solo or STOP	Online and Diagnostics view (Page 100) and Restrictions in the RUN-Solo system state (Page 121)
Online data and diagnostics of the backup CPU The following are not displayed: • Online data and diagnostics from the primary CPU • Online data and diagnostics of the distributed I/O	Backup CPU	RUN-Solo or STOP	

Diagnostics view in STEP 7	An online connection is available to the	System state	Examples in section
Display of the 3 operator panels in the "Online Tools" task card	Primary CPU or backup CPU	Not relevant	"Online Tools" task card (Page 103)
Cycle time of the primary CPU (of the system) and memory of the primary CPU in "Online Tools" task card	Primary CPU or backup CPU	RUN-Redundant	
Cycle time and memory of the primary CPU in the "Online Tools" task card	Primary CPU	RUN-Solo or STOP	
Cycle time and memory of the backup CPU in the "Online Tools" task card	Backup CPU	RUN-Solo or STOP	
Memory reset of the primary CPU via "Online Tools" task card	Primary CPU	STOP	
Memory reset of the backup CPU via "Online Tools" task card	Backup CPU	RUN-Solo or STOP	
"Alarm display" tab: Alarms from the primary CPU	Primary CPU	Not relevant	Diagnostics view in the project tree and in the device view and network view (Page 106)
"Alarm display" tab: Alarms from the backup CPU	Backup CPU	Not relevant	
Diagnostics of the distributed I/O	Primary CPU or backup CPU	RUN-Redundant	Diagnostics in the RUN-Redundant system state (Page 115)
Diagnostics of the distributed I/O	Primary CPU	RUN-Solo	Restrictions in the RUN-Solo system state (Page 121)

Accessible devices

As for standard S7-1500 systems, the following can be displayed in STEP 7:

- All devices accessible from programming device/PC
- The diagnostics information of devices of a redundant system, for example, from the R/H CPUs

The procedure is described in the section Accessible devices (without project) (Page 34).

8.1 Online and Diagnostics view

Introduction

You open the Online and Diagnostics view for the redundant system or for each CPU of the redundant system.

Online & diagnostics for the redundant system

"Online access":
For the S7-1500R/H redundant system, it is displayed whether an online connection exists between the programming device/PC and a CPU. The additional note "Online (via Primary CPU)" or "Online (via Backup CPU)" indicates which role the "Online" connected CPU has.

If you enable "Receive alarms", you receive asynchronous alarms of diagnostics events from the CPU with online connection. The display corresponds to the representation for standard CPUs.

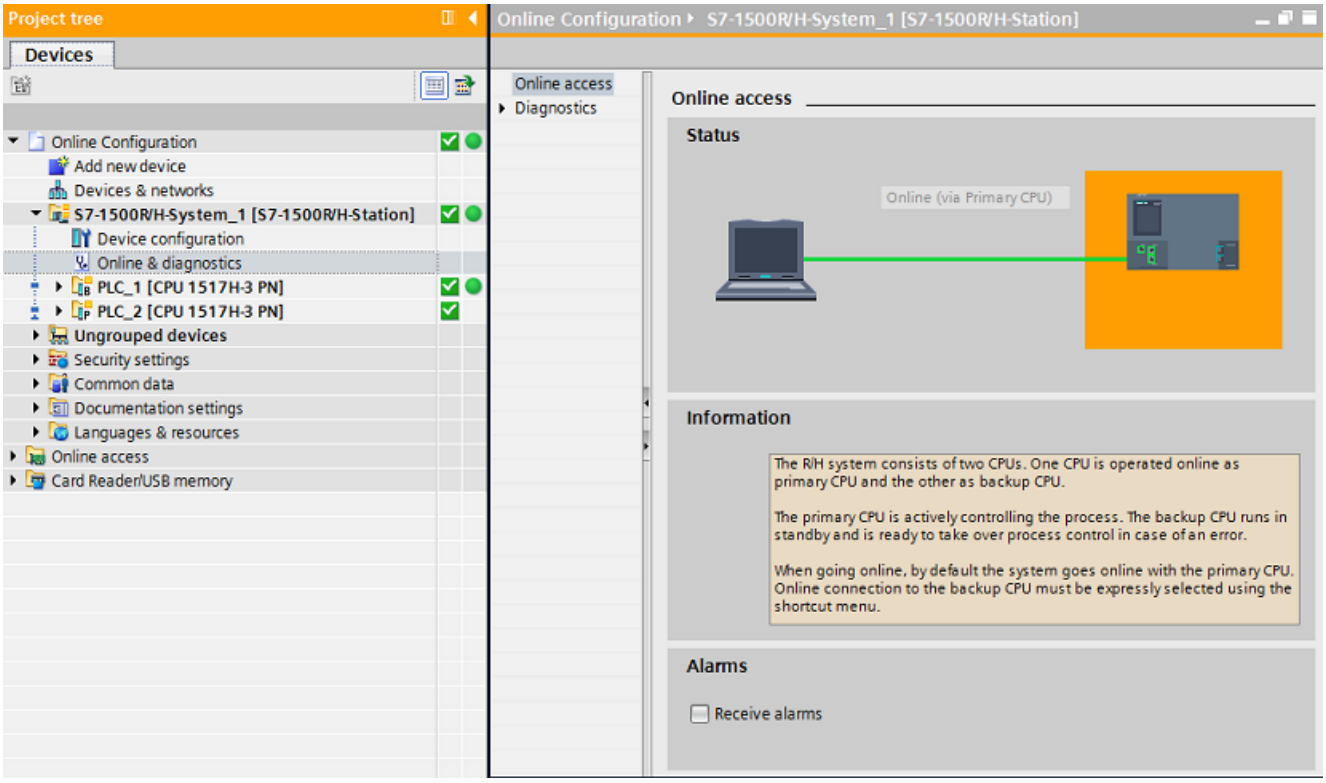


Figure 3-71 Online and Diagnostics view: Redundant system S7-1500R/H

"Diagnostics":
"Diagnostics" provides an overview for the redundant system about the:

- System state
- Pairing state
- Operating states of the CPU
- Status of which CPU is the primary CPU and which CPU is the backup CPU

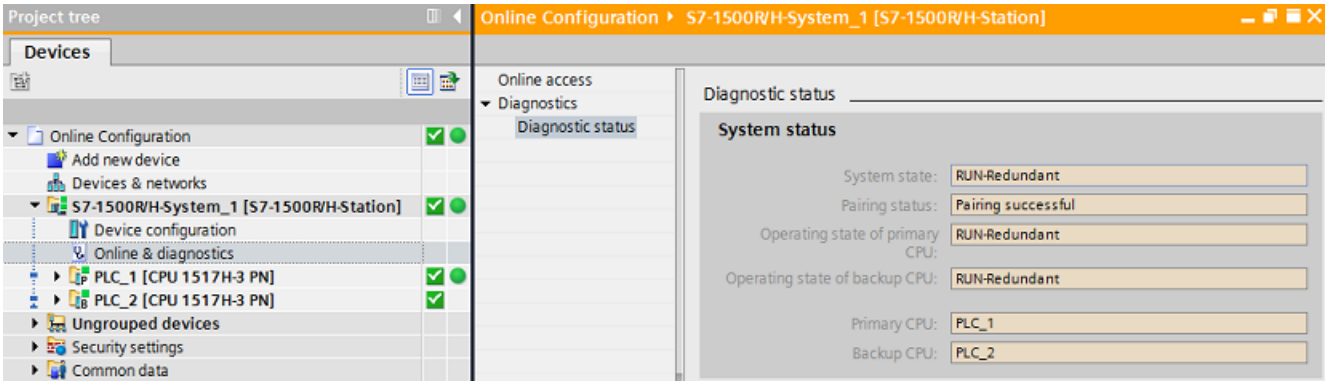


Figure 3-72 Online and Diagnostics view: Diagnostics status of the S7-1500R/H system

Online & diagnostics for the primary CPU or backup CPU

The Online and Diagnostics view for the CPUs of the redundant system match the display for standard CPUs.

In the RUN-Redundant system state, the primary and backup CPUs display the online data of the redundant system irrespective of which of the two CPUs has the online connection.

In non-redundant mode, the programming device/PC displays the data of the CPU that has an online connection.

You select the CPU for display of the online data in the project tree.

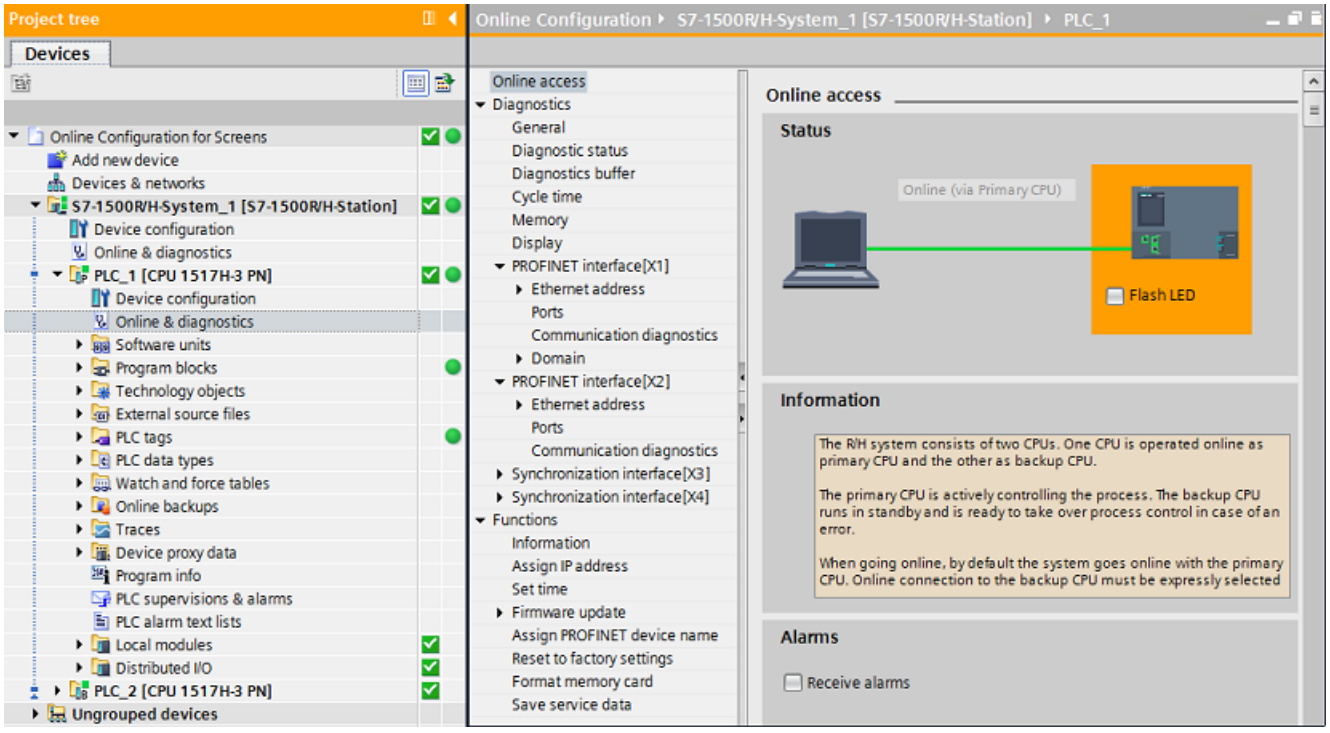


Figure 3-73 Online and Diagnostics view: CPU (RUN-Redundant system state)

Reference

You can find information on the operating and system states in the Redundant System S7-1500R/H System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833).

Online & diagnostics for IO devices in a line topology in the S7-1500H system

As of STEP 7 V18, you have the option to configure R1 devices. You assign each interface module of an R1 device to one of the two H-CPUs.

In the device view of the IO device, open the "Online & diagnostics" window. You will find the "Redundancy" dialog in the "Diagnostics" menu. It is divided as follows:

- "Module" column: The interface modules of the IO device.
- "Controller" column: The CPU assigned in each case.
- "Connection status" column: The current status of the connection between the interface module and assigned CPU and which interface module is currently being used.

The "Online & diagnostics" function for IO devices is independent of the configuration variant of the redundant S7-1500H system. You can use the "Online & diagnostics" function for ring or line topologies or a combination topology.

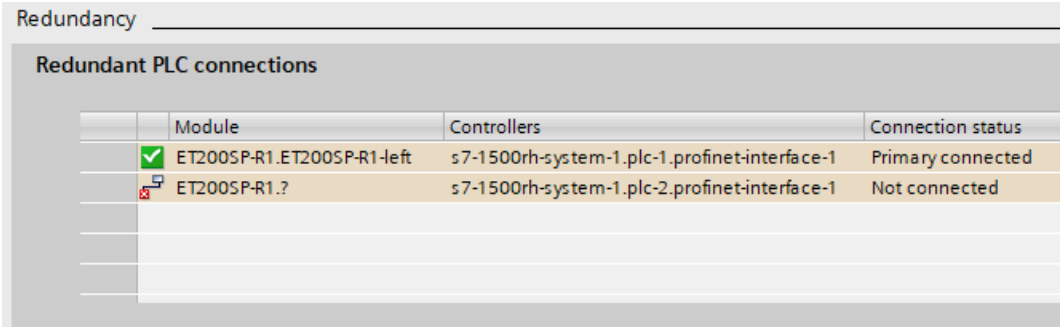


Figure 3-74 View of the "Redundancy" dialog window

NOTE

View of the interface module of an S2 device

In contrast to an R1 device, an S2 device has only one interface module. For this reason, the "Interface module" column shows only one interface modules for an S2 device.
The interface module is assigned to both H-CPUs.

8.2 "Online Tools" task card

Introduction

If an online connection exists to a CPU of the redundant system, the "Online Tools" task card displays online information for the redundant system.

For a S7-1500R/H redundant system, "Online Tools" displays:

- 3 panes operator panel
- Cycle time
- Memory

R/H system operator panel

For the redundant system, the "R/H system operator panel" pane shows the:

- Current states of the LEDs of the primary CPU
- System state
- Status of which CPU is the primary CPU and which CPU is the backup CPU with their current operating states

The "STOP R/H-System" button can be used to switch the S7-1500R/H system to the system state STOP.

NOTE

Reaching RUN-Redundant system state
Note that you cannot switch the S7-1500R/H to RUN-Redundant system state using the R/H-System operator panel. You reach the RUN-Redundant system state only by switching the operating state for each CPU to RUN in your CPU operator panel.

CPU operator panel

The two "CPU operator panel" panes show for the respective CPU of the redundant system:

- The role of the CPU, primary CPU or backup CPU
- The current states of the LEDs
- The operating state of the CPU

Use the "RUN / STOP" button to change the operating state for the respective CPU.

Use the "MRES" button to perform a memory rest for the CPU, under the following conditions:

- Online connection to this CPU is available
- The CPU is in STOP operating state.

The switch position at the real CPU is displayed under "Mode selector".

Example

The following figure shows an example of the "Online Tools" task card for the RUN-Solo system state. The primary CPU is in RUN operating state, the backup CPU in STOP operating state.

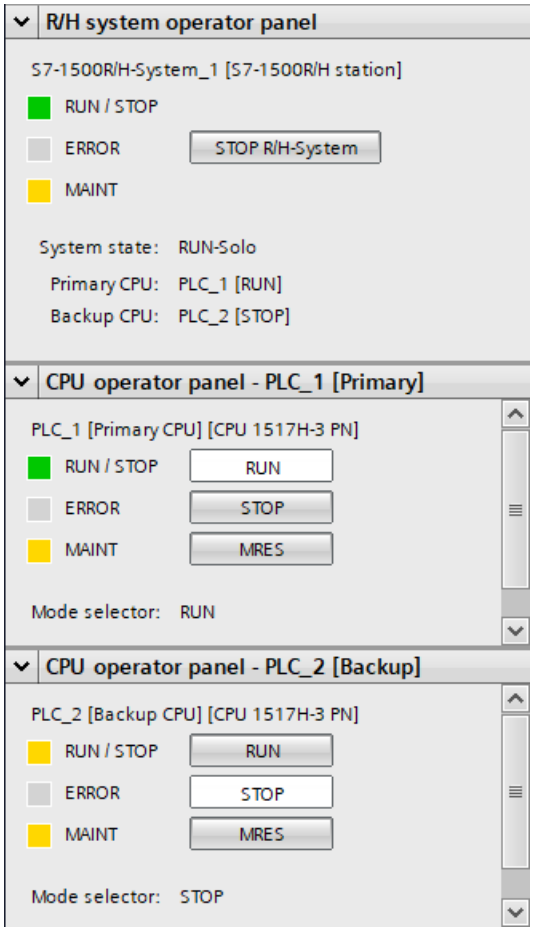


Figure 3-75 "Online Tools" task card: Operator panel (RUN-Solo system state)

Cycle time and memory

In the RUN-Redundant system state, the "Cycle time" and "Memory" panes show the current values of the primary CPU. In redundant mode, the cycle time of the primary CPU matches the cycle time of the system.

In the RUN-Solo system state, the panes show the current values for the CPU for which there is an online connection.

The display corresponds to the representation for standard CPUs.

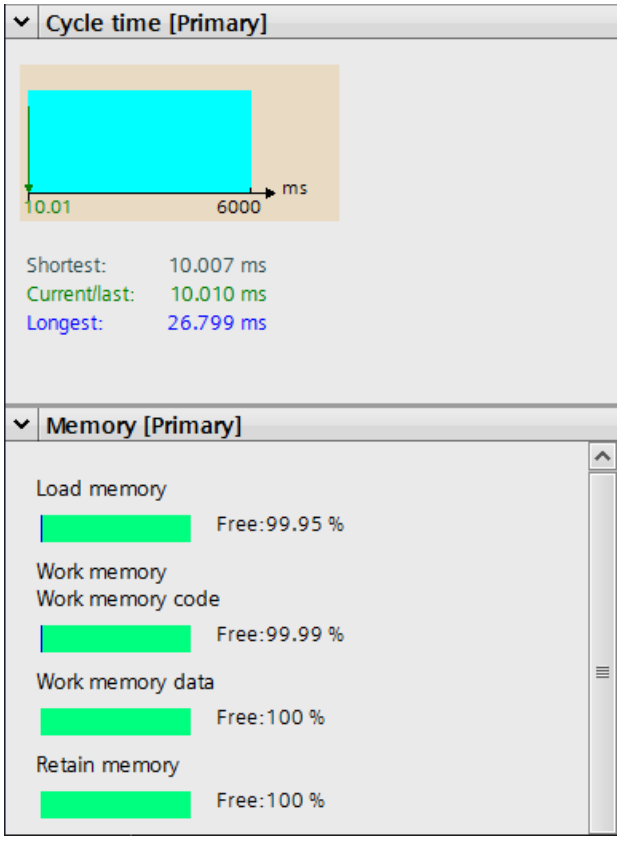


Figure 3-76 "Online Tools" task card: Cycle time and memory of the primary CPU

Reference

You can find information on the operating and system states in the Redundant System S7-1500R/H System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833).

8.3 Diagnostics view in the project tree and in the device view and network view

Additional icons for redundant systems in the project tree

Table 3-13 Icons for redundant systems in the project tree of STEP 7

Icon in the project tree	Meaning
	Identifier of the folder S7-1500R/H-System: RUN-Redundant system state
	Identifier of the folder S7-1500R/H-System: RUN-Solo system state

Icon in the project tree	Meaning
	Identifier of the folder S7-1500R/H-System: STARTUP system state
	Identifier of the folder S7-1500R/H-System: STOP system state
	Identifier of the folder for the primary CPU: RUN operating state
	Identifier of the folder for the backup CPU: RUN operating state
	Identifier of the folder for the primary CPU: STARTUP operating state
	Identifier of the folder for the backup CPU: SYNCUP operating state
	Identifier of the folder for the primary CPU: STOP operating state
	Identifier of the folder for the backup CPU: STOP operating state
	Identifier of the folder of a CPU of the redundant system: "Online via partner": The other CPU of the redundant system is connected online to the programming device / PC.

Example: Diagnostics view in the project tree and in the device view and network view

An example of the diagnostics view for a S7-1500R/H system is shown below.

The example configuration consists of two CPUs S7-1517H-3 PN and one interface module IM 155-6 PN HF as PROFINET IO device. PLC_1 is the primary CPU (in RUN operating state). PLC_2 is the backup CPU (in STOP operating state). The hardware configuration and the user program were loaded in the primary CPU.

The system is connected online via PLC_1 (primary CPU) and is in RUN-Solo system state.

View of the system in the project tree

The system is in RUN-Solo system state . PLC_1 is in RUN operating state , PLC_2 is in STOP operating state .

Because the system is in RUN-Solo system state, the following is displayed:

- For the system, maintenance demanded with problem in lower-level component 
- For PLC_1, maintenance demanded 

For PLC_2, online connection via partner is displayed, as the programming device/PC is connected online to PLC_1.

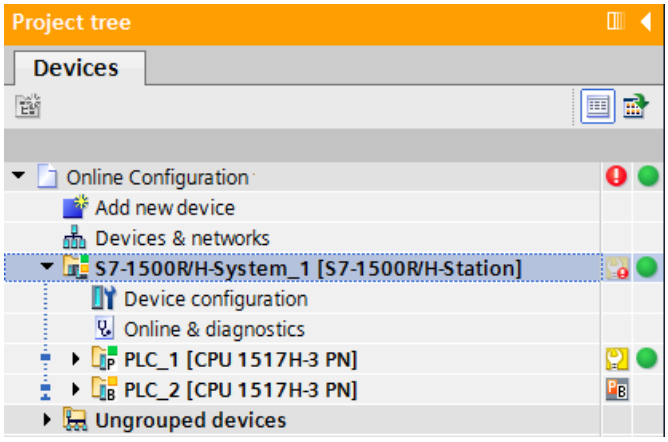


Figure 3-77 Diagnostics example: Redundant system project tree (RUN-Solo)

Network view of the system

The network view shows no faults for the H-CPUs or the IO device.

Maintenance demanded in lower-level component indicated for the system, since the system is not in the RUN-Redundant system state.

No operating states and system states of the redundant system are displayed in the network view.

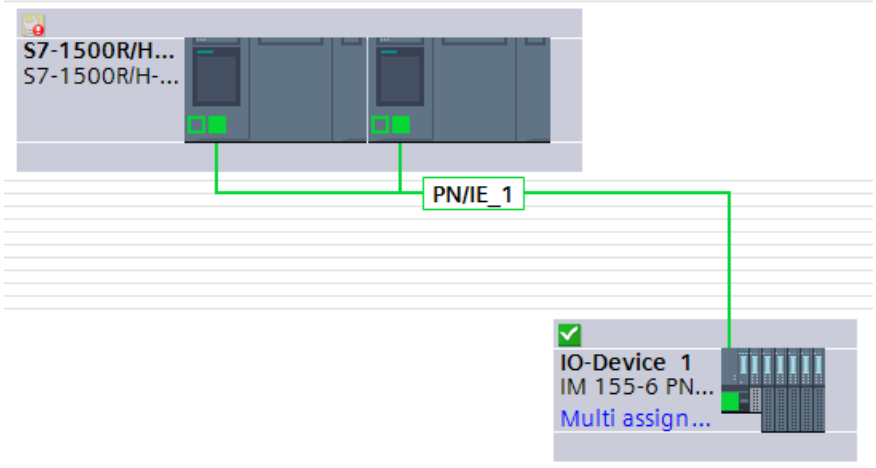


Figure 3-78 Diagnostics example: Network view of redundant system (RUN-Solo)

Doubling-clicking on the system gives you access to the device view of both CPUs.

Device view of the system

The device view shows you the operating states of the CPUs based on the icons next to PLC_1:

- Green icon: PLC_1 is in the RUN operating state.
- Yellow icon (wrench) for maintenance demanded: PLC_2 is in the STOP operating state.

The icon next to PLC_2 indicates that the online connection exists via the partner (PLC_1).

You can find more detailed information on the system faults in the "Diagnostics" tab, in "Device information". The device information indicates maintenance demanded and RUN operating state for PLC_1.

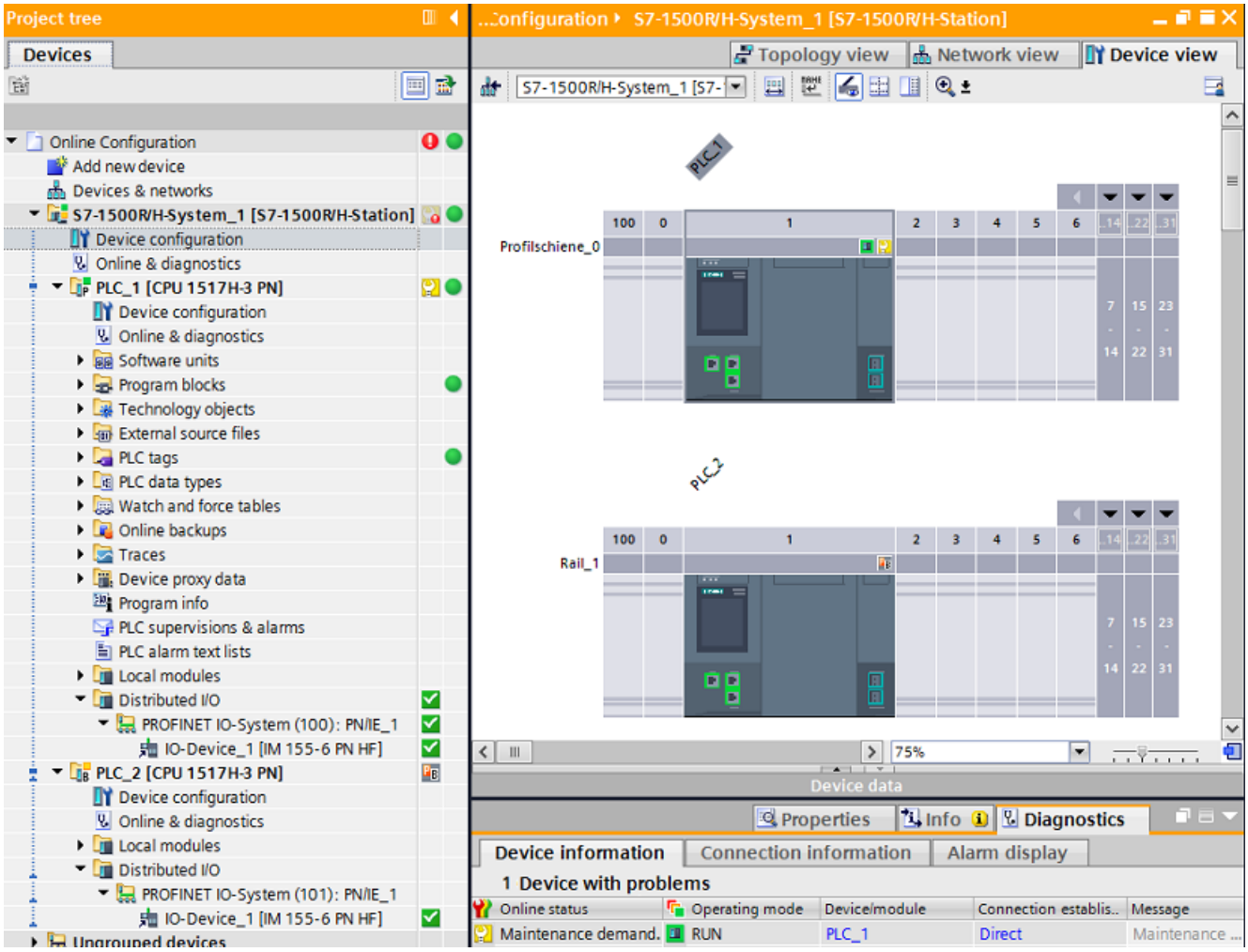


Figure 3-79 Diagnostics example: Device view of redundant system (RUN-Solo)

Alarm display of the system

As in the RUN-Solo system state, the alarms of the CPU for which there is an online connection are displayed via the "Alarm display" tab (in the example from PLC_1).

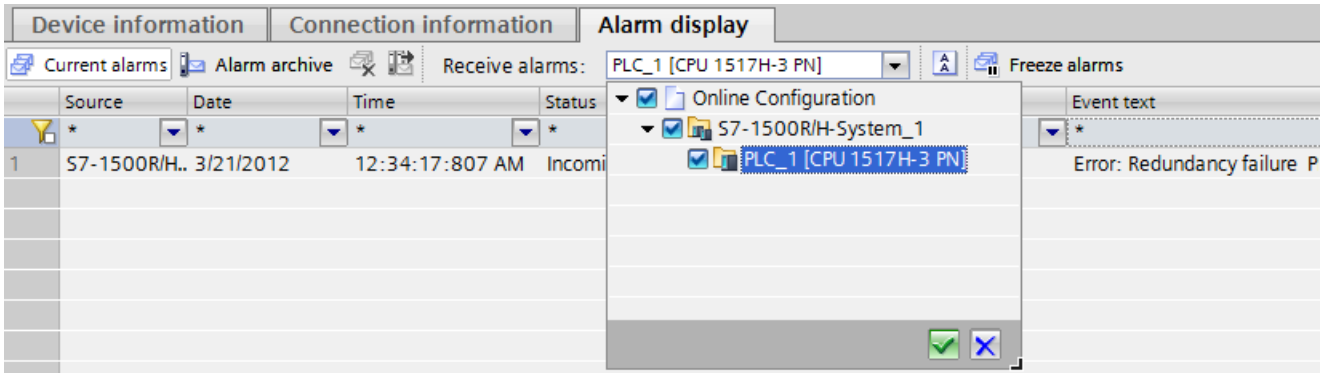


Figure 3-80 Diagnostics example: Alarm display of redundant system (RUN-Solo)

Device view of the IO device

The IO device is an interface module IM 155-6 PN HF with two I/O modules and one server module. The device view shows that there is no faults in the modules.

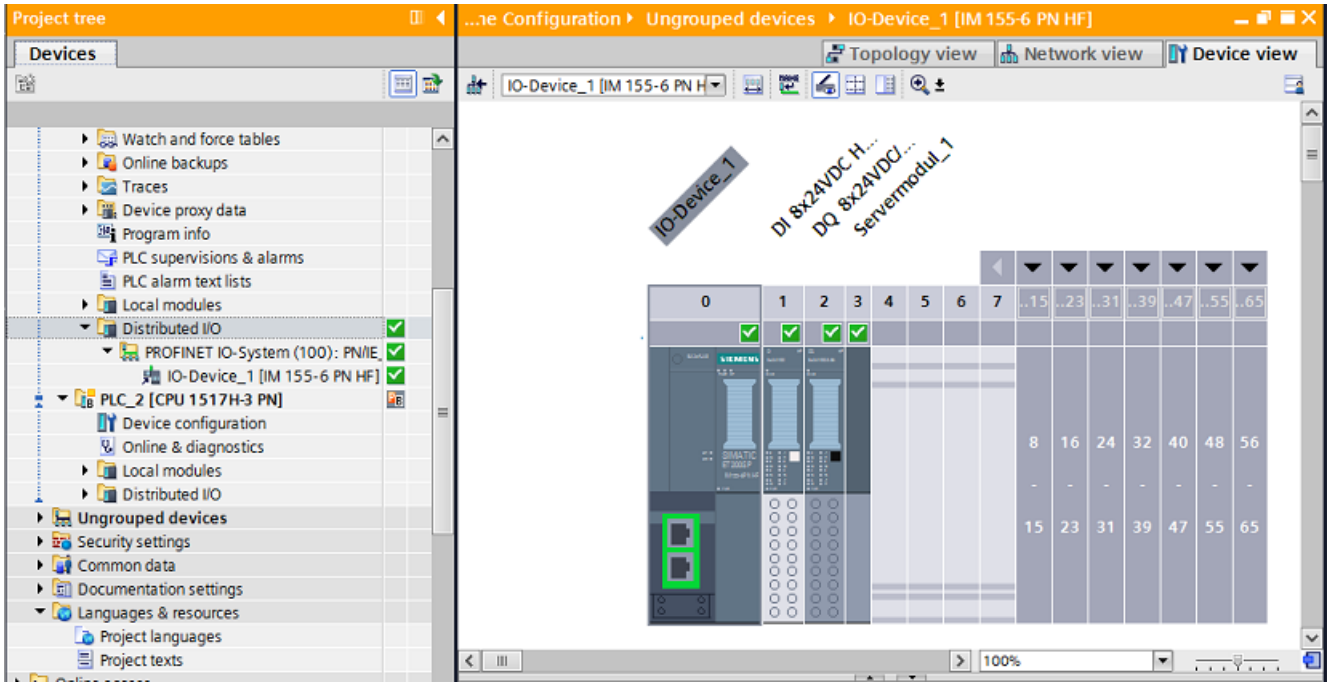


Figure 3-81 Diagnostics example: Device view of IO device

Diagnostics display for IO devices in the S7-1500H system

With the diagnostics display, you identify the following error scenarios, for example, based on the diagnostics icons:

- The PROFINET connection to an IO device is interrupted.
- An I/O module of an S2 device has been removed or is faulty.
- The PROFINET connection to an R1 device is interrupted.
- An interface module of an R1 device has been removed or is faulty.

The first two error scenarios are comparable to the diagnostics display of standard S7-1500 systems. The diagnostics of R1 devices is described in the next section.

Example: Diagnostics display of a faulty R1 device

An example of the diagnostics display for IO devices in the redundant S7-1500H system is shown below. The example configuration consists of the following components:

- 2 CPUs S7-1517H-3 PN
- R1 device: Interface module ET 200SP IM 155-6 PN R1
- S2 device: Interface module ET 200SP IM 155-6 PN HF

Requirements:

- You have an online connection to the redundant S7-1500H system.
- All connected IO devices are accessible via all interface modules.

In the project tree, you see the diagnostics display of the IO devices as follows:

- In the device folder of a CPU under "Distributed I/O > PROFINET IO system", you see the status of the assigned interface modules in each case.
- In the "Ungrouped devices" folder, you see the overall status of the IO devices. If you open the folder of an IO device, you also see the status of the interface modules.

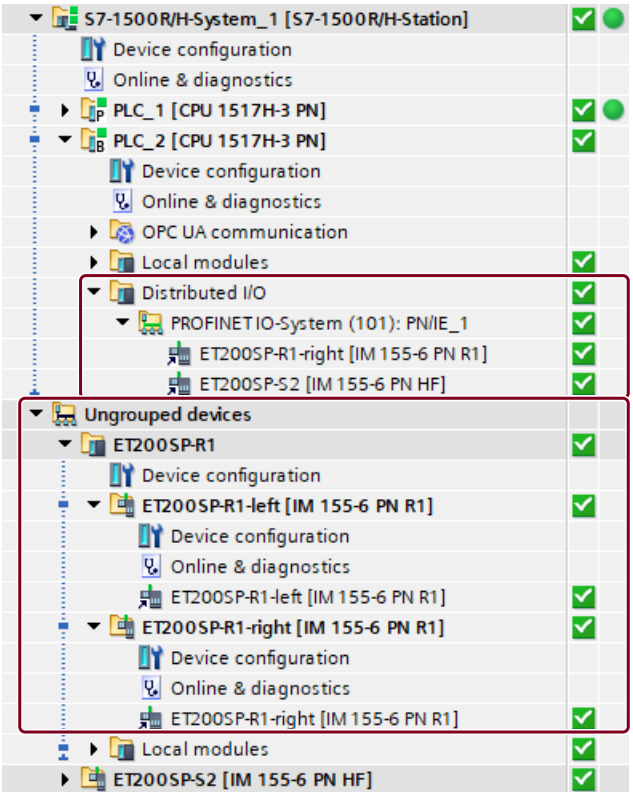


Figure 3-82 Diagnostics display of an R1 device in the project tree

The right interface module of the R1 device is removed or is faulty.

In the project tree, you see to the right of the device folder of the CPU the diagnostic information "Maintenance demanded, error in lower-level component" .

In the network view, the CPU and the R1 device also display the error through "Maintenance demanded, error in lower-level component" .

To display the diagnostics of the assigned interface modules, proceed as follows:

1. Open the device folder of the CPU.
2. Open the "Distributed I/O > PROFINET IO system" folder.
3. Displayed to the right of the interface modules is a corresponding diagnostics icon.

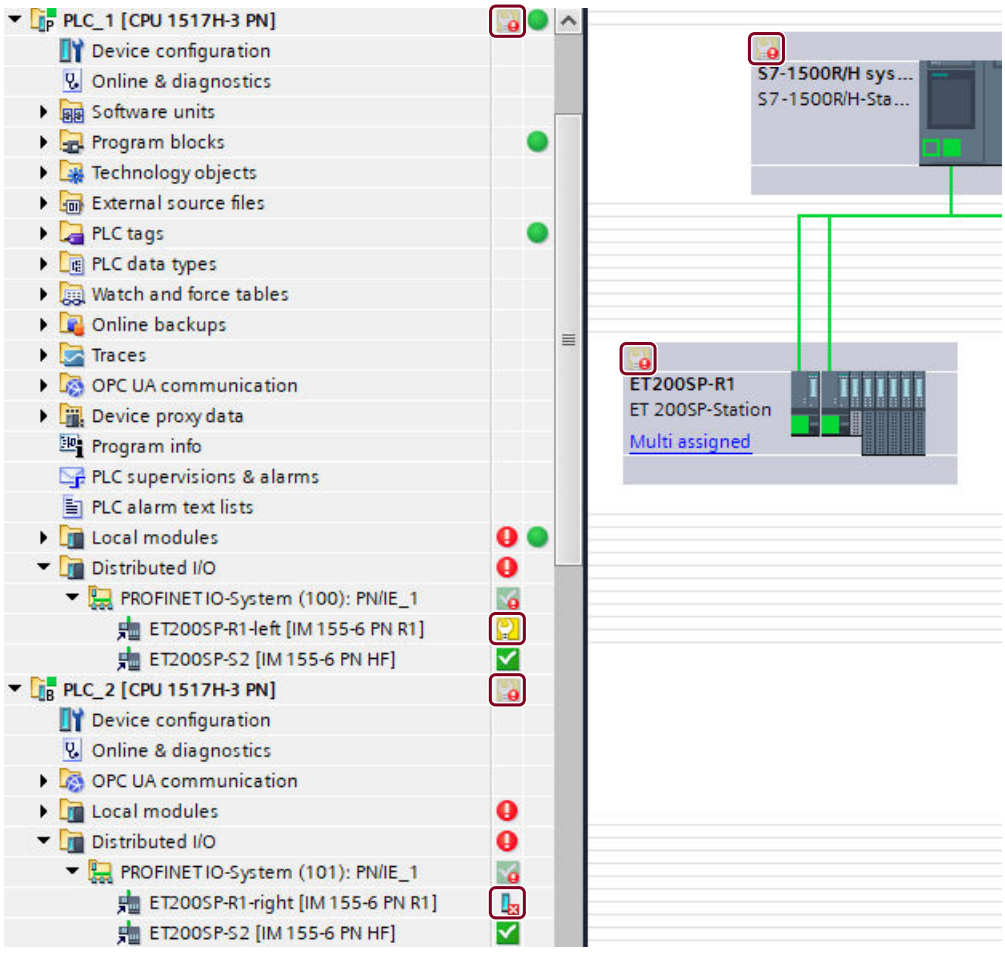


Figure 3-83 Project tree and network view of a faulty R1 device.

In the device view of the faulty IO device, you see the status of the individual interface modules.

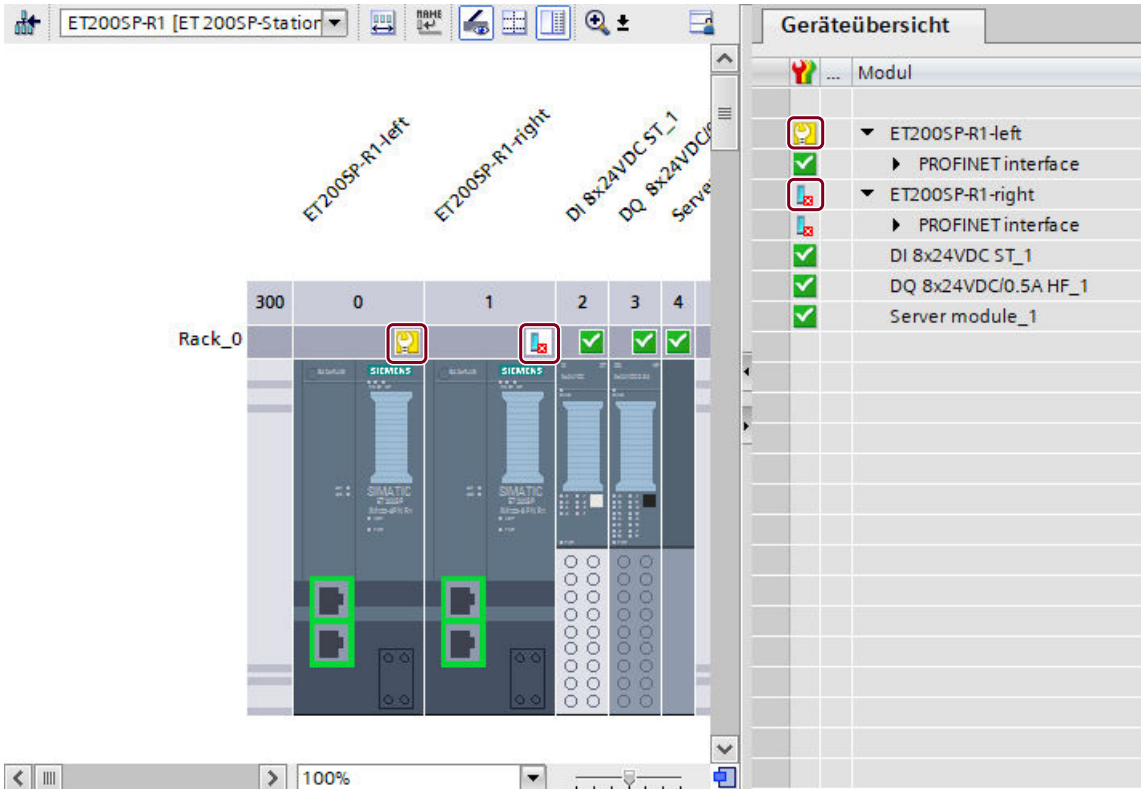


Figure 3-84 Diagnostics display of a faulty R1 device in the device view

To display extended diagnostics of the interface modules, proceed as follows:

1. Right-click the faulty interface module to open the shortcut menu.
2. Click the "Online and diagnostics" function.
3. Open the "Diagnostics" menu of the "Online and diagnostics" function and click "Redundancy".

In the "Redundancy" dialog window, you see the following information:

- "Icon" column: The diagnostics display of the interface module
- "Module" column: The interface modules of the IO device.
- "Controller" column: The CPU assigned in each case.
- "Connection status" column: The current status of the connection between the interface module and assigned CPU and which interface module is currently being used.

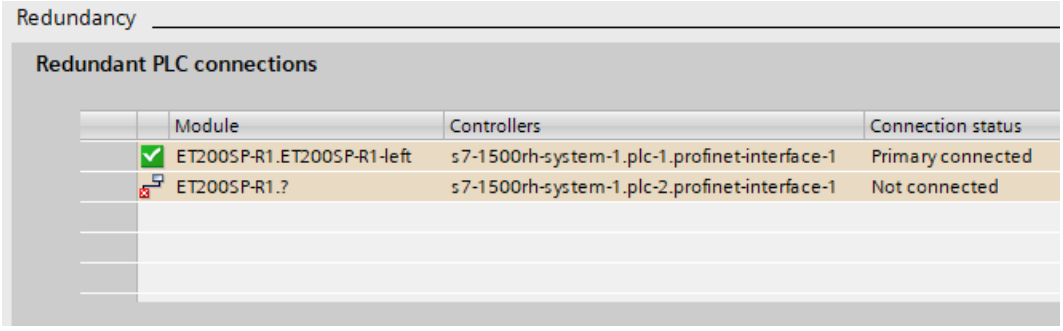


Figure 3-85 View of the "Redundancy" dialog window

NOTE

Deviating diagnostics display

If you remove an interface module of an R1 device, the other interface module signals this error with a red flashing ERROR LED. The LED error display has no effect on the process because the second interface module of the R1 device takes over.

In the STEP 7 online diagnostics, the R1 device is shown only as "Maintenance demanded, error in lower-level component". The reason for this is the different diagnostics views of the R1 device and H-CPU.

The IO device has only a local view and signals a missing module. The H-CPU, on the other hand, has a higher-level view of the redundancy of the two interface modules. The redundancy then results in the understated diagnostic information.

Therefore, when evaluating diagnostic information, pay attention not only to the LED error display on the devices. For a complete evaluation of diagnostic information, you must also look at the STEP 7 online diagnostics and evaluate the diagnostics buffer.

8.4 Diagnostics in the RUN-Redundant system state

Diagnostics view in redundant mode

Primary CPU and backup CPU are each in the RUN-Redundant operating state.

In the RUN-Redundant system state, the primary and backup CPUs display the online data of the redundant system irrespective of which of the two CPUs has the online connection.

The diagnostics between the two CPUs is synchronized (diagnostics entries, diagnostics events).

The "Alarm display" tab shows the alarms of the redundant system.

You can find more information in the Diagnostics view in the project tree and in the device view and network view (Page 106).

No error in RUN-Redundant system state

If no error is detected in the RUN-Redundant system state, all diagnostics icons in the project tree and in the network view show "No fault" ✅.

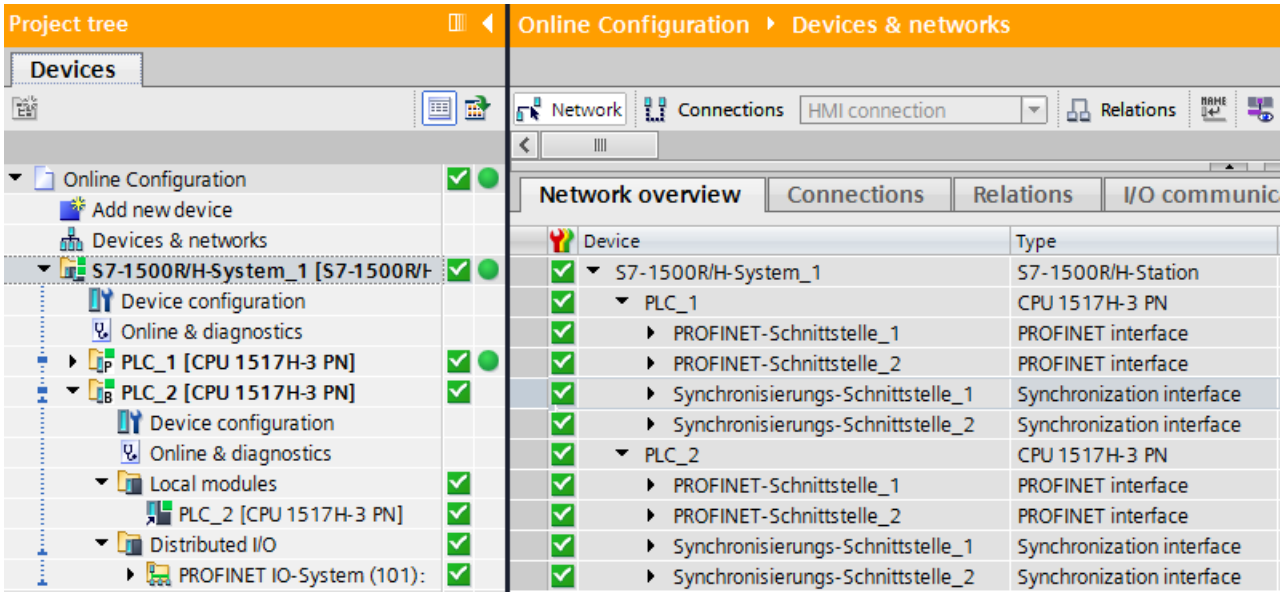


Figure 3-86 Diagnostics example: No fault in the RUN-Redundant project tree

Error in the RUN-Redundant system state

Most errors in the redundant system do not result in a loss of redundancy. The RUN-Redundant system state is retained, for example, if a module in an IO device fails. The diagnostics view is similar to the standard S7-1500 systems.

In the RUN-Redundant system state the redundancy of the system can be restricted, e.g. during the interruption of one of the two redundancy connections in S7-1500H. You can find information on the redundancy scenarios in the Redundant System S7-1500R/H System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833).

Special examples of a redundant system S7-1500H are shown below:

S7-1500H Example 1:
The PROFINET ring between the CPU of the redundant S7-1500H system and an IO device was interrupted.

Requirements:

- No topology has been configured in the project.
- Both CPUs are in the same PROFINET ring.

Evaluate diagnostics via LINK TX/RX LEDs on the CPU
TX/RX X1 P1 LED is not illuminated. This means:

- No Ethernet connection between the P1 port of the respective PROFINET interface and the communication partner

Diagnostics in STEP 7
The diagnostics buffer of the CPU that was "MRP Manager' at this time indicates that the PROFINET ring is open.

The diagnostics in the project tree shows:

- Maintenance demanded in lower-level component in the S7-1500H system
- Maintenance demanded in lower-level components of PLC_1 and PLC_2
- Maintenance demanded in lower-level components of local modules of PLC_2

The diagnostics in the network view indicates errors at the affected port of the PROFINET interfaces of PLC_2.

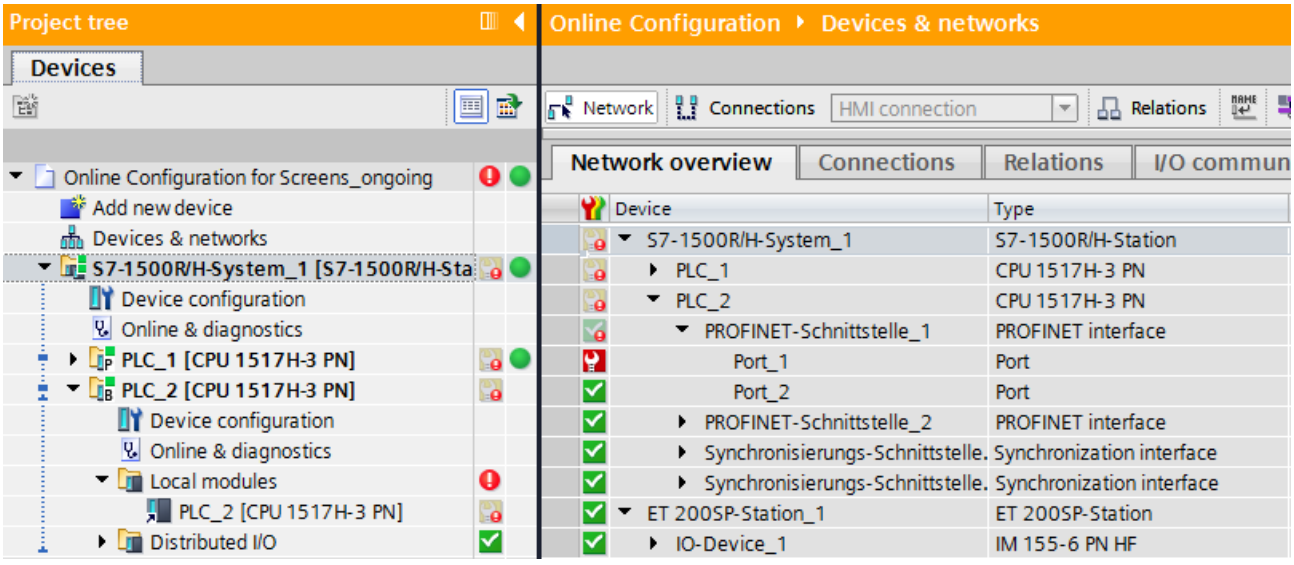


Figure 3-87 Diagnostics example: RUN-Redundant system state, open PROFINET ring

You can evaluate the diagnostics using the displays of the CPUs via the "Diagnostics" menu as with standard CPUs. You can find additional information in the section Display of the CPU (Page 30).

S7-1500H Example 2:
A synchronization module has been removed from a CPU of the redundant S7-1500H system.

Evaluating diagnostics via X3 and X4 LEDs on the CPU
The X3 LED on PLC_2 CPU is not illuminated. This means:

- The redundancy connection on the synchronization module was interrupted at the H-Sync interface X3.

  or

- There is no synchronization module at the H-Sync interface X3.

Diagnostics in STEP 7
The diagnostics buffer of the CPU displays:

- that there is only one redundancy connection
- which synchronization module has failed on which CPU

The diagnostics in the project tree shows:

- Maintenance demanded in lower-level component in the S7-1500H system
- Maintenance demanded in lower-level components of PLC_1 and PLC_2
- Maintenance demanded in lower-level components of local modules of PLC_1 and PLC_2

The diagnostics in the network view displays:

- Errors for the Synchronisationsmodul_1 of the Synchronisationsschnittstelle_2 of PLC_1
- Synchronisationsmodul_1 of Synchronisationsschnittstelle_1 of PLC_2 not reachable

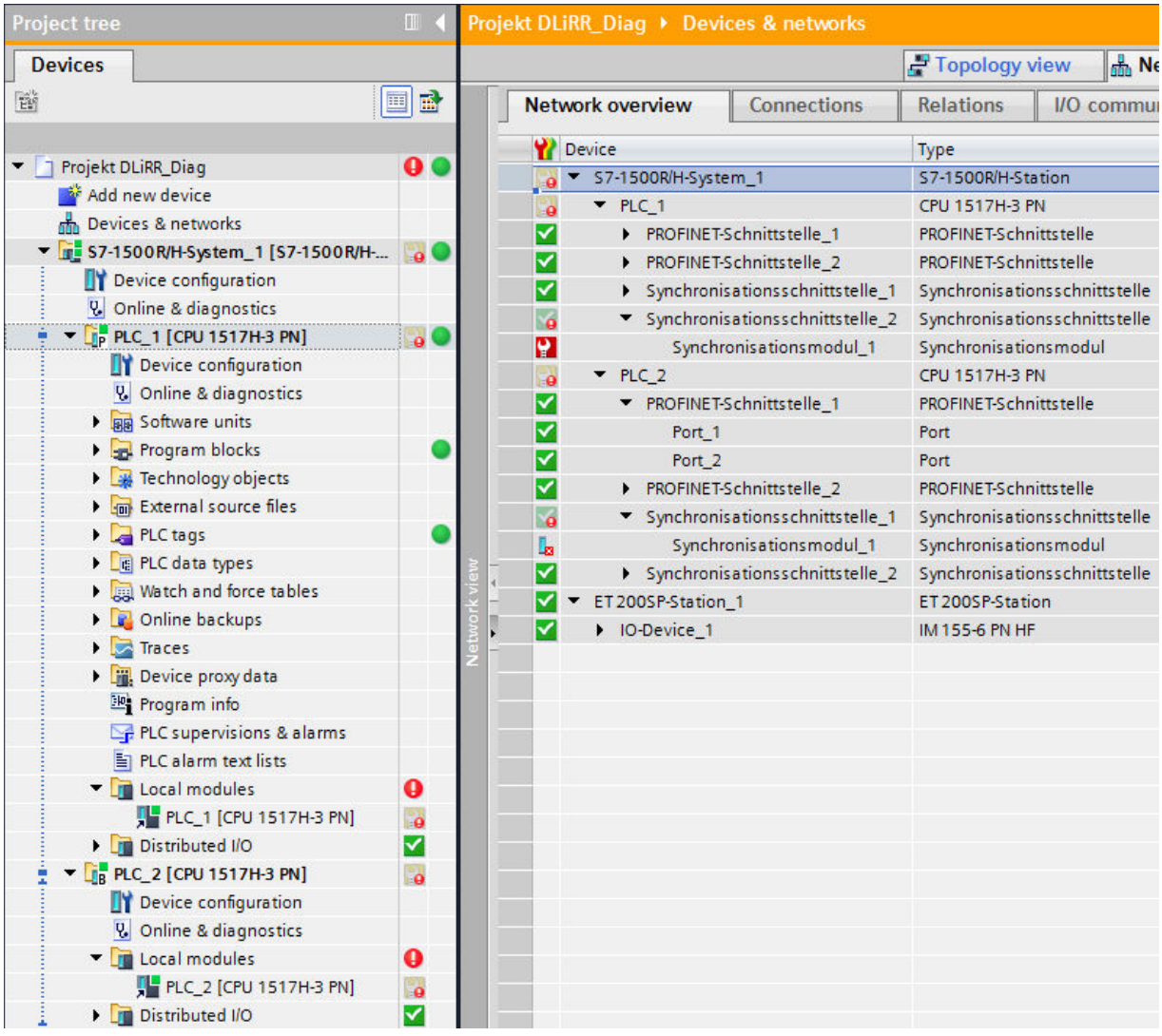


Figure 3-88 Diagnostics example: RUN-Redundant system state, a synchronization module fails

Evaluate diagnostics on the display

For example 2, display of the PLC_2 CPU shows:



- In the "Overview" menu command: A message is available in the next lower level page.
- In the "Diagnostics" menu command: A message is available in the next lower level page.
- In the Module menu command: An error has occurred.

To evaluate the display, proceed as follows:

1. Navigate to "Pairing state" via the menu commands "Overview" > "Redundancy".
2. This is displayed as the pairing state: Single paired (X4).
   This means that the redundancy connection is available at the H-Sync interface X4, but not at the X3.
3. Navigate to "Alarms" via the "Diagnostics" menu command.
4. View the details of the alarm (evaluate diagnostics buffer).

S7-1500H Example 3:
A redundancy connection in S7-1500H is interrupted.

Evaluating diagnostics via X3 and X4 LEDs on the CPU
The LED X4 on CPU PLC_1 does not light up. This means:

- The redundancy connection on the synchronization module was interrupted at the H-Sync interface X4.
  or
- There is no synchronization module at the H-Sync interface X4.

Diagnostics in STEP 7
The diagnostics buffer of the CPU displays:

- that there is only one redundancy connection
- Fiber-optic error with specification of the CPU and the synchronization module

The diagnostics in the project tree shows:

- Maintenance demanded in lower-level component in the S7-1500H system
- Maintenance demanded in lower-level components of PLC_1 and PLC_2
- Maintenance demanded in lower-level components of local modules of PLC_1 and PLC_2

The diagnostics in the network view displays:

- Errors for the Synchronisationsmodul_1 of the Synchronisationsschnittstelle_2 of PLC_1
- Errors for the Synchronisationsmodul_1 of the Synchronisationsschnittstelle_1 of PLC_2

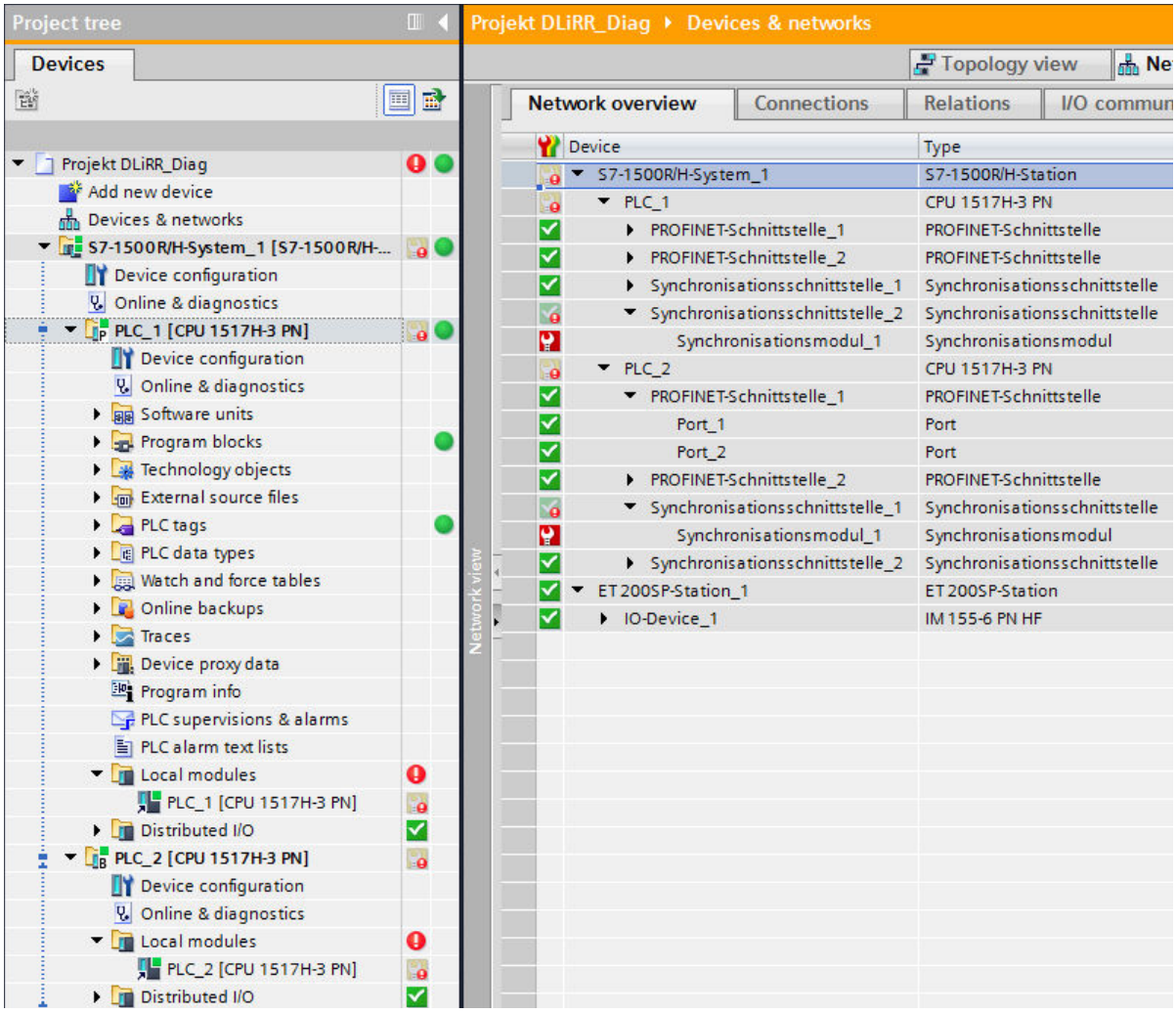


Figure 3-89 Diagnostics example: RUN-Redundant system state, a redundancy connection has failed

Evaluate diagnostics on the display

Perform the analysis of the display of PLC_2 CPU exactly as for example 2.

8.5 Restrictions in the RUN-Solo system state

The primary CPU is in RUN operating state. The Backup CPU is in STOP operating state, is switched off, defective, or not available.

Restrictions in the RUN-Solo system state

The primary CPU records the diagnostics states of the distributed I/O.

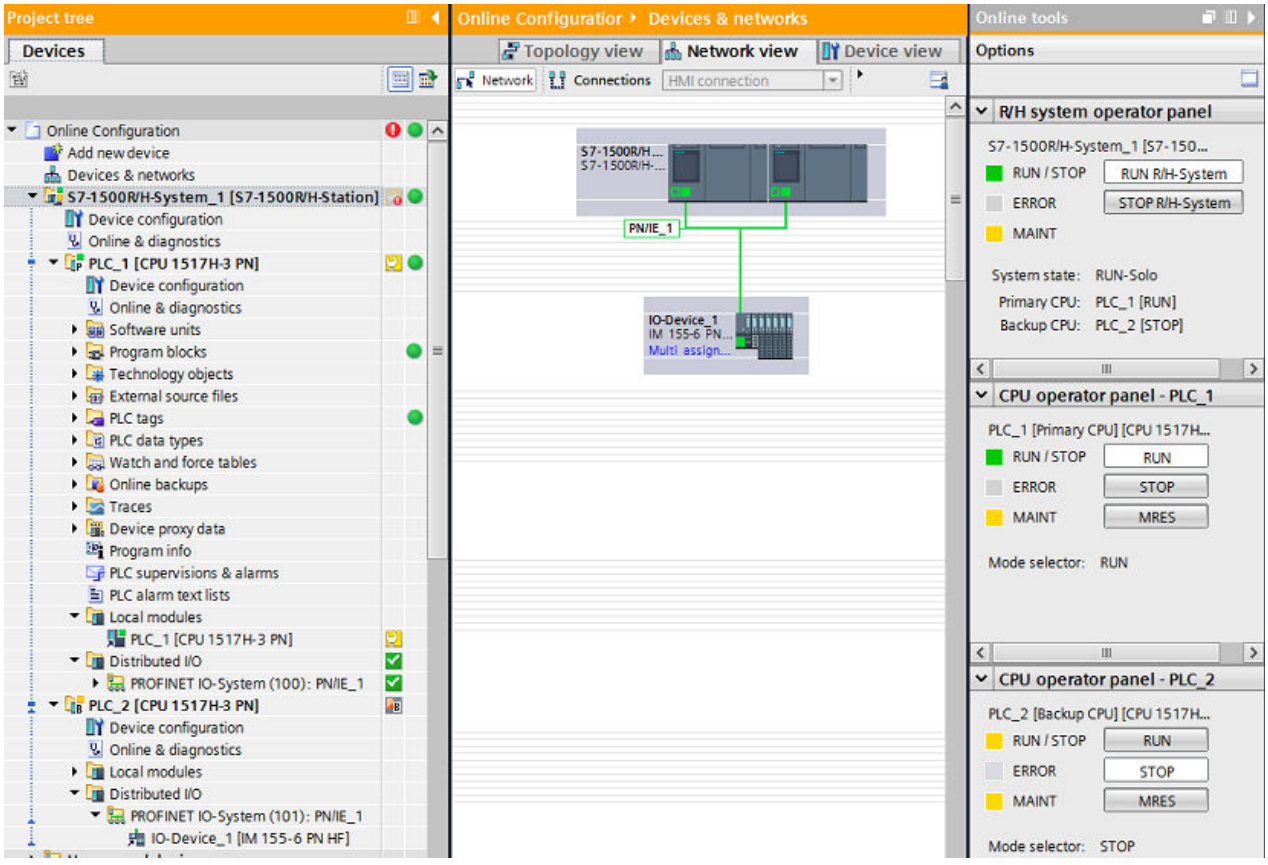


Figure 3-90 Diagnostics of the primary CPU and backup CPU in RUN-Solo system state

Diagnostics of the backup CPU

The following restrictions apply to the backup CPU:

- Diagnostics information from the backup CPU is only available when there is an online connection to the backup CPU.
- A memory reset can only be performed with the backup CPU operator panel when an online connection to the backup CPU is available.

Reference

You can evaluate the diagnostics using the displays of the CPUs via the "Diagnostics" menu as with standard CPUs. You can find additional information in the section Display of the CPU (Page 30).

8.6 System diagnostics by means of the user program

Instructions

Instructions for determining the system diagnostics are listed in the section System diagnostics options in the user program (Page 75).

The following instruction for diagnostics cannot be used for S7-1500R/H redundant systems:

- DPNRM_DG: Read diagnostics data from a DP slave

Organization blocks

You can find the description of the applicable OBs for S7-1500R/H in the S7-1500R/H redundant system (https://support.industry.siemens.com/cs/ww/en/view/109754833) system manual.

SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200BL,ET 200AL, ET 200pro, ET 200eco PN, ET 200clean Communication

Function Manual

Introduction 1

Security information 2

Industrial cybersecurity 3

Product overview 4

Communications services 5

PG communication 6

HMI communication 7

Open User Communication 8

S7 communication 9

Point-to-point link 10

OPC UA communication 11

Addressing via DHCP 12

Routing 13

Connection resources 14

Diagnostics and fault correction 15

Continued on next page

11/2025
A5E03735815-AN

Continued
Communication with the redundant system S7-1500R/H 16

Industrial Ethernet Security with CP 1543-1 17

S7-1500, ET 200MP, ET 200SP, ET 200BL,ET 200AL, ET 200pro, ET 200eco PN, ET 200clean Communication

Function Manual

Table of contents

1 Introduction 9

1.1 SiePortal 16

1.2 Function Manuals documentation guide 16
1.2.1 Information classes Function Manuals 16
1.2.2 Basic tools 18
1.2.3 S7 Port Configuration Tool (S7-PCT) 20
1.2.4 S7 Failsafe Configuration Tool (S7-FCT) 20
1.2.5 MultiFieldbus Configuration Tool (MFCT) 20
1.2.6 SIMATIC Technical Documentation 21

2 Security information 24

2.1 General security information 24

3 Industrial cybersecurity 25

3.1 Cybersecurity information 25

3.2 Security-relevant information in this manual 26

4 Product overview 27

5 Communications services 33

5.1 Overview of communication options 33

5.2 Communications protocols and port numbers used for Ethernet communication 35

5.3 Overview of connection resources 43

5.4 Setting up a connection 44

5.5 Data consistency 48

5.6 Secure Communication 51
5.6.1 Basics of Secure Communication 51
5.6.1.1 Useful information on Secure Communication 51
5.6.1.2 Device-dependent security features 54
5.6.1.3 Confidentiality through encryption 56
5.6.1.4 Authenticity and integrity through signatures 58
5.6.2 Managing certificates 62
5.6.2.1 What you should know about the certificate management 62
5.6.2.2 Certificate management with TIA Portal 63
5.6.2.3 Examples for the management of certificates 67
5.6.2.4 How communication with certificates works: HTTP over TLS 72
5.6.2.5 Tip: Updating loaded certificates in RUN 75
5.6.3 Requirements for secure communication 76
5.6.3.1 Protection of confidential configuration data 76
5.6.3.2 Useful information for the protection of confidential PLC configuration data 78
5.6.3.3 Changing your password 80
5.6.3.4 Resetting the password 81

5.6.3.5 Assign password via SIMATIC Memory Card 84
5.6.3.6 Special features when backing up and restoring a CPU 85
5.6.3.7 Tips for error avoidance and error handling 86
5.6.3.8 Rules for the replacement parts scenario 87
5.6.4 Secure Open User Communication 88
5.6.4.1 Secure OUC of an S7-1500 CPU as TLS client to an external PLC (TLS server) 88
5.6.4.2 Secure OUC of an S7-1500 CPU as TLS server to an external PLC (TLS client) 91
5.6.4.3 Secure OUC between two S7-1500 CPUs 93
5.6.4.4 Secure OUC via CP interface 96
5.6.4.5 Secure OUC with Modbus TCP 101
5.6.4.6 Secure OUC via e-mail 103
5.6.5 Secure PG/HMI communication 106
5.6.5.1 PG/HMI communication based on standardized security mechanisms 106
5.6.5.2 Additional settings for the secure PG/HMI communication 107
5.6.5.3 Tip for certificate-based communication between PG and CPU 109
5.6.5.4 CPU behavior from loading to operational readiness 110
5.6.5.5 Using secure HMI communication 113
5.6.5.6 Using Legacy PG/PC communication for TIA Portal 115
5.6.5.7 Information about compatibility 116
5.7 SNMP 117
5.7.1 Activating and deactivating SNMP 117
5.7.2 Activating/deactivating SNMP by data record transfer: Example for a CPU 1516-3 PN/DP 120
5.7.3 Activating/deactivating SNMP by data record transfer with S7-1500R/H CPUs 122

6 PG communication 125

7 HMI communication 127

8 Open User Communication 129
8.1 Overview of Open User Communication 129
8.2 Protocols for Open User Communication 130
8.3 Instructions for Open User Communication 131
8.4 Open User Communication with addressing via domain names 135
8.5 Setting up Open User Communication via TCP, ISO-on-TCP, UDP and ISO 138
8.6 Setting up communication over FDL 142
8.7 Setting up communication with Modbus TCP 145
8.8 Setting up communication via e-mail 147
8.9 Setting up communication via FTP 148
8.10 Establishment and termination of communications relations 151

9 S7 communication 152

10 Point-to-point link 160

11 OPC UA communication 165
11.1 What you need to know about OPC UA 165

11.1.1 OPC UA and Industry 4.0 ... 165
11.1.2 General features of OPC UA ... 166
11.1.3 OPC UA for S7-1200/S7-1500 CPUs ... 169
11.1.4 Access to OPC UA applications ... 170
11.1.5 Addressing nodes ... 174
11.1.6 Namespace overview for the OPC UA server of the S7-1200/1500 CPUs ... 177
11.1.7 What you need to know about OPC UA clients ... 178

11.2 Security at OPC UA ... 182
11.2.1 Security settings ... 182
11.2.2 Certificates pursuant to ITU X.509 ... 183
11.2.3 Certificates with OPC UA ... 186
11.2.4 Creating self-signed certificates ... 186
11.2.5 Generating PKI key pairs and certificates yourself ... 187
11.2.6 Secure transfer of messages ... 190
11.2.7 Certificate management via Global Discovery Server (GDS) ... 193
11.2.7.1 Automated certificate management with GDS ... 193
11.2.7.2 Configuration limits for Push function ... 196
11.2.7.3 Setting and loading GDS parameters ... 197
11.2.7.4 GDS commissioning ... 199
11.2.7.5 Address model for the push certificate management ... 203
11.2.7.6 CertificateGroups in the address model ... 207
11.2.8 Role-based security in OPC UA ... 210
11.2.8.1 Interesting facts about role-based security ... 210
11.2.8.2 Configuring role-based access control for OPC UA ... 213
11.2.8.3 How the OPC UA server evaluates permissions on nodes ... 217
11.2.8.4 Importing nodeset files with role definitions ... 219

11.3 Using the S7-1500 as an OPC UA server ... 222
11.3.1 Interesting information about the OPC UA server of the S7-1500 CPUs ... 222
11.3.1.1 The OPC UA server of the S7-1500 CPUs ... 222
11.3.1.2 End points of the OPC UA server ... 224
11.3.1.3 Mapping of data types ... 226
11.3.1.4 Runtime behavior of the OPC UA server ... 229
11.3.2 Accessing OPC UA server data ... 231
11.3.2.1 Client accesses and local accesses to the OPC UA server ... 231
11.3.2.2 Managing write and read rights ... 235
11.3.2.3 Managing write and read rights for a complete DB ... 237
11.3.2.4 Coordinating write and read rights for CPU tags ... 239
11.3.2.5 Consistency of CPU tags ... 241
11.3.2.6 Write accesses to OPC UA variables from S7-1500 Motion Control ... 242
11.3.2.7 Accessing OPC UA server data ... 243
11.3.2.8 MinimumSamplingInterval attribute ... 244
11.3.2.9 Export OPC UA XML file ... 244
11.3.3 Configuring the OPC UA server ... 245
11.3.3.1 Enabling the OPC UA server ... 245
11.3.3.2 Access to the OPC UA server ... 248
11.3.3.3 General settings of the OPC UA server ... 250
11.3.3.4 Settings of the server for subscriptions ... 252
11.3.3.5 Using the TransferSubscription service ... 254
11.3.3.6 Handling client and server certificates ... 255
11.3.3.7 Generating server certificates with STEP 7 ... 261
11.3.3.8 User authentication ... 264

11.3.3.9	Users and roles with OPC UA function rights	266
11.3.3.10	Diagnostic settings of the server	268
11.3.3.11	License for OPC UA	269
11.3.4	OPC UA server interface configuration	270
11.3.4.1	What is a server interface?	270
11.3.4.2	Using OPC UA companion specifications	271
11.3.4.3	Creating a server interface for companion specification	278
11.3.4.4	Creating a user-defined server interface	283
11.3.4.5	Data types for companion specifications	289
11.3.4.6	LocalizedText and ByteString data types	290
11.3.4.7	Using additional OPC UA data types for companion specifications	292
11.3.4.8	Dynamic arrays	295
11.3.4.9	Rules for OPC UA XML files	298
11.3.4.10	Creating a server interface for reference namespace	299
11.3.4.11	Generating OPC UA nodes based on local data mappings of FB types and UDTs	301
11.3.4.12	Notes on configuration limits when using server interfaces	306
11.3.5	Providing methods on the OPC UA server	306
11.3.5.1	Useful information about server methods	306
11.3.5.2	Boundary conditions for using server methods	310
11.3.6	Providing alarms on the OPC UA server	311
11.3.6.1	Useful information on alarms	311
11.3.6.2	OPC UA Events	316
11.3.6.3	OPC UA conditions and OPC UA alarms	318
11.3.6.4	Activating Alarms and Conditions	320
11.3.6.5	Subscribing to events of an OPC UA server	321
11.3.6.6	Processing associated values of alarms	324
11.3.6.7	Simultaneous receipt of messages in multiple languages	327
11.3.6.8	Methods for OPC UA Alarms and Conditions	329
11.3.6.9	Handling memory limits for OPC UA Alarms and Conditions	332
11.3.7	Using diagnostics options	335
11.3.7.1	Diagnostics of the OPC UA server	335
11.3.7.2	Running diagnostics for OPC UA servers in the program	336
11.3.7.3	Server state transition diagnostics	337
11.3.7.4	Session state transition diagnostics	338
11.3.7.5	Check for security events	339
11.3.7.6	Request of a remote client failed	340
11.3.7.7	Subscription diagnostics	341
11.3.7.8	Summarizing diagnostics	344
11.4	Using the S7-1500 CPU as an OPC UA client	346
11.4.1	Overview and requirements	346
11.4.2	Useful information about the client instructions	347
11.4.3	Number of client instructions that can be used simultaneously	349
11.4.4	Example configuration for OPC UA	350
11.4.5	Creating client interfaces	351
11.4.6	Determine server interface online	358
11.4.7	Using multilingual texts	361
11.4.8	Rules for the access to structures	363
11.4.9	Using connection parameter assignment	365
11.4.9.1	Creating and configuring connections	365
11.4.9.2	Handling of the client certificates of the S7-1500 CPU	368
11.4.9.3	Handling client certificates during runtime	371

11.4.9.4 User authentication ... 374
11.4.9.5 Using a configured connection ... 375
11.5 Tips and recommendations ... 380
11.5.1 Rules for subscriptions ... 380
11.5.2 Rules for the user program ... 381
11.5.3 Master copies for OPC UA communication ... 382

12 Addressing via DHCP ... 384
12.1 Principle of address assignment via DHCP ... 386
12.2 DHCP with DNS ... 388
12.3 Activate DHCP ... 392
12.4 Configuring the client ID ... 393
12.5 Get addresses of the DNS servers via DHCP ... 394
12.6 Get addresses of the NTP servers via DHCP ... 395
12.7 Obtain host and domain name via DHCP ... 395

13 Routing ... 397
13.1 Overview of the routing mechanisms of S7-1500 CPUs ... 397
13.2 S7 routing ... 397
13.3 IP forwarding ... 402
13.3.1 Enabling and disabling IP forwarding ... 409
13.3.2 Enabling/disabling IP forwarding via data record transfer: Example for a CPU 1516-3 PN/DP ... 410
13.3.3 Enabling/disabling IP forwarding via data record transfer with S7-1500R/H CPUs ... 412
13.4 Data record routing ... 415
13.5 Virtual interface for IP-based applications ... 417

14 Connection resources ... 421
14.1 Connection resources of a station ... 421
14.2 Allocation of connection resources ... 424
14.3 Display of the connection resources ... 428

15 Diagnostics and fault correction ... 431
15.1 Connection diagnostics ... 431
15.2 Emergency address ... 434

16 Communication with the redundant system S7-1500R/H ... 435
16.1 System IP addresses for R/H CPUs ... 436
16.2 System IP addresses for communications processors ... 442
16.3 Improved accessibility by switching the system IP address ... 446
16.4 Behavior during SYNCUP ... 447

16.5 Response to primary-backup switchover 447
16.6 Connection resources of the redundant system S7-1500R/H 448
16.7 HMI communication with the redundant system S7-1500R/H 449
16.7.1 HMI connection via the system IP address 449
16.8 Open User Communication with the redundant system S7-1500R/H 452
16.8.1 Setting up the connection of the Open User Communication with the redundant S7-1500R/H system 453
16.8.2 Open User Communication with CP 1543-1 communications processors 457
16.9 Using an OPC UA server in an S7-1500R/H system 459
16.9.1 Information worth knowing on the OPC UA server in the S7-1500R/H system 459
16.9.2 Transparent Mode (transparent Redundancy) 462
16.9.3 Non-transparent Mode (non-transparent Redundancy) 463
16.9.4 Information model in detail 468
16.9.5 Updated instructions for server methods 471

17 Industrial Ethernet Security with CP 1543-1 475

17.1 Firewall 476
17.2 Logging 476
17.3 NTP client 477
17.4 SNMP 477
17.5 VPN 478

Introduction

1

Purpose of the documentation

This function manual provides an overview of the communication options offered by the CPUs, communication modules and processors, and PC systems of the SIMATIC S7-1500, ET 200 and SIMATIC Drive Controller systems. This Function Manual describes connection-oriented, asynchronous communication.

The documentation covers the following:

- Overview of communications services
- Properties of communications services
- Overview of user activities for setting up communications services

Basic knowledge required

The following knowledge is required in order to understand the Function Manual:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge about how to use STEP 7 (TIA Portal)

Scope of the documentation

This documentation is the basic documentation for all products of the SIMATIC S7-1500 and ET 200 systems. The product documentation is based on this documentation.

What's new in the Communication Function Manual, Edition 11/2025 compared to Edition 11/2024?

What's new?	What are the customer benefits?	Where can I find the information?
Information on the validity period of certificates	Information on the validity period of certificates and the special case when a certificate expires while a protected connection is established.	Section Certificate management with TIA Portal (Page 63)
Access control with OPC UA server	You can read how to configure user roles and authorizations for OPC UA namespaces.	Section Role-based security in OPC UA (Page 210)
Automatic generation of the application URI	The application URI is the unique identifier of the application. As of FW version V4.1, the application URI is automatically generated from the application name. You can read the relationships between the application name and application URI as well as the dependencies in the event of changes.	Section Enabling the OPC UA server (Page 245)

What's new?	What are the customer benefits?	Where can I find the information?
Standard security settings of the OPC UA server	For CPUs as of FW version V4.1, the security policy "No security" is deactivated by default. The information on the individual security policies has been updated.	Section Handling client and server certificates (Page 255)
Managing certificates of OPC UA clients at runtime	With CPUs as of FW version V4.1, you can manage the certificates of the OPC UA client at runtime.	Section Handling client certificates during runtime (Page 371)
Enabling/disabling IP forwarding via data record	You can activate IP forwarding by writing a data record, e.g. during commissioning, and deactivate it during operation without having to change the hardware configuration of the CPU in STEP 7.	Section Enabling and disabling IP forwarding (Page 409)
Increased number of method calls for OPC UA client instructions	With CPUs as of FW version V4.1, you can use a higher number of method calls for OPC UA client instructions.	Section Number of client instructions that can be used simultaneously (Page 349)
GDS (certificate management at runtime) for S7-1500R/H	With R/H CPUs as of FW version V4.1, you can use the certificate management services of the OPC UA server and transfer certificates at runtime. The following elements can be updated automatically via GDS Push Management functions: • OPC UA server certificate • Trust lists • Certificate Revocation Lists (CRL) • Web server certificate	Section Using an OPC UA server in an S7-1500R/H system (Page 459)

What's new in the Communication Function Manual, Edition 11/2024 as compared to Edition 11/2023

What's new?	What are the customer benefits?	Where can I find the information?
Table for communication protocols and port numbers used in Ethernet communication interface modules	Information on protocols and ports used by interface modules. You can see at first glance which default settings apply. This allows you to specifically adjust only those settings that are relevant to your application.	Section Communications protocols and port numbers used for Ethernet communication (Page 35)
OPC UA: Increased configuration limits for the following S7-1500 CPUs as of FW version V4.0 • CPU 151x(F)-3 PN • CPU 151xT(F)-3 PN	The S7-1500 CPUs 151x(F)-3 PN and 151xT(F)-3 PN from FW version V4.0 allow the creation of a larger number of nodes for server interfaces and a larger number of server methods. In addition, the performance for read, write and subscriptions has been improved.	Equipment Manual of the respective CPU
OPC UA: Simultaneous receipt of messages in multiple languages	For S7-1500 CPUs, OPC UA clients as of firmware V4.0 can, for example, select one of the available languages for messages. In addition, an OPC UA client can request the message texts in all three active project languages simultaneously. For example, the messages are collected on a central server so that the messages can be evaluated by people in different languages.	Section Simultaneous receipt of messages in multiple languages (Page 327)

What's new?	What are the customer benefits?	Where can I find the information?
OPC UA: Role-based security for S7-1500 CPUs as of FW version V4.0	With the implementation of the role-based concept for the S7-1500 CPUs as of FW version V4.0, the OPC UA server can manage in detail the access of specific OPC UA clients to the address space.	Section Role-based security in OPC UA (Page 210)
OPC UA: Support of the "Transfer Subscription" function for S7-1500	The "Transfer Subscription" function is available for S7-1500 CPUs as of version V3.1.4 to support applications for load distribution on different OPC UA clients. With this, a subscription can be transferred to another OPC UA client. It is not necessary to configure the function.	Section Using the TransferSubscription service (Page 254)

What's new in the Communication Function Manual, Edition 11/2023 as compared to Edition 11/2022?

What's new?	What are the customer benefits?	Where can I find the information?
"Industrial cybersecurity" section	Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities. The section contains the following information: • Basic information on the subject of industrial cybersecurity • Measures to protect individual components and the entire system against manipulation and unwanted access.	Industrial cybersecurity (Page 25)
Revision of the tables for communication protocols and port numbers used in Ethernet communication	Updated information on protocols and ports used. You can see at first glance which default settings apply. This allows you to specifically adjust only those settings that are relevant to your application.	Communications protocols and port numbers used for Ethernet communication (Page 35)
Updated information about the connection resources of the CPU and HMI.	Updated information on the following connection resources: • Maximum number of connection resources supported for some CPU types • Maximum occupied connection resources for different HMI devices	Connection resources (Page 421)
Expanding the redundant system with communications processors	As of STEP 7 V19, you can expand an S7-1500R/H redundant system as of FW version V3.1 with the CP 1543-1 communications processors.	System IP addresses for communications processors (Page 442).
Secure Open User Communication with the redundant system	As of STEP 7 V19, an S7-1500R/H redundant system FW version V3.1 and higher also supports Secure Open User Communication.	Open User Communication with the redundant system S7-1500R/H (Page 452)

What's new in the Communication Function Manual, Edition 11/2022 as compared to Edition 05/2021?

What's new?	What are the customer benefits?	Where can I find the information?
Revision of the tables for communication protocols and port numbers used in Ethernet communication	Updated information on protocols and ports used. You can see at first glance which default settings apply. This allows you to specifically adjust only those settings that are relevant to your application.	Communications protocols and port numbers used for Ethernet communication (Page 35)
Activate / Deactivate the SNMP	Depending on the FW version of the S7-1500 CPUs, the SNMP is activated or deactivated in the default settings. You can change the default settings as required.	SNMP (Page 117)
Revision of the virtual interface for IP-based applications	With a CP 1543-1 with firmware version V3.0 or higher, the internal CP firewall is available. This is used to secure data traffic via the virtual interface.	Virtual interface for IP-based applications (Page 417)
OPC UA server: Reading the diagnostics status of the own address space	By using the OPC UA instruction for reading ("OPC_UA_ReadList"), the own namespace of the OPC UA Server can be accessed. This makes it possible to read out the status of the own OPC UA server as well as the connections of OPC UA clients, the session as well as the subscriptions and to react to them in the user program. This allows connection problems to be quickly detected, for example, and plant availability to be increased.	Running diagnostics for OPC UA servers in the program (Page 336)
OPC UA server: Time stamping of the source time of nodes	By using the OPC UA instruction for writing ("OPC_UA_WriteList"), it is possible to change the "SourceTimestamp" as well as the status code of an OPC UA variable (node). This makes it possible to distinguish between the "Source" and "Server" time as of V18.	Client accesses and local accesses to the OPC UA server (Page 231)
OPC UA GDS mechanism: Now also usable for Web server certificates	The Web server certificate for HTTPS communication can now also be managed via the OPC UA GDS mechanism, without separate download of the hardware configuration.	What you should know about the certificate management (Page 62) Automated certificate management with GDS (Page 193)

What's new in the Communication Function Manual, Edition 05/2021 as compared to Edition 11/2019?

What's new?	What are the customer benefits?	Where can I find the information?
Improved security for SIMATIC PG/HMI communication	• Allows unique identification of each PLC based on individual certificates • Provides additional confidentiality protection through encrypted communication • Protection of the configuration data through individual passwords	Secure PG/HMI communication (Page 106)
Security wizard for new PLC security mechanisms	• Quick and easy configuration of the new security mechanisms of the PLC in one operation • Supporting information to select suitable settings for own application	Protection of confidential configuration data (Page 76)

What's new?	What are the customer benefits?	Where can I find the information?
Certificate management via OPC UA Global Discovery Server (GDS)	• Certificate update during runtime • Support of CRLs • Access protection for certificate management	Certificate management via Global Discovery Server (GDS) (Page 193)
Transferring CPU alarms to OPC UA clients	• Subscriptions allow clients to subscribe to CPU alarms as "Alarms and Conditions" from the OPC UA server of the CPU. • Program messages including associated values are made available by the OPC UA server • Alarms requiring acknowledgment can be acknowledged by the OPC UA client (can be disabled) • An alarm burst is displayed as "overload" and clients can be reloaded with the refresh method	Providing alarms on the OPC UA server (Page 311)
Dynamic assignment of the network configuration with DHCP	Deployment of the CPU in IT managed networks using the following functions: • Connection of the CPU to an existing network without additional manual configuration of the network interface • Request for network parameters for the CPU according to RFC 2131 from a DHCPv4 server (IP address and subnet mask, default IP router address and further optional network parameters such as DNS and NTP server addresses)	Addressing via DHCP (Page 384)
Name-based addressing with DNS	• DNS server addresses can be obtained from the CPU via DHCP • The CPU can obtain host and domain names from a DHCP server for applications that are implemented with OPC UA or (Secure) OUC. • The CPU may transfer configured host or domain names to DHCP servers coupled with DNS servers for dynamic matching (Dynamic DNS). • The NTP client of the CPU can address NTP servers with names • Network parameters can be written with the new "CommConfig" instruction, for example, IP address parameters, DNS server, host and domain name	DHCP with DNS (Page 388)

What's new in the Communication Function Manual, Edition 11/2019 as compared to Edition 10/2018?

What's new?	What are the customer benefits?	Where can I find the information?
IP forwarding	Simple access from the control level to the field level for configuration and parameter assignment of devices, e.g. via PDM or Web browser.	IP forwarding (Page 402)
OPC UA server expansion	For S7-1500 CPUs as of firmware V2.8 and TIA Portal version 16, with a corresponding Runtime license, you can benefit from the following expansions of the integrated OPC UA server:	Section OPC UA communication (Page 165)

What's new?	What are the customer benefits?	Where can I find the information?
	• Improved diagnostics: The OPC UA user receives information on the status of the OPC UA server via alarms in the diagnostics buffer, an OPC UA category in the Online & Diagnostics area of TIA Portal as well as an improved connection resources display. • Download behavior: In RUN mode, the OPC UA server only performs a restart during download from the TIA Portal when the newly downloaded data has an effect on the data management of the OPC UA server. • Server interface modeling: It is now possible in the TIA Portal to model server interfaces or import OPC UA Companion Specifications and map them to the PLC data management.	

What's new in the Communication Function Manual, Edition 10/2018 as compared to Edition 12/2017?

What's new?	What are the customer benefits?	Where can I find the information?
Description of communication with the S7-1500R/H redundant system	You receive information on the particularities of communication with the S7-1500R/H redundant system	Section Communication with the redundant system S7-1500R/H (Page 435)
Scope of the Function Manual expanded to include the S7-1500R/H redundant system	Functions with which you are familiar from the SIMATIC S7-1500 automation system are implemented for the S7-1500R/H redundant system.	S7-1500R/H redundant system System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833)

What's new in the Communication Function Manual, Edition 12/2017 compared to Edition 09/2016

What's new?	What are the customer benefits?	Where can I find the information?
OPC UA Companion Specification	Through OPC UA Companion Specification, methods can be specified in a uniform and manufacturer-neutral way. Using these specified methods, you can easily integrate devices from various manufacturers into the plant and the production processes.	Section OPC UA server interface configuration (Page 270)
Setting up a secure connection to a mail server over the CPU interface	You can set up a secure connection to a mail server without additional hardware.	Section Secure OUC via e-mail (Page 103)
Secure communication over Modbus TCP	You can establish secure TCP connections between a Modbus TCP client and a Modbus TCP server.	Section Secure OUC with Modbus TCP (Page 101)

What's new in the Communication Function Manual, Edition 09/2016 compared to Edition 12/2014

What's new?	What are the customer benefits?	Where can I find the information?
OPC UA server	OPC UA is a uniform standard for data communication and is independent of any particular operating system platforms. OPC UA uses integrated safety mechanisms on various automation systems, for example with data exchange, at application level, for the legitimation of the user. The OPC UA server provides a large amount of data: • Values of PLC tags that clients can access • Data types of these PLC tags • Information about the OPC UA server itself and the CPU In this way, clients can gain an overview of the tag management and can read and write values.	Section OPC UA communication (Page 165)
Secure Open User Communication	Secure data exchange with other devices.	Section Secure Open User Communication (Page 88)
Certificate handling in STEP 7	You can manage certificates for the following applications in STEP 7: • OPC UA server • Secure Open User Communication • Web server of the CPU	Section Certificate management with TIA Portal (Page 63)
Deactivating SNMP for the CPU	You can deactivate SNMP for the CPU. This can make sense under certain conditions, for example if the security guidelines in your network do not permit SNMP.	Section SNMP (Page 117)

Conventions

STEP 7: We refer to "STEP 7" in this documentation as a synonym for the configuration and programming software "STEP 7 as of V12 (TIA Portal)".

Due to continuous controller functions, the term "S7-1500 CPUs" also usually refer to the CPU variants S7-1500F, S7-1500T, S7-1500TF, S7-1500C, S7-1500R/H, S7-1500pro, ET200SP, S7-1500 Software Controller, as well as SIMATIC Drive Controller. Variations arise due to different designs and applications between Advanced Controllers, Distributed Controllers, and Software Controllers.

This documentation contains pictures of the devices described. The figures may differ slightly from the device supplied.

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product, on handling of the product and on the section of the documentation to which you should pay particular attention.

1.1 SiePortal

You can find current information on the following topics quickly and easily here:

- **Catalog and ordering system**
  Ordering system for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).
- **Product support**
  All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.
- **Application examples**
  Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.
- **Services**
  Information about Industry Services, Field Services, Technical Support, spare parts and training offers.
- **Forums**
  For answers and solutions concerning automation technology.
- **mySiePortal**
  Your personal work area in the SiePortal for notifications, support requests, and configurable documents.

This information is provided by SiePortal on the Internet (https://sieportal.siemens.com/).

1.2 Function Manuals documentation guide

1.2.1 Information classes Function Manuals



The documentation for the SIMATIC S7-1500 automation system, for the 1513/1516pro-2 PN, SIMATIC Drive Controller CPUs based on SIMATIC S7-1500 and the SIMATIC ET 200MP, ET 200SP, ET 200AL and ET 200eco PN distributed I/O systems is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742705).

Basic information



The system manuals and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500, SIMATIC Drive Controller, ET 200MP, ET 200SP, ET 200AL and ET 200eco PN systems. Use the corresponding operating instructions for 1513/1516pro-2 PN CPUs.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- Getting Started S7-1500
- System manuals
- Operating instructions ET 200pro and 1516pro-2 PN CPU
- Online help TIA Portal

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment manuals for CPUs
- Equipment manuals for interface modules
- Equipment manuals for digital modules
- Equipment manuals for analog modules
- Equipment manuals for communication modules
- Equipment manuals for technology modules
- Equipment manuals for power supply modules
- Equipment manuals for BaseUnits

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC Drive Controller and the S7-1500 automation system.

Examples:

- Function Manual Diagnostics
- Function Manual Communication
- Function Manuals Motion Control
- Function Manual Web Server
- Function Manual Cycle and Response Times
- PROFINET Function Manual
- PROFIBUS Function Manual

Product Information

Changes and supplements to the manuals are documented in a Product Information. The Product Information takes precedence over the device and system manuals.

You will find the latest Product Information on the Internet:

- S7-1500/ET 200MP (https://support.industry.siemens.com/cs/de/en/view/68052815)
- SIMATIC Drive Controller (https://support.industry.siemens.com/cs/de/en/view/109772684/en)
- Motion Control (https://support.industry.siemens.com/cs/de/en/view/109794046/en)
- ET 200SP (https://support.industry.siemens.com/cs/de/en/view/73021864)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109765611)

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- S7-1500/ET 200MP/SIMATIC Drive Controller (https://support.industry.siemens.com/cs/ww/en/view/86140384)
- ET 200SP (https://support.industry.siemens.com/cs/ww/en/view/84133942)
- ET 200AL (https://support.industry.siemens.com/cs/ww/en/view/95242965)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109781058)

1.2.2 Basic tools

Tools

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet. (https://support.industry.siemens.com/cs/ww/en/view/109767888)

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities on various SIMATIC S7 stations as bulk operations independent of TIA Portal.

The SIMATIC Automation Tool offers a wide range of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Assignment of addresses (IP, subnet, Gateway) and device name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization through LED flashing
- Reading out of CPU error information
- Reading the CPU diagnostic buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/98161300)

PRONETA

SIEMENS PRONETA (PROFINET network analysis) is a commissioning and diagnostic tool for PROFINET networks. PRONETA Basic has two core functions:

- In the network analysis, you get an overview of the PROFINET topology. Compare a real configuration with a reference installation or make simple parameter changes, e.g. to the names and IP addresses of the devices.
- The "IO test" is a simple and rapid test of the wiring and the module configuration of a plant, including documentation of the test results.

You can find SIEMENS PRONETA Basic on the Internet:
(https://support.industry.siemens.com/cs/ww/en/view/67460624)

SIEMENS PRONETA Professional is a licensed product that offers you additional functions. It offers you simple asset management in PROFINET networks and supports operators of automation systems in automatic data collection/acquisition of the components used through various functions:

- The user interface (API) offers an access point to the automation cell to automate the scan functions using MQTT or a command line.
- With PROFIenergy diagnostics, you can quickly detect the current pause mode or the readiness for operation of devices that support PROFIenergy and change these as needed.
- The data record wizard supports PROFINET developers in reading and writing acyclic PROFINET data records quickly and easily without PLC and engineering.

You can find SIEMENS PRONETA Professional on the Internet.
(https://www.siemens.com/proneta-professional)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

1.2.3 S7 Port Configuration Tool (S7-PCT)

SIMATIC S7-PCT

The Port Configuration Tool (PCT) is a PC-based software for the parameter assignment of Siemens IO-Link Master modules and IO-Link devices from any manufacturer.

You integrate IO-Link-devices using the standardized device description "IODD", which you get from the respective device manufacturer. S7-PCT supports version 1.0 and V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link Master from STEP 7. When STEP 7 is not used or the IO-Link Master is not operated on a SIMATIC controller, "standalone"-operation is also possible.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

1.2.4 S7 Failsafe Configuration Tool (S7-FCT)

SIMATIC S7-FCT

Failsafe Configuration Tool (FCT) enables you to GSD configure the following devices in third-party engineering systems:

- Selected, functionally fail-safe SIMATIC I/O devices
- Functionally fail-safe SIRIUS ACT PROFINET interfaces

The engineering system must meet the following requirements for this:

- Support of the CPD system integration acc. to "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO"
- TCI implementation to Conformance Class C3

Additional information on S7-FCT can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109762827).

1.2.5 MultiFieldbus Configuration Tool (MFCT)

MultiFieldbus Configuration Tool

MultiFieldbus Configuration Tool (MFCT) is a PC-based software and supports the configuration of MultiFieldbus- and DALI-devices. In addition, the MFCT offers convenient options for mass firmware updates of ET 200 devices with MultiFieldbus- support and reading service data for many other Siemens devices.

Functional scope of the MFCT

- MultiFieldbus configuration:
  Engineering, configuration and diagnostics of MultiFieldbus-devices, provision of the required project files (project, UDT-, CSV- and EDS-file), transfer/export of the files to device and/or data memory.
- DALI configuration:
  Device selection and online configuration of DALI devices.

- TM FAST:
  Generation and download of FPGA-UPD- and FPGA-DB-files.
- Maintenance:
  Topology scan of a Ethernet network, reading of service data, parameter assignment and firmware update.
- Settings:
  Language switching German / English, network scanner speed, setting of the network adapter, installation of GSDML-and EDS-files.

System/installation requirements for MFCT

The MFCT runs under Microsoft Windows and does not require installation or administrator rights.

For MFCT you must also install the following software:

- Microsoft .NET Framework 4.8 (You can find an Offline Installer on the Internet. (https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0))
- NPcap from directory "Misc"
- PG/PC interface from directory "Misc"
- Microsoft C++ Redistributable for x86-systems (you can find the installation data for download on the Internet. (https://aka.ms/vs/15/release/vc_redist.x86.exe))

The download of the tool and further information as well as documentation on the individual functions of the MFCT can be found on the Internet.
(https://support.industry.siemens.com/cs/de/en/view/109773881)

1.2.6 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International
(https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.

Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Security information

2

2.1 General security information

Note the security-relevant information provided in the corresponding system manual.
You can find information relevant to cybersecurity in the section Industrial cybersecurity (Page 25).

Industrial cybersecurity 3

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual and the Security guidelines for SIMATIC HMI devices (https://support.industry.siemens.com/cs/us/en/view/109481300) for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to the communication of your SIMATIC system.

NOTE

Security-relevant changes to software or devices are documented in the section Introduction (Page 9).

3.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

3.2 Security-relevant information in this manual

Observe all security-relevant notes on topics in this Communication manual.

Security-relevant notes on ...	Section
Interfaces	Product overview (Page 27)
Ports and protocols	Overview of communication options (Page 33) Communications protocols and port numbers used for Ethernet communication (Page 35)
Secure communication	Secure communication (Page 51)
Activate/deactivate services	Activating and deactivating SNMP (Page 117) Addressing via DHCP (Page 384) IP forwarding (Page 402)
Security functions of OPC UA communication (authentication, certificates, user creation and roles, secure message transmission)	OPC UA communication (Page 165)
Activating security functions in the communications modules	Virtual interface for IP-based applications (Page 417)
Communication with the redundant system S7-1500R/H	Communication with the redundant system S7-1500R/H (Page 435)
Protection by Industrial Ethernet Security with CP 1543-1	Industrial Ethernet Security with CP 1543-1 (Page 475)
Secure PG/HMI communication	Secure PG/HMI communication (Page 106)
Protection of confidential data	Protection of confidential configuration data (Page 76)
Protection against tampering during loading and unauthorized access	PG communication (Page 125)

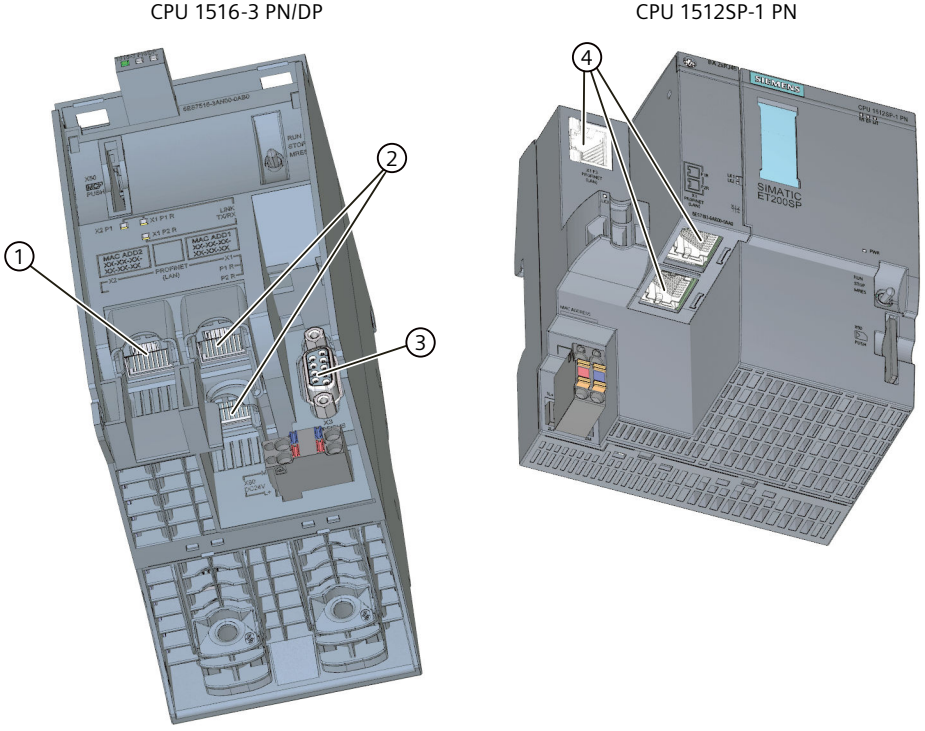
Product overview

4

PC systems, CPUs, communications modules and processors, and interface modules of the S7-1500 and ET 200 systems provide you with interfaces for communication via PROFINET, PROFIBUS and point-to-point connections.

CPUs, communications modules and communications processors

PROFINET and PROFIBUS DP interfaces are integrated in the S7-1500 CPUs. The CPU 1516-3 PN/DP for example has 2 PROFINET interfaces and 1 PROFIBUS DP interface. Other PROFINET and PROFIBUS DP interfaces are available by using communications modules (CM) and communications processors (CP).

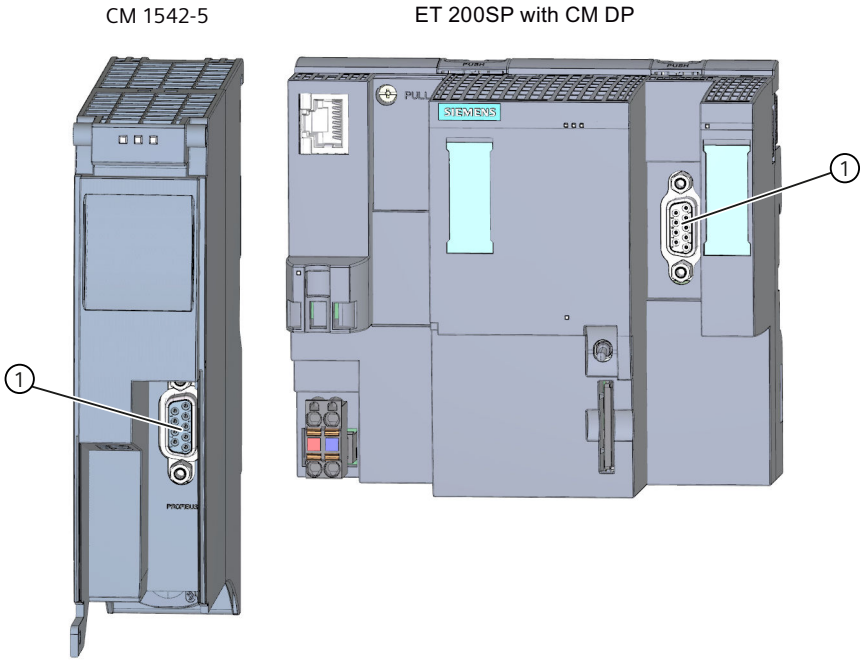


① PROFINET interface (X2) with 1 port
② PROFINET interface (X1) with 2-port switch
③ PROFIBUS DP interface (X3)
④ PROFINET interface (X1) with 3-port switch

Figure 3-91 Interfaces of the CPU 1516-3 PN/DP and CPU 1512SP-1 PN

Interfaces of communications modules

Interfaces of communications modules (CMs) extend the interfaces of CPUs (for example, the communication module CM 1542-5 adds a PROFIBUS interface to S7-1500 automation system).

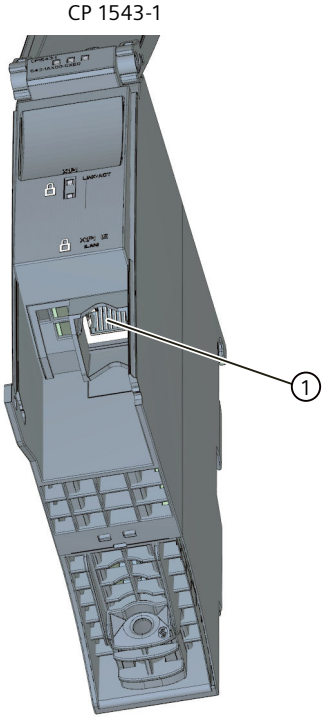


① PROFIBUS DP interface

Figure 3-92 PROFIBUS DP interface of the CM 1542-5 and CM DP (to an ET 200SP CPU)

Interfaces of communications processors

Interfaces of communication processors (CP) offer additional functionality to what is provided by the integrated interfaces of the CPUs. CPs allow special applications, for example the CP 1543-1 provides security functions for protecting Industrial Ethernet networks via its Industrial Ethernet interface.



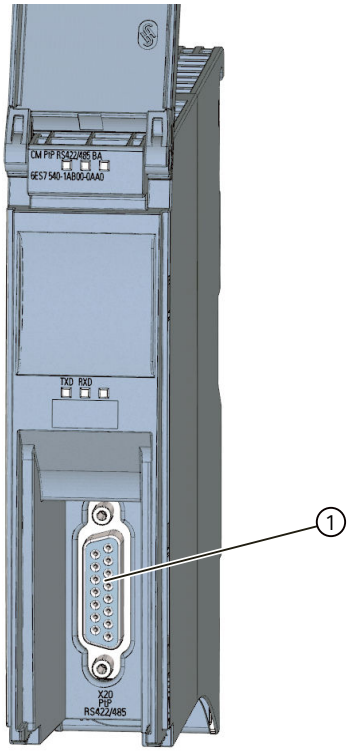
① Industrial Ethernet interface

Figure 3-93 Industrial Ethernet interface of the CP 1543-1

Interfaces of communications modules for point-to-point connections

The communication modules for point-to-point connections provide communication via their RS 232-, RS 422- and RS 485 interfaces, for example, Freeport or Modbus communication.

CM PtP RS422/485 BA

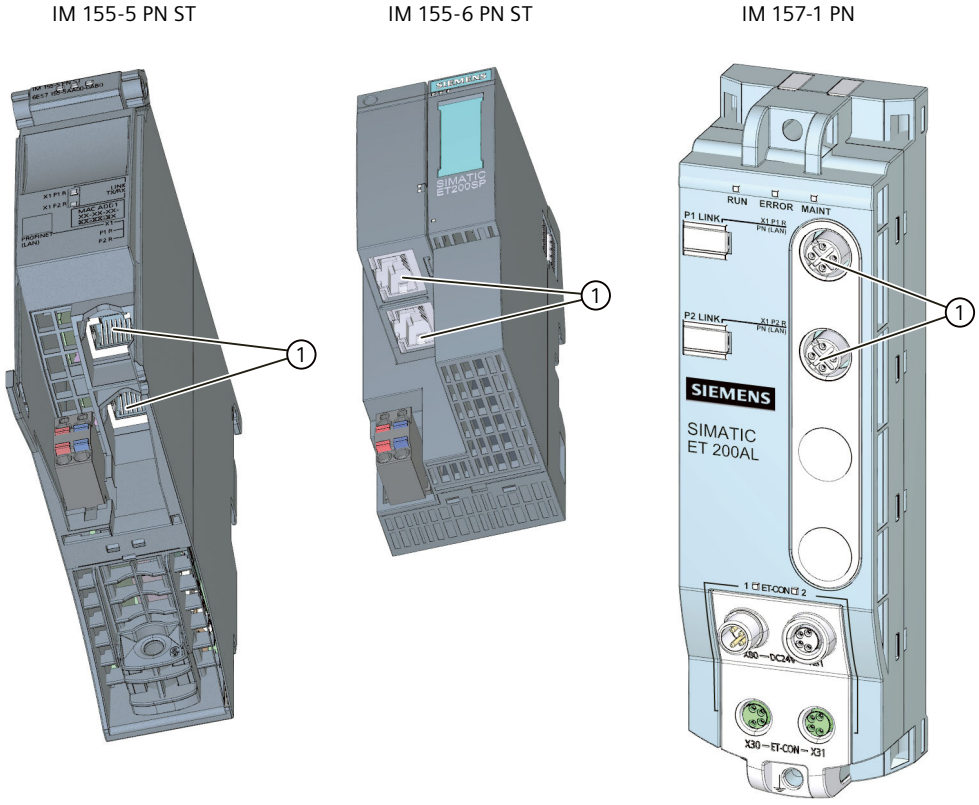


① Interface for point-to-point connections

Figure 3-94 Example of interface for point-to-point connection at the CM PtP RS422/485 BA

Interfaces of interface modules

PROFINET and PROFIBUS DP interfaces of interface modules (IM) are used to connect the ET 200 distributed I/O systems to PROFINET or PROFIBUS of the higher-level IO controller or DP master.



① PROFINET interface with 2-port switch

Figure 3-95 PROFINET interfaces IM 155-5 PN ST (ET 200MP), IM 155-6 PN ST (ET 200SP), and IM 157-1 PN (ET 200AL)

Deactivating the port of a PROFINET interface

Activated ports represent a potential risk of unauthorized access to the network and programs.
To minimize the risk, deactivate all unused ports.
Procedure:

1. Select the port of the PROFINET interface in the device view of the CPU/IM in STEP 7.
2. In the Inspector window, navigate to "Advanced options > Port [x]> Port options > Activate".
3. Clear the "Activate" check box.

At least one port of a CPU/IM remains activated.

Communications services

The communications services described below use the interfaces and communication mechanisms provided by the system via CPUs, communication modules and processors.

Communications services

5

5.1 Overview of communication options

Overview of communications options

The following communications options are available for your automation task.

Table 3-14 Communications options

Communications options	Functionality	Via interface:		
		PN/IE[1]	DP	serial
PG communication[2]	On commissioning, testing, diagnostics	X	X	-
HMI communication[2]	On operator control and monitoring	X	X	-
Open communication via TCP/IP[2]	Data exchange via PROFINET/Industrial Ethernet with TCP/IP Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Open communication using ISO-on-TCP[2]	Data exchange via PROFINET/Industrial Ethernet with ISO-on-TCP Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Open communication via UDP[2]	Data exchange via PROFINET/Industrial Ethernet with UDP Instructions: • TSEND_C/TRCV_C • TUSEND/TURCV • TCON • T_DISCON	X	-	-
Open communication via ISO (only CPs with PROFINET/Industrial Ethernet interface)	Data exchange via PROFINET/Industrial Ethernet with the ISO protocol Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Open communication with FDL (only CM 1542-5 as of firmware V2.0)	Data exchange via PROFIBUS with the FDL protocol Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TUSEND/TURCV • TCON • T_DISCON	-	X	-

1 IE - Industrial Ethernet

2 Observe the special characteristics for S7-1500R/H

3 Only via internal PROFINET interface of the CPU and via Ethernet interface CP 1543 1 with activated "Access to PLC via communication module" function

Communications options	Functionality	Via interface:		
		PN/IE[1]	DP	serial
OPC UA server[3]	Data exchange with OPC UA clients	X	-	-
Communication via Modbus TCP	Data exchange via PROFINET with Modbus TCP protocol Instructions: • MB_CLIENT • MB_SERVER	X	-	-
Email	Sending process alarms via email Instruction: • TMAIL_C	X	-	-
FTP (only CPs with PROFINET/Industrial Ethernet interface)	File management and file access via FTP (File Transfer Protocol); CP can be FTP client and FTP server Instruction: • FTP_CMD	X	-	-
Fetch/Write (only CPs with PROFINET/Industrial Ethernet interface)	Server services via TCP/IP, ISO-on-TCP and ISO Via special instructions for Fetch/Write	X	-	-
S7 communication	Data exchange via PROFINET/PROFIBUS with the S7 protocol. Instructions: • PUT/GET • BSEND/BRCV • USEND/URCV	X	X	-
Serial point-to-point connection	Data exchange via point-to-point with Freeport, 3964(R), USS or Modbus protocol Via special instructions for PtP, USS or Modbus RTU	-	-	X
Web server	Data exchange via HTTP(S), for example for diagnostics	X	-	-
SNMP (Simple Network Management Protocol)	For monitoring and error recognition of IP networks, possibly parameterization of the IP network components via standard SNMP protocol	X	-	-
Time-of-day synchronization	Via PN/IE interface: CPU is NTP client (Network Time Protocol)	X	-	-
	Via DP interface: CPU/CM/CP is time-of-day master or time slave	-	X	-

1 IE - Industrial Ethernet

2 Observe the special characteristics for S7-1500R/H

3 Only via internal PROFINET interface of the CPU and via Ethernet interface CP 1543 1 with activated "Access to PLC via communication module" function

Information on S7-1500R/H

You can find information on the communication options with the S7-1500R/H redundant system in the section Communication with the redundant system S7-1500R/H (Page 435) and in the S7-1500R/H System Manual (https://support.industry.siemens.com/cs/us/en/view/109754833).

More information

- An application example for the configuration of the TLS-based PG/HMI communication and protection of confidential configuration data of the CPU can be found in this Application example (https://support.industry.siemens.com/cs/ww/en/view/109798583).
- A general application example for CPU-CPU communication with SIMATIC controllers (compendium) can be found in this application example (https://support.industry.siemens.com/cs/ww/en/view/20982954).
- A TIA library "LOpcUa", which provides you with function blocks for the implementation of OPC UA PubSub for SIMATIC S7-1500, can be found in this Application example (https://support.industry.siemens.com/cs/ww/en/view/109782455).

- This FAQ (https://support.industry.siemens.com/cs/ww/en/view/102420020) describes how to configure fetch/write communication via CP1543-1 with S7-1500.
- More information about the Fetch/Write services is available in the STEP 7 online help.

- You can find more information on the PtP connection in the function manual CM PtP - Configurations for Point-to-Point Connections (https://support.industry.siemens.com/cs/us/en/view/59057093).
- You will find the description of the web server functionality in the function manual Web server (https://support.industry.siemens.com/cs/us/en/view/59193560).

- You can find general information about the standard protocol SNMP on the Service & Support pages on the Internet (https://support.industry.siemens.com/cs/us/en/view/15166742). Answers to the question of which SNMP requests support S7-1500 CPUs and S7-1200 CPUs can be found in this FAQ (https://support.industry.siemens.com/cs/at/en/view/79993228).
- You will find information about time-of-day synchronization in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/86535497).

5.2 Communications protocols and port numbers used for Ethernet communication

This section provides an overview of the supported protocols and port numbers used for communication over PN/IE interfaces. For each protocol the address parameters, the respective communications layer as well as the communications role and the communications direction are specified.

This information makes it possible to match the security measures for protection of the automation system to the used protocols (for example firewall). Because the security measures are limited to Ethernet or PROFINET networks, the tables do not include PROFIBUS protocols.

NOTE

Port numbers used

The specified port numbers are the standard port numbers used by S7-1500 CPUs, communications modules and ET 200 interface modules. Many communication protocols and implementations enable you to use other port numbers.

The following tables show the different layers and protocols used in S7-1500 CPUs, S7-1500 communications modules and ET 200 interface modules.

Layers and protocols of the S7-1500 CPUs and Software Controllers (via PROFINET interface of the CPU)

The following table shows the protocols supported by S7-1500 CPUs, ET 200SP CPUs, and the 1513/1516pro-2 PN CPUs. The S7-1500 Software Controllers also support the protocols listed in the following table for the Ethernet interfaces that are assigned to the Software Controller.

Table 3-15 Layers and protocols of the S7-1500 CPUs and Software Controllers (via PROFINET interface of the CPU)

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
PROFINET protocols				
DCP	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Discovery and Basic Configuration Protocol. DCP determines PROFINET devices and enables the basic settings.	Default: Up to FW version V3.0 enabled, as of FW version V3.1 write protection enabled. DCP does not allow DCP Set commands from the outside in write-protected mode during an active communication relationship. Function can be deactivated in the CPU properties by Boundary "End of detection of accessible nodes" of the interface.
DHCP Client	68	(4) UDP	Dynamic Host Configuration Protocol. The IP address suite is obtained from a DHCP server during the startup of the PROFINET interface.	Default: Deactivated. Can be changed in the CPU properties (as of FW version 2.9).
LLDP	Not relevant	(2) Ethertype 0x88CC (LLDP)	PROFINET Link Layer Discovery Protocol. LLDP determines and manages neighborhood relations between PROFINET devices.	Default: Activated. Send function can be deactivated by Boundary "End of topology discovery" in the CPU properties; readiness to receive remains active. LLDP uses the special multicast MAC address 01-80-C2-00-00-0E.
MRP	Not relevant	(2) Ethertype 0x88E3 (IEC 62493-2)	Media Redundancy Protocol. MRP enables control of redundant transmission paths in a ring topology.	Default: "Manager (Auto)". Can be changed in the CPU properties. If you configure the CPU and connect the PN interface with a subnet, the default setting in the TIA Portal is "Not device in the ring". MRP uses standard-compliant multicast MAC addresses.
PROFINET IO data	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Cyclic IO Data Transfer. With PROFINET IO telegrams, IO data is transferred cyclically between the PROFINET IO controller and IO devices via Ethernet.	Default: Deactivated. The protocol is only activated for PROFINET IO data traffic.
PROFINET Context Manager	34964	(4) UDP	PROFINET communication. Management of application and communication relationships between IO controller and IO devices.	Default: Activated (UDP port open). This function cannot be deactivated.

1 Note: OUC (Open User Communication) provides direct access to the UDP and TCP protocols. You must take into consideration the IANA (Internet Assigned Numbers Authority) port restrictions and definitions.

2 Do not use ports for OUC, which are already used by other protocols.

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
PTCP	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Precision Transparent Clock Protocol, based on IEEE 1588. PTCP provides a time delay measurement between RJ45 ports and thus the send clock and time synchronization.	Default: Deactivated. Can be activated by the following configurations: • IRT with a sync domain. • Port interconnection with a specified cable length. Function can be deactivated in the CPU properties by "End of sync domain" Boundary of the interface. PTCP uses standard-compliant multicast MAC addresses.
Connection-oriented communication protocols				
HTTP Server	80	(4) TCP	Hypertext Transfer Protocol. HTTP is used for communication with the CPU-internal web server.	Default: Deactivated. Can be enabled in the CPU properties. Requirement: Web server in the CPU properties is enabled.
HTTPS Server	443	(4) TCP	Hypertext Transfer Protocol Secure. HTTPS is used for communication with the CPU-internal Web server via Secure Socket Layer (SSL).	Default: Deactivated. Can be enabled in the CPU properties. Requirement: Web server in the CPU properties is enabled.
IGMPv2	Not relevant	(3) Network layer	Internet Group Management Protocol. IGMPv2 is a network protocol for the organization of multicast groups (UDP multicast only).	IGMPv2 is a functionality of the IP stack. This system function is activated by the multicast function.
ISO-on-TCP Server	102	(4) TCP	ISO-on-TCP protocol (according to RFC 1006). The S7 protocol uses ISO-on-TCP according to RFC 1006 for PG/HMI communication with the engineering system (TIA Portal).	Default: Activated. This function cannot be deactivated.
Modbus TCP Server / Client	502	(4) TCP	Modbus Transmission Control Protocol. Modbus/TCP is used by MB_CLIENT/MB_SERVER instructions in the user program.	Default: Deactivated. Can be activated via Modbus instructions in the user program.
NTP Client	49152 ... 65535	(4) UDP	Network Time Protocol. NTP is used for synchronization of the CPU system time with the time of an NTP server.	Default: Deactivated. Can be enabled in the CPU properties.
OPC UA Server / Client	4840	(4) TCP	Open Platform Communications Unified Architecture (based on TCP/IP protocol). A communication standard ranging from the enterprise level to the field level.	Default: Deactivated. Server and client function can be enabled in the CPU properties. Client access can be configured in the user program.

[1] Note: OUC (Open User Communication) provides direct access to the UDP and TCP protocols. You must take into consideration the IANA (Internet Assigned Numbers Authority) port restrictions and definitions.

[2] Do not use ports for OUC, which are already used by other protocols.

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
OUC[1] Secure OUC Server / Client	1 ... 1999 can be used to limited extent[2] 2000 ... 5000 Recommended As of FW version V3.0, the following applies to programmed and configured connections: 5001 ... 65535 can be used to limited extent[2]	(4) TCP (4) UDP (4) ISO-on-TCP (Port: 102)	Open User Communication (TCP/UDP). Secure Open User Communication (TLS). OUC instructions enable connection establishment, connection termination and data transfer via the user program.	Default: Deactivated. You activate the respective protocol with the corresponding Open User Communication instruction in the user program or with the configuration of connections in the network view. The following applies to FW versions lower than V3.0: • Programmed connections: 5001 ... 49152 • Configured connections: 5001 ... 65535
SMTP Client	25	(4) TCP	Simple Mail Transfer Protocol. SMTP is used for sending emails.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the user program.
SMTPS (SMTP over TLS) Client	465	(4) TCP	Simple Mail Transfer Protocol Secure. SMTP is used for sending emails over secure connections.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the user program.
SMTP with STARTTLS Client	25 587	(4) TCP	Simple Mail Transfer Protocol with the SMTP command "STARTTLS". SMTP is used for sending emails.	Default: Deactivated. Can be enabled via TMAIL_C instruction in the user program.
SNMP Agent	161	(4) UDP	Simple Network Management Protocol. SNMP is used for reading and setting of network management data (SNMP-managed objects) by the SNMP manager. The SNMP agent does not support traps.	Default: Activated up to FW version V2.9, deactivated as of FW version V3.0. Can be enabled via data record in the user program. Can be enabled in the CPU properties as of FW version V3.0. As of FW version V3.1, can additionally be enabled as write-protected in the CPU properties.
Syslog Client	6514 514	(4) TCP (4) UDP	System logging. Syslog is an IETF standard protocol (RFC 5424) for the transmission of events that a CPU detects.	Default: Deactivated. Can be enabled in the CPU properties. You can configure the forwarding of syslog messages to a syslog server in the CPU properties. The collection of system logging events within a CPU cannot be disabled as of FW version V3.1.

[1] Note: OUC (Open User Communication) provides direct access to the UDP and TCP protocols. You must take into consideration the IANA (Internet Assigned Numbers Authority) port restrictions and definitions.

[2] Do not use ports for OUC, which are already used by other protocols.

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
Reserved	49152 ... 65535	(4) TCP (4) UDP	If an application does not address a local port, then the CPU uses this port range for the active connection point. For connected IO devices, an IO controller opens a further port (client port) from this area for each protocol used. The port is selected at random.	-

1 Note: OUC (Open User Communication) provides direct access to the UDP and TCP protocols. You must take into consideration the IANA (Internet Assigned Numbers Authority) port restrictions and definitions.

2 Do not use ports for OUC, which are already used by other protocols.

Layers and logs of the S7-1500 Software Controller (via Ethernet interface on the Windows side)

The following table shows the protocols that are supported by the S7-1500 Software Controller via the Ethernet interfaces assigned by Windows.

Table 3-16 Layers and logs of the S7-1500 Software Controller (via Ethernet interface on the Windows side)

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Notes / default setting
PROFINET protocols				
DCP	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Discovery and Basic Configuration Protocol. DCP determines PROFINET devices and enables the basic settings.	Default: Enabled up to version V30.0. Write-protection enabled as of version V30.1 . DCP does not allow DCP Set commands from the outside in write-protected mode during an active communication relationship. Function can be disabled with Boundary "End of detection of accessible nodes" in the CPU properties.
DHCP Client	68	(4) UDP	Dynamic Host Configuration Protocol. The IP address suite is obtained from a DHCP server during the startup of the PROFINET interface.	Default: Deactivated. Can be changed in the CPU properties (as of FW version 2.9).
Connection-oriented communication protocols				
HTTP Server	Adjustable [1]	(4) TCP	Hypertext Transfer Protocol. HTTP is used for communication with the CPU-internal web server.	Default: Deactivated. Can be changed in the CPU properties. Adapt the port number to avoid conflicts with other web servers under Windows. If you use the Web server access of the S7-1500 Software Controller, you must enable the assigned port in the Windows firewall.

1 Default setting for Windows assigned interfaces: 81

2 Note: OUC (Open User Communication) provides direct access to the UDP and TCP protocols. You must take into consideration the IANA (Internet Assigned Numbers Authority) port restrictions and definitions.

3 Do not use ports for OUC, which are already used by other protocols.

4 Do not use ports for OUC, which are already used by other Windows applications.

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Notes / default setting
IGMPv2	Not relevant	(3) Network layer	Internet Group Management Protocol. IGMPv2 is a network protocol for the organization of multicast groups (UDP multicast only).	IGMPv2 is a functionality of the IP stack. This system function is activated by the multicast function.
ISO-on-TCP Server	102	(4) TCP	ISO-on-TCP protocol (according to RFC 1006). The S7 protocol uses ISO-on-TCP according to RFC 1006 for PG/HMI communication with the engineering system (TIA Portal).	Default: Deactivated.
OUC[2] and Secure OUC	1 ... 1999 can be used to limited extent[3, 4]	(4) TCP (4) UDP (4) ISO-on-TCP (Port: 102)	Open User Communication (TCP/UDP). Secure Open User Communication (TLS). OUC instructions enable connection establishment, connection termination and data transfer based on the socket layer.	Default: Deactivated. Can be enabled via data record in the user program. If you want to use OUC, you must activate the ports in the Windows Firewall.
	2000 ... 5000 recommended[4]			
	5001 ... 49151 can be used to limited extent[3, 4]			
SMTP Client	25	(4) TCP	Simple Mail Transfer Protocol. SMTP is used for sending emails.	Default: Deactivated. Can be activated by calling the block in the user program or as of version V3.0 via CPU settings.
Syslog Client	6514 514	(4) TCP (4) UDP	System logging. Syslog is an IETF standard protocol (RFC 5424) for the transmission of events that a CPU detects.	Default: Deactivated. Can be enabled in the CPU properties. You can configure the forwarding of syslog messages to a syslog server in the CPU properties. The collection of system logging events within a CPU cannot be disabled as of FW version V3.1.
Reserved	49152 ... 65535	(4) TCP (4) UDP	If the application does not specify the local port number, this dynamic port range is used for the active connection end point.	If you want to use this communication, you must activate the ports in the Windows Firewall.

1 Default setting for Windows assigned interfaces: 81

2 Note: OUC (Open User Communication) provides direct access to the UDP and TCP protocols. You must take into consideration the IANA (Internet Assigned Numbers Authority) port restrictions and definitions.

3 Do not use ports for OUC, which are already used by other protocols.

4 Do not use ports for OUC, which are already used by other Windows applications.

Layers and protocols of S7-1500 communications modules

The documentation for the protocols of S7-1500 communications modules (e.g. CP 1543-1) can be found here (https://support.industry.siemens.com/cs/ww/en/view/67700710).

Layers and protocols of interface modules

The following table shows the protocols supported by ET 200 interface modules. To find out which protocols your ET 200 interface module supports, refer to the technical specifications in the relevant equipment manual.

Table 3-17 Layers and protocols of the ET 200 interface modules

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
PROFINET protocols				
DCP	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Discovery and Basic Configuration Protocol. DCP determines PROFINET devices and enables the basic settings.	Default setting for supported interface modules if the higher-level IO controller also supports DCP: • Write-protection enabled DCP does not allow DCP Set commands from the outside in write-protected mode during an active communication relationship. Function can be deactivated in the properties of the PROFINET interface.
LLDP	Not relevant	(2) Ethertype 0x88CC (LLDP)	PROFINET Link Layer Discovery Protocol. LLDP determines and manages neighborhood relations between PROFINET devices.	Default: Activated. Send function can be deactivated by Boundary "End of topology discovery" in the properties of the PROFINET interface; readiness to receive remains active. LLDP uses the special multicast MAC address 01-80-C2-00-00-0E.
MRP	Not relevant	(2) Ethertype 0x88E3 (IEC 62493-2)	Media Redundancy Protocol. MRP enables control of redundant transmission paths in a ring topology.	Default: "Not device in the ring". Can be changed in the properties of the PROFINET interface. If you want to configure the interface module and activate MRP, assign the "Client" media redundancy role to the interface module. MRP uses standard-compliant multicast MAC addresses.
PROFINET IO data	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Cyclic IO Data Transfer. With PROFINET IO telegrams, IO data is transferred cyclically between the PROFINET IO controller and IO devices via Ethernet.	Default: Deactivated. Is activated indirectly as soon as the interface module receives a valid configuration.
PROFINET Context Manager	34964	(4) UDP	PROFINET communication. Management of application and communication relationships between IO controller and IO devices.	Default: Activated (UDP port open). This function cannot be deactivated.

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
PTCP	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Precision Transparent Clock Protocol, based on IEEE 1588. PTCP enables the following functions: • Time delay measurement between two ports • Send clock and time synchronization	Default setting for time delay measurement: Activated for supported interface modules. PTCP cannot be deactivated for time delay measurement. Default setting for send clock and time synchronization: Deactivated. Can be activated by the higher-level IO controller according to the configuration. PTCP uses standard-compliant multicast MAC addresses.
Connection-oriented communication protocols				
IGMPv2	Not relevant	(3) Network layer	Internet Group Management Protocol. IGMPv2 is a network protocol for the organization of multicast groups (UDP multicast only).	IGMPv2 is a functionality of the IP stack. This system function is activated by the multicast function.
MODBUS TCP Slave	502	(4) TCP	MODBUS Transmission Control Protocol.	Default: Deactivated. Can be activated via MultiFieldbus Configuration Tool (MFCT).
SNMP Agent	161	(4) UDP	Simple Network Management Protocol. SNMP is used for reading and setting of network management data (SNMP-managed objects) by the SNMP manager. The SNMP agent does not support traps.	Default setting for supporting interface modules: • Synchronize default values from IO controller • Deactivated
EtherNet/IP CIP	44818 (TCP) 2222 (UDP)	(4) TCP (4) UDP	The EtherNet/IP protocol and Common Industrial Protocol (CIP) protocols enable communication between interface modules and CPUs. EtherNet/IP use MultiFieldbus devices for data exchange. CIP Implicit Messaging is used for the continuous transmission of real-time data in time-critical applications. CIP Explicit Messaging is used for the targeted retrieval or transmission of configuration and diagnostic data.	Default: Deactivated. Can be activated via MultiFieldbus Configuration Tool (MFCT).
TCP/IP	Not relevant	(4) TCP	Transmission Control Protocol. TCP ensures a reliable connection between 2 communication partners.	Default: Activated. This function cannot be deactivated.
UDP	Not relevant	(4) UDP	User Datagram Protocol. UDP works without a connection and is based on the unsecured Internet Protocol (IP).	Default: Activated. This function cannot be deactivated.

Protocol / Role	Port number	(2) Link layer (4) Transport layer	Description / function	Default setting / notes
ARP	Not relevant	(2) Ethertype 0x0806	Address Resolution Protocol. Assignment of the IP addresses to the MAC addresses.	Default: Activated. This function cannot be deactivated.
IPv4	Not relevant	(3) Network layer	Internet Protocol Version 4. Identification of devices by IP addresses. IPv4 is used to send data packets from their origin to their destination.	Default: Activated. This function cannot be deactivated.
Reserved	49152 ... 65535	(4) TCP (4) UDP	If an application does not address a local port, then the CPU uses this port range for the active connection point. For connected IO devices, an IO controller opens a further port (client port) from this area for each protocol used. The port is selected at random.	-

5.3 Overview of connection resources

Connection resources

Some communications services require connections. Connections allocate resources on the CPUs, CPs and CMs involved (for example memory areas in the CPU operating system). In most cases one resource per CPU/CP/CM is allocated for a connection. In HMI communication, up to 3 connection resources are required per HMI connection.

The connection resources available depend on the CPU being used, the CPs and CMs and must not exceed a defined high limit for the automation system.

Available connection resources in a station

The maximum number of resources of a station is determined by the CPU.

Each CPU has reserved connection resources for PG, HMI and web server communication. In addition, there are available resources for other communication services, e.g. for SNMP, e-mail connections, HMI and S7 communication as well as for open communication.

When are connection resources allocated?

The time for allocation of connection resources depends on how the connection is set up, automatic, programmed or configured (see section Setting up a connection (Page 44)).

Additional information

You will find more detailed information on the allocation of connection resources and the display of connection resources in STEP 7 in the section Connection resources (Page 421).

5.4 Setting up a connection

Automatic connection

STEP 7 sets up a connection automatically (for example PG or HMI connection) if you have connected the PG/PC interface to an interface of the CPU physically and have made the interface assignment in STEP 7 in the "Go online" dialog.

Setting up a programmed connection

You set up the programmed connection in the program editor of STEP 7 in the context of a CPU by assigning instructions for communication, for example TSEND_C.

When specifying the connection parameters (in the Inspector window, in the properties of the instruction), you are supported by the easy-to-use user interface.

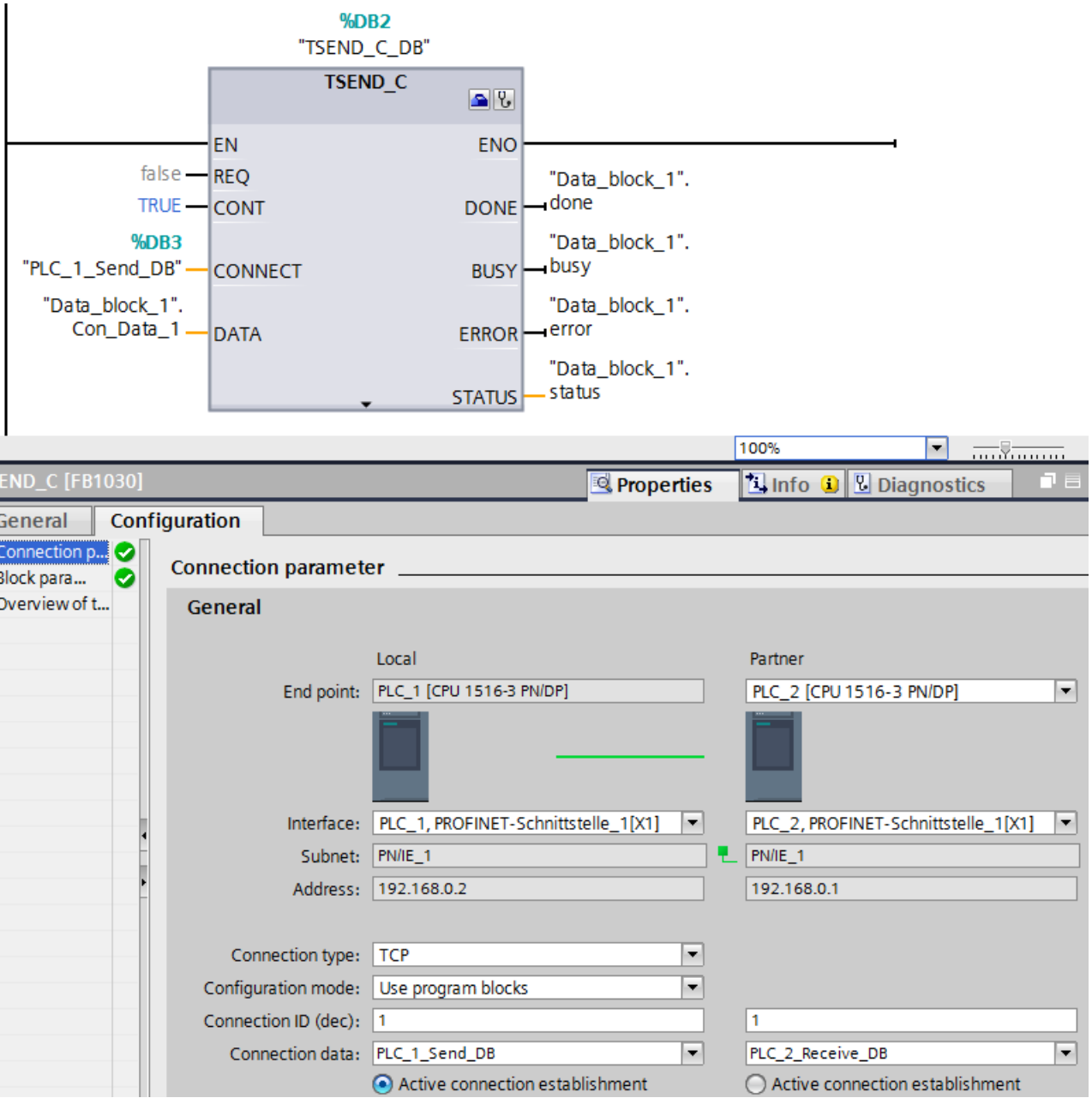


Figure 3-96 Programmed setup

Setting up a configured connection

You set up the configured connection in the network view of the Devices & networks editor of STEP 7 in the context of a CPU or a software controller.

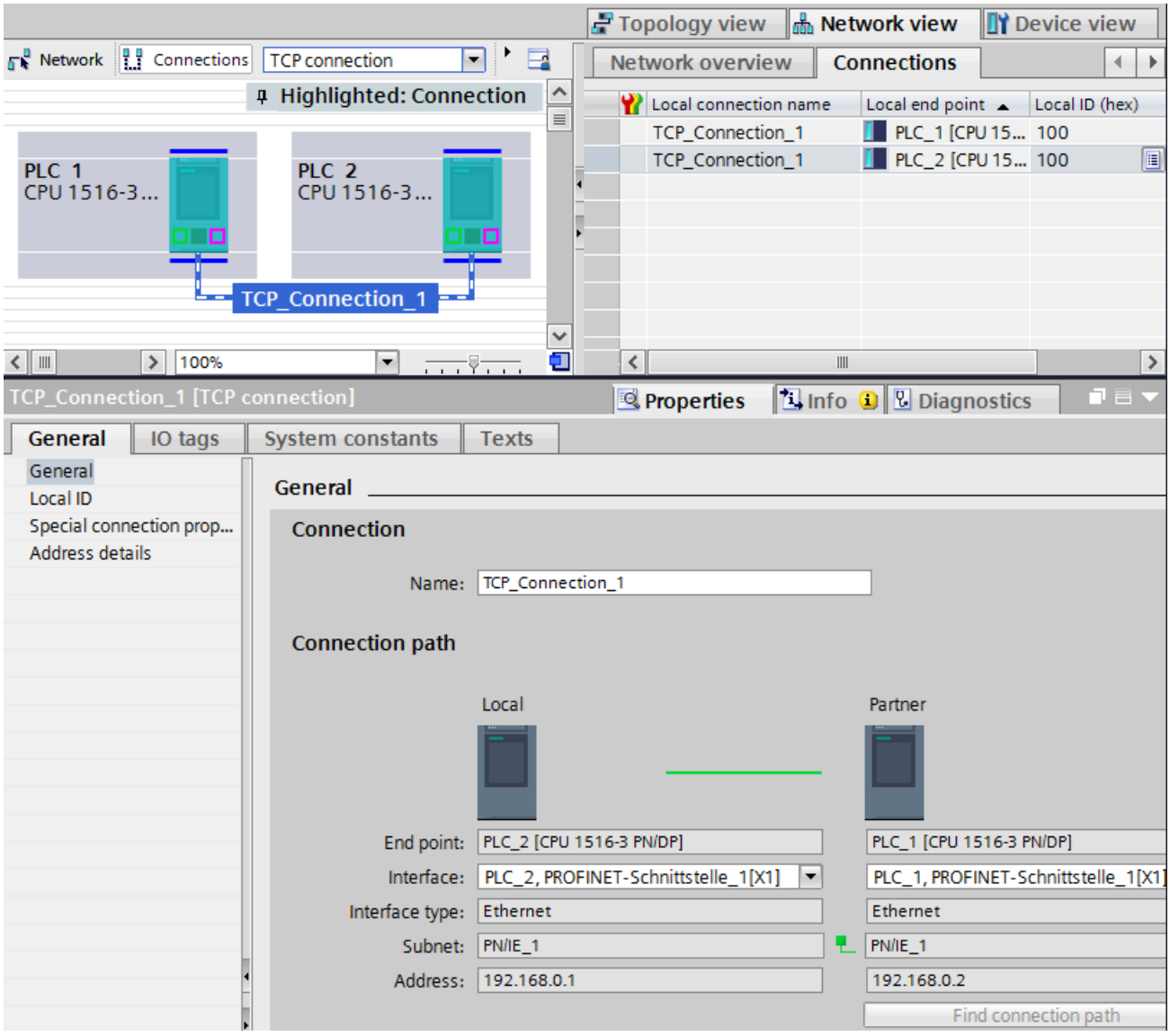


Figure 3-97 Configured setup

Effects on the connection resources of the CPU

You can often choose between a configured or a programmed connection. Programmed connection setup allows connection resources to be released following data transfer. Like routed connections, programmed connections are not guaranteed, meaning that they are only established when resources are available. With configured connection setup, the resource is available after download of the configuration until the configuration changes again. Corresponding resources are therefore reserved for connection establishment via

configured connections. The "Connection resources" table in the Inspector window of the CPU displays an overview of connection resources already used and those still available.

How do I set up a connection?

Table 3-18 Setting up the connection

Connection	Automatically	Programmed setup	Configured setup
Programming device connection	X	-	-
HMI connection	X	-	X
Web communication	X	-	-
OPC UA server communication	X	-	-
OPC UA client communication	-	X	-
Open communication via TCP/IP connection	-	X	X
Open communication via ISO-on-TCP connection	-	X	X
Open communication via UDP connection	-	X	X
Open communication via ISO connection	-	X	X
Open communication via FDL connection	-	X	X
Communication via Modbus TCP connection	-	X	-
E-mail connection	-	X	-
FTP connection	-	X	-
S7 connection*	-	-	X

* Note that for an S7-1500 CPU you must enable the use of PUT/GET communication in the properties of the CPU. You can find more information on this topic in the STEP 7 online help.

Additional information

You will find further information on the allocation of connection resources and the display of connection resources in STEP 7 in the section Connection resources (Page 421).

5.5 Data consistency

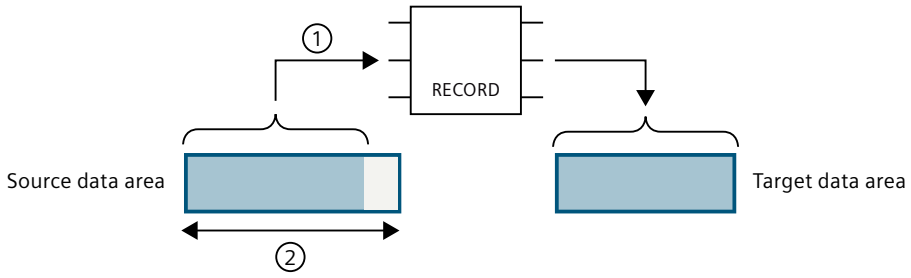
Definition

Data consistency is important for data transfer and you need to take this into account when configuring the communication task. Otherwise, malfunctions may occur.

A data area which cannot be modified by concurrent processes is called a consistent data area. There is a maximum size for consistent data areas for the transfer of CPU data.
If a data area that belongs together is larger than the maximum size of the consistent data area, it can consist of new and old data at any one time.

An inconsistency can occur when an instruction for communication is interrupted, for example by a hardware interrupt OB with higher priority. This interrupts the transfer of the data area. If the user program in this OB now changes the data that has not yet been processed by the communication instruction, the transferred data originates from different times:

The following figure shows a data area that is smaller than the maximum size of the consistent data area. In this case, when transferring the data area, it is ensured that there is no interruption by the user program during data access so that the data is not changed.

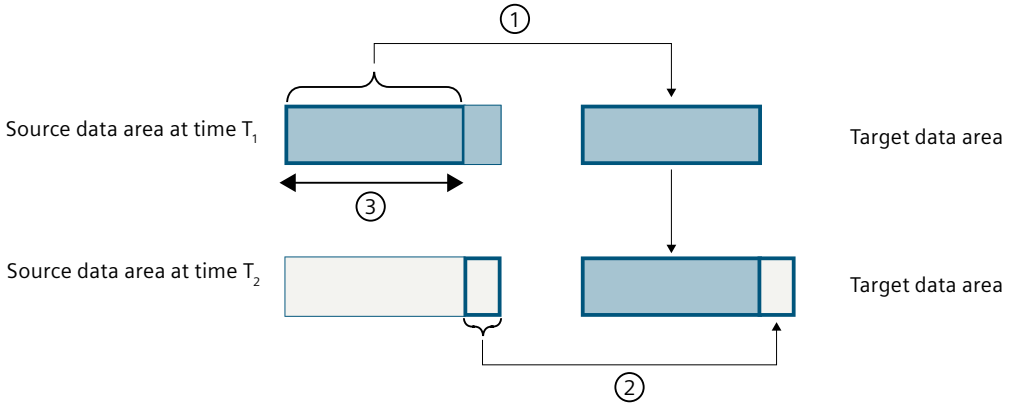


① The source data area is smaller than the maximum size of the consistent data area (②). The instruction transfers the data together to the destination data area.

② Maximum size of the consistent data area

Figure 3-98 Consistent transfer of data

The following figure shows a data area that is larger than the maximum size of the consistent data area. In this case, the data can be changed during an interruption of the data transfer. An interruption also occurs if, for example, the data area needs to be transferred in several parts. If the data is changed during the interruption, the transferred data originates from different times.



① The source data area is larger than the maximum size of the consistent data area (③). At time T1, the instruction only transfers as much data from the source data area into the destination data area as fits in the consistent data area.

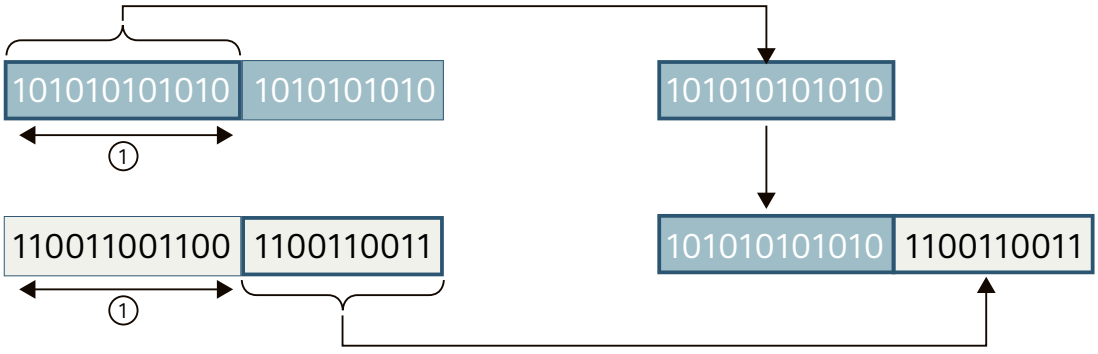
② At time T2, the instruction transfers the rest of the source data area to the destination data area. After the transfer, data from different points in time exist in the destination data area. If the data in the source data area has changed in the meantime, an inconsistency may result.

③ Maximum size of the consistent data area

Figure 3-99 Transfer of data larger than the maximum consistency area

Example of an inconsistency

The figure below shows an example of changing data during the transfer. The destination data area contains data from different points in time.



① Maximum size of the consistent data area

Figure 3-100 Example: Changing data during the transfer

System-specific maximum data consistency for S7-1500:

No inconsistency occurs if the system-specific maximum size of the consistent data is kept to. With an S7-1500, communication data is copied consistently into or out of the user memory in blocks of up to 512 bytes during the program cycle. Data consistency is not ensured for larger data areas. Where defined data consistency is required, the length of communication data in the user program of the CPU must not exceed 512 bytes. You can then access these data areas consistently, for example from an HMI device by reading/writing tags.

If more data than the system-specific maximum size needs to be transferred consistently, you yourself must ensure the data consistency with suitable measures in the user program.

Ensuring data consistency

Use of instructions for access to common data:

If the user program contains instructions for communication that access common data, for example TSEND/TRCV, you can coordinate access to this data area yourself, for example using the "DONE" parameter. The data consistency of the data areas that are transferred with an instruction for communication can therefore be ensured in the user program.

NOTE

Measures in the user program

To achieve data consistency, you can copy transferred data to a separate data area (for example, global data block). While the user program continues to work with the original data, you can transfer the data saved in the separate data area consistently with the communication instruction.

For the copying, use uninterruptible instructions such as UMOVE_BLK or UFILL_BLK. These instructions ensure data consistency up to 16 KB.

Use of PUT/GET instructions or Write/Read via HMI communication:

In S7 communication with the PUT/GET instructions or Write/Read via HMI communication, you need to take into account the size of the consistent data areas during programming or

configuration. In the user program of an S7-1500 as server, there is no instruction available that can coordinate the data transfer in the user program. The data exchanged using PUT/GET instructions updates the S7-1500 while the user program is running. There is no point in time within the processing of the cyclic user program at which the data is exchanged consistently. The length of the data area to be transferred should be smaller than 512 bytes.

More information

- You will also find the maximum amount of consistent data in the device manuals of the communications modules in the Technical Specifications.
- You will find further information on data consistency in the description of the instructions in the STEP 7 online help.

5.6 Secure Communication

5.6.1 Basics of Secure Communication

5.6.1.1 Useful information on Secure Communication

For STEP 7 (TIA Portal) as of V14 and for S7-1500 CPUs as of firmware V2.0, the options for "Secure Communication" have been broadened considerably.

"S7-1500 CPUs" also refers to CPU versions S7-1500F, S7-1500T, S7-1500C as well as S7-1500pro CPUs and ET200SP CPUs.

In subsequent versions, additional components will support Secure Communication (e.g. secure OUC), see next section.

As of firmware version V4.4, S7-1200 CPUs also support Secure Communication.

Requirement

- CPUs that support connection description DBs with the structure of the SDT TCON_IP_V4_SEC or SDT TCON_QDN_SEC. These are the following CPUs:
  - S7-1200 as of firmware V4.4
  - S7-1500 as of firmware V2.0
- Also optional via the following CPs:
  - CP 1243-1 as of firmware V3.2
  - CP 1243-8 IRC as of firmware V3.2
  - CP 1543-1 as of firmware V2.0
  - CP 1545-1
  - CP 1543SP-1

  Secure Communication via CP 1242-7 GPRS V2 is not possible.

Public Key Infrastructure (PKI)

The attribute "secure" is used for the identification of communication mechanisms that are based on a Public Key Infrastructure (PKI) (for example RFC 5280 for Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile). A Public Key Infrastructure (PKI) is a system that can issue, distribute and check digital certificates. The digital certificates issued are used in the PKI to secure computer-based communication. If a PKI uses asymmetric key cryptography, the messages in a network can be digitally signed and encrypted.

Components that you have configured in STEP 7 (TIA Portal) for secure communication use an asymmetric key encryption scheme with a Public Key and Private Key. TLS (Transport Layer Security) is used as the encryption protocol. TLS is the successor for the SSL (Secure Sockets Layer) protocol.

Objectives of secure communication

Secure communication is used to achieve the following objectives:

- Confidentiality
  i.e. the data are secret / cannot by read by eavesdroppers.
- Integrity
  i.e. the message that reaches the recipient is the same message, unchanged, that the sender sent. The message has not been altered on the way.
- End point authentication
  i.e. the end point communication partner is exactly who it claims to be and the party who is to be reached. The identity of the partner has been checked.

These objectives were in the past primarily relevant to IT and networked computers. Now, industrial machinery and control systems with sensitive data are at equally high risk, as they are also networked, and consequently pose strict security requirements for data exchange.

Protection of the automation cell by means of the cell protection concept through firewall, or via connection through VPN, for example with the security module, was common in the past and remains so.

However, it is becoming increasingly necessary to also transfer data to external computers in encrypted form via Intranet or public networks.

Common principles of secure communication

Independent of the context, secure communication is based on the concept of the Public Key Infrastructure (PKI) and contains the following components:

- An asymmetric encryption scheme that allows:
  - Encryption or decryption of messages using public or private keys.
  - The verification of signatures in messages and certificates.

    The messages/certificates are signed by the sender/certificate subject with their private key. The recipient/verifier checks the signature with the public key of the sender/certificate subject.

- Transport and storage of the public key using X.509 certificates:
  - X.509 certificates are digitally signed data that allow public key authentication in terms of the bound identity.
  - X.509 certificates can contain information that describes in more detail or restricts use of the public key. For example the date as of which a public key in a certificate is valid and when it expires.
  - X.509 certificates contain information about the issuer of the certificate in secure form.

The following paragraphs give an overview of these basic concepts, which are required for managing certificates in STEP 7 (TIA Portal), for example, and for programming communication instructions for secure Open User Communication (sOUC).

Secure communication with STEP 7

STEP 7 as of V14 provides the required PKI for the configuration and operation of secure communication.

Examples:

- The Hypertext Transfer Protocol (HTTP) becomes the Hypertext Transfer Protocol Secure (HTTPS) using TLS (Transport Layer Security) protocol. Since HTTPS is a combination of HTTP and TLS, it is called "HTTP over TLS" in the corresponding RFC. You can see in the browser that HTTPS is being used; this is indicated by the URL "https://" instead of "http://" in the address bar of the browser. Most browsers highlight such secure connections.
- Open User Communication turns into secure Open User Communication. The underlying protocol is also TLS.
- Email providers also offer access over the "Secure SMTP over TLS" protocol to increase the security of email communication.

The figure below shows the TLS protocol in the context of communication layers.

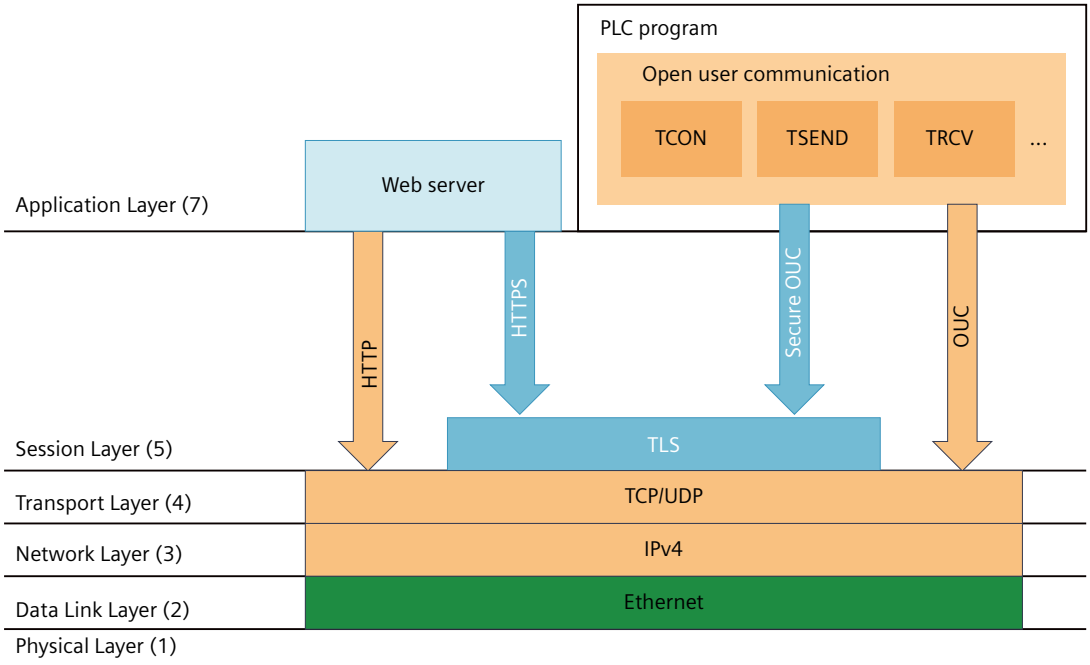


Figure 3-101 TLS protocol in the context of communication layers

Secure communication with OPC UA

An OPC UA server is implemented in S7-1500 CPUs as of firmware V2.0. OPC UA Security also covers authentication, encryption and data integrity with digital X.509 certificates and also uses a Public Key Infrastructure (PKI). Depending on the requirements placed by the application, you can select different security levels for the end point security. The description of the OPC UA server functionality is covered in a separate section.

Secure communication for PG/HMI communication

With the central components of the TIA Portal, STEP 7 and WinCC, an innovative and standardized Secure PG/PC and HMI Communication - PG/HMI communication for short - is implemented starting with version V17 together with the latest controllers and latest HMI devices.

More information

You can find more information on OPC UA in the section Using the S7-1500 as an OPC UA server (Page 222).

For more information on secure programming device/HMI communication, refer to the section Secure PG/HMI communication (Page 106).

5.6.1.2 Device-dependent security features

Transport Layer Security (TLS) is a widespread security protocol that improves the data security for communications. For the S7-1500 automation system, TLS is used for secure communication for the following certificate-based applications:

- Web server (HTTPS protocol variant)
- Secure Open User Communication (OUC) including secure email (TMAIL_C instruction)
- Secure PG/HMI communication

TLS takes care of the authenticity, confidentiality and integrity of the communication between client and server for the listed applications, for example, between the web server of CPU and web browsers, which, for example, have to display a diagnostics web page of the CPU.

The OPC UA server and OPC UA client applications do not actually directly use TLS, but the cryptographical processes used are comparable.

TLS is continuously being further developed, resulting in various TLS versions, which are distinct with regard to the cipher suites (standardized collection of cryptographic methods) supported and the performance.

The Internet Engineering Task Force (IETF) is responsible for the description of the TLS protocol. The following correlation applies:

- TLS 1.3 corresponds to RFC 8446
- TLS 1.2 corresponds to RFC 5246

In addition, not every device supports all the cryptographic methods defined in the RFCs. Therefore, after establishing the connection, the client and server negotiate a method that both support (Handshake) as well as the parameters to be used.

Supported TLS versions S7-1500

The following table shows, which TLS versions are supported in a given CPU firmware version.

CPU firmware version	Supported TLS version
as of V2.9	TLS 1.2, TLS 1.3
V2.8 ... V2.0	TLS 1.2

Supported encryption methods and parameters for creating certificates

To generate the public key for a new certificate, in the TIA Portal, set the encryption method and encryption parameters. These certificate parameters are device-dependent and dependent on the application used

One possibility: In the CPU properties, go to "Protection & Security > Certificate manager" and generate a new device certificate. You can find settings for the encryption method and the encryption parameters under "Certificate Parameters" in the "Generate Certificates" dialog.

Example: RSA 2048 stands for asymmetric RSA encryption method with cryptographic key length 2048 bits.

NOTE

Key lengths no longer recommended

RSA key lengths less than 3000 bits are no longer considered secure and lead to a warning during compiling as of TIA Portal V21 and a configured CPU with FW version V4.1.

As of TIA Portal V21 and a configured CPU with FW version V4.1, using the 1024-bit RSA key length leads to an error.

The following table shows the supported encryption methods and encryption parameters depending on the CPU application or services.

Encryption method/parameters S7-1500	Web server (HTTPS) Secure PG/HMI communication Secure OUC	OPC UA
EC prime256v1	Yes	No
EC secp384r1	Yes	No
EC secp256k1	No	No
RSA 1024	Yes, up to FW V4.0*	Yes, up to FW V4.0*
RSA 2048	Yes	Yes
RSA 3072	Yes	Yes
RSA 4096	Yes	Yes
RSA 8192	No	No

* A CPU with FW version V4.1 or higher only supports RSA 1024 in a spare part scenario, i.e. you load the configuration of a CPU with FW version up to V4.0 onto a CPU with FW version V4.1.

5.6.1.3 Confidentiality through encryption

Message encryption is an important element of data security. When encrypted messages are intercepted by third parties during communication, these potential eavesdroppers cannot access the information they contain.

There is a wide range of mathematical processes (algorithms) for encrypting messages.

All algorithms process a "key" parameter to encrypt and decrypt messages.

- Algorithm + key + message => encrypted message
- Encrypted message + key + algorithm => (decrypted) message

Symmetric encryption

The central aspect of symmetric encryption is that both communication partners use the same key for message encryption and decryption, as shown in the figure below. Bob uses the same key for encryption as Alice uses for decryption. In general, we also say that the two sides share the secret key with which they encrypt or decrypt a message as a secret.



① Bob encrypts his message with the symmetric key
② Alice decrypts the encrypted message with the symmetric key

Figure 3-102 Symmetric encryption

The process can be compared to a briefcase to which the sender and recipient have the same key, which both locks and opens the case.

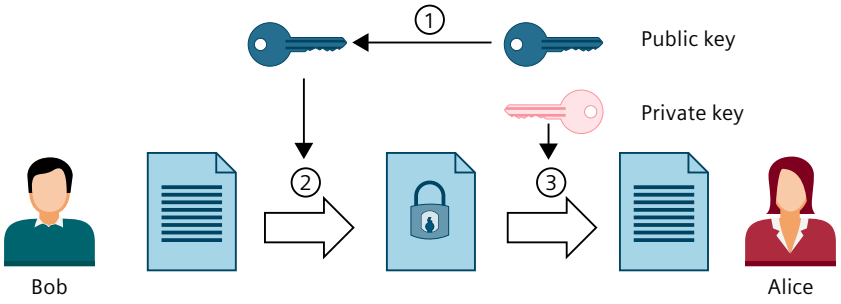
- Advantage: Symmetric encryption algorithms (such as AES, Advanced Encryption Algorithm) are fast.
- Disadvantages: How can the key be sent to a recipient without getting into the wrong hands? This is a key distribution problem. If enough messages are intercepted, the key can also be worked out and must therefore be changed regularly.

If there are a large number of communication partners, there is also a large number of keys to distribute.

Asymmetric encryption

Asymmetric encryption works with a pair of keys consisting of one public key and one private key. Used with a PKI, it is also known as Public Key cryptography or simply PKI cryptography. A communication partner, Alice in the figure below, has a private key and a public key. The public key is provided to the public, in other words any potential communication partner. Anyone with the public key can encrypt messages for Alice. In the figure below, this is Bob.

Alice's private key, which she must not disclose, is used by Alice to decrypt an encrypted message addressed to her.



① Alice provides Bob with her public key. No precautionary measures are required to this purpose: Anyone can use the public key for messages to Alice if they are sure that it is actually Alice's public key.

② Bob encrypts his message with Alice's public key.

③ Alice decrypts the encrypted message from Bob with her private key. As only Alice has the private key and never discloses it, only she can decrypt the message. With her private key, she can decrypt any message encrypted with her public key - not only messages from Bob.

Figure 3-103 Asymmetric encryption

The system can be compared to a mailbox into which anyone can put a message, but from which only the person with the key can remove messages.

- Advantages: A message encrypted with a public key can only be decrypted by the owner of the private key. As another (private) key is required for decryption, it is also much harder to work out the decryption key on the basis of large numbers of encrypted messages. This means that the public key does not have to be kept strictly confidential, unlike with symmetric keys.

  Another advantage is easier distribution of public keys. No specially secured channel is required in asymmetric cryptography to transfer the public key from the recipient to the sender encrypting the messages. Less work is thus required in managing the keys than would be the case in symmetric encryption procedures.
- Disadvantages: Complex algorithm (e.g. RSA, named after the three mathematicians Rivest, Shamir and Adleman), and therefore poorer performance than with symmetric encryption.

Encryption processes in practice

In practice, for example with a CPU Web server and Secure Open User Communication, the TLS protocol is used below the relevant application layer. Application layers are HTTP or SMTP, for example, as detailed above.

TLS (Transport Layer Security) uses a combination of asymmetric encryption and symmetric encryption (hybrid encryption) for secure data transfer, for example, over the Internet, and uses the following subprotocols:

- TLS Handshake Protocol, responsible for authentication of communication partners and negotiation of the algorithms and keys to be used for subsequent data transfer on the basis of asymmetric encryption.
- TLS Record Protocol, responsible for encryption of user data with symmetric encryption and data exchange.

Both asymmetric and symmetric encryption are considered secure encryption schemes - there is basically no difference in security between the two procedures. The degree of security depends on parameters such as the selected key length.

Abuse of encryption

You cannot tell what identity is assigned to a public key from the bit string. A fraud could provide their public key and claim to be someone else. If a third party then uses this key thinking that they are addressing their required communication partner, confidential information could end up with the fraud. The fraud then uses their private key to decrypt the message that was not intended for them, and sensitive information falls into the wrong hands.

To prevent this type of abuse, the communication partners must be confident that they are dealing with the right communication partner. This trust is established by using digital certificates in a PKI.

5.6.1.4 Authenticity and integrity through signatures

Attacks from programs that intercept communication between the server and client and act as if they themselves were client or server, are called man-in-the-middle attacks. If the false identity of these programs is not detected, they can obtain important information about the S7 program, for example, or set values in the CPU and attack a machine or plants. Digital certificates are used to avoid such attacks.

Secure communication uses digital certificates that meet the X.509 standard of the International Telecommunication Union (ITU). This allows the identity of a program, a computer or an organization to be checked (authenticated).

How certificates establish trust

The main role of X.509 certificates is to bind an identity with the data of a certificate subject (for example, e-mail address or computer name) to the public key of the identity. Identities can be people, computers or machines.

Certificates are issued by certificate authorities (Certificate Authority, CA) or by the subject of a certificate itself. PKI systems specify how users can trust the certificate authorities and the certificates that they issue.

The certificate process:

1. Anyone wishing to own a certificate submits a certificate application to a registration authority linked to the certificate authority.
2. The certificate authority assesses the application and applicant on the basis of set criteria.
3. If the identity of the applicant can be clearly established, the certificate authority confirms that identity by issuing a signed certificate. The applicant has now become the certificate subject.

The figure below is a simplified overview of the process. It does not show how Alice can check the digital signature.

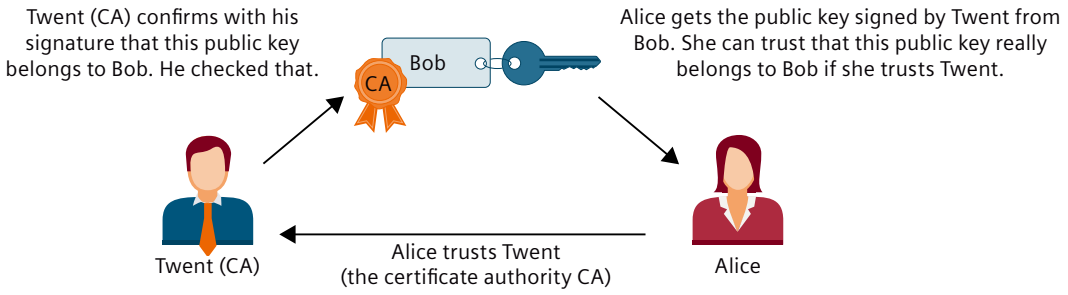


Figure 3-104 Signing of a certificate by a certificate authority

Self-signed certificates

Self-signed certificates are certificates whose signature comes from the certificate subject and not from an independent certificate authority.

Examples:

- You can create and sign a certificate yourself, for example, to encrypt messages to a communication partner. In the example above, Bob (instead of Twent) could himself sign his certificate with his private key. Using Bob's public key, Alice can check that the signature and public key from Bob match. This procedure is sufficient for simple internal plant communication that is to be encrypted.
- A root certificate is, for example, a self-signed certificate, signed by the certificate authority (CA), that contains the public key of the certificate authority.

Features of self-signed certificates

The "CN" (Common Name of Subject) for the certificate subject and "Issuer" attributes of self-signed certificates are identical: You have signed your certificate yourself. The "CA" (Certificate Authority) field must be set to "False"; the self-signed certificate should not be used to sign other certificates.

Self-signed certificates are not embedded in a PKI hierarchy.

Certificate content

A certificate to the X.509 V3 standard, the standard that is also used by STEP 7 and the S7-1500 CPUs, consists primarily of the following elements:

- Public key
- Details of the certificate subject (i.e. the holder of the key), for example, the Common Name (CN) of Subject .
- Attributes such as serial number and validity period
- Digital signature from the certificate authority (CA) confirming that the information is correct.

There are also extensions, for example:

- Specification of what the public key may be used for (Key Usage), for example, signing or key encryption.
  When you create a new certificate with STEP 7, for example in the context of Secure Open User Communication, select the correct entry from the list of possible usages, e.g. "TLS".
- Specification of a Subject Alternative Name ("SAN"), which is used in secure communication with Web servers (HTTP over TLS), for example, to ensure that the certificate in the address bar of the Web browser also belongs to the Web server specified in the URL.

How signatures are generated and verified

Asymmetric key usage ensures that certificates can be verified: The example of the "MyCert" certificate illustrates the "Sign" and "Verify signature" processes.

Generating a signature:

1. The authority of the "MyCert" certificate generates a hash value from the certificate data using a specific hash function (for example SHA-1, Secure Hash Algorithm).
   The hash value is a bit string of a constant length. The advantage of the constant length of the hash value is that it always takes the same amount of time to sign.
2. Using the hash value generated in this way and the private key, the authority of the certificate then generates a digital signature. The RSA signature scheme is often used.
3. The digital signature is saved in the certificate. The certificate is now signed.

Verifying a signature:

1. The authenticator of the "MyCert" certificate obtains the certificate of the issuer and thus the public key.
2. A new hash value is formed from the certificate data with the same hash algorithm that was used for signing (for example SHA-1).
3. This hash value is then compared with the hash value that is determined by means of the public key of the certificate authority and the signature algorithm for checking the signature.
4. If the signature check produces a positive result, both the identity of the certificate subject as well as the integrity, meaning authenticity and genuineness, of the certificate content are proven. Anyone who has the public key, i.e. the certificate from the certificate authority, can check the signature and thus recognize that the certificate was actually signed by the certificate authority.

The figure below shows how Alice uses the public key in the certificate from Twent (who represents the certificate authority, CA) to verify the signature on Bob's public key. All that is required for verification is therefore the availability of the certificate from the certificate authority at the moment of checking. The validation itself is executed automatically in the TLS session.

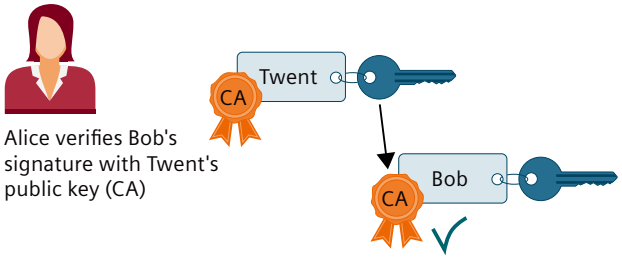


Figure 3-105 Verification of a certificate with the public key of the certificate of a certificate authority

Signing messages

The method described above for signing and verifying certificates also uses the TLS session for signing and verifying messages:

If a hash value is generated by a message and this hash value is encrypted with the private key of the sender and attached to the original message, the receiver of the message is able to check the integrity of the message. The recipient decrypts the hash value with the public key of the sender, puts together the hash value from the message received and compares the two values. If the values are different, the message or the encrypted hash value has been corrupted in transit.

Chain of certificates to root certificate

The certificates of a PKI are often organized hierarchically: The top of the hierarchy is formed by root certificates. Root certificates are certificates that are not signed by a higher-level certificate authority. The certificate subject and certificate issuer of root certificates are identical. Root certificates enjoy absolute trust. They form the "anchor" of trust and must therefore be known to the receiver as trusted certificates. They are stored in an area provided for trusted certificates.

Depending on the PKI, the function of root certificates is, for example, to sign certificates from lower-level certificate authorities, so-called intermediate certificates. This transfers the trust from the root certificate to the intermediate certificate. An intermediate certificate can sign a certificate just like a root certificate; both are therefore referred to as "CA certificates".

This hierarchy can be continued over multiple intermediate certificates until the end-entity certificate. The end-entity certificate is the certificate of the user who is to be identified.

The validation process runs through the hierarchy in the opposite direction: As described above, the certificate authority is established and the signature checked with the authority's public key. Then the certificate of the higher-level certificate authority is established along the entire chain of trust to the root certificate.

Conclusion: The chain of intermediate certificates to the root certificate, the certificate path, must be available in every device that is to validate an end-entity certificate of the communication partner, irrespective of the type of secure communication that you configure.

5.6.2 Managing certificates

5.6.2.1 What you should know about the certificate management

This section shows the available certificate management options of an S7-1500 CPU depending on the service (CPU application) used and on the versions of the TIA Portal / the CPU firmware.

Overview of certificate management options

Since TIA Portal version V14 and CPU firmware version V2.0, it has been possible to manage certificates for secure communications for different services of S7-1500 CPU in the TIA Portal and load them in the CPU.

TIA Portal as of version V17, along with the S7-1500 CPUs as of version V2.9 support another option of certificate management: With GDS push methods, you can transfer or renew certificates in the CPU at runtime without having to reload the CPU.

Using the same route, as of TIA Portal version V18, you can also transfer web server certificates for a S7-1500 CPU (as of firmware V3.0).

The following table provides an overview of the certificate management options depending on the service used and the TIA Portal firmware version or CPU firmware version.

Service	Certificate management with TIA Portal (TIA Portal version / S7-1500 CPU-FW version)	Certificate management with OPC UA GDS push methods (TIA Portal version / S7-1500 CPU-FW version)
Web server	as of V14 / as of V2.0	as of V18 / as of V3.0
Secure OUC communication	as of V14 / as of V2.0	-
OPC UA server	as of V14 / as of V2.0	as of V17 / as of V2.9
OPC UA client	as of V15.1 / as of V2.6	as of V21 / as of V4.1
Secure PG/HMI Communication	as of V17 / as of V2.9	-

You can find information on the certificate management options for R/H CPUs in the section Using an OPC UA server in an S7-1500R/H system (Page 459).

More information

Click here for a description of the certificate management with GDS push methods: Certificate management via Global Discovery Server (GDS) (Page 193).

If you do not need to load new certificates, but need to renew a certificate, e.g. because the validity period has expired, this is also possible in RUN while adhering to the conditions: See Tip: Updating loaded certificates in RUN (Page 75).

5.6.2.2 Certificate management with TIA Portal

STEP 7 as of version V14 together with the S7-1500 CPUs as of FW version 2.0 support the Internet PKI (RFC 5280) to such an extent that an S7 1500 CPU is able to communicate with devices that also support the Internet PKI.

The usage of X.509 certificates for verifying certificates as described in the preceding sections, for example, is a result of this.

STEP 7 as of V14 uses a PKI similar to the Internet PKI, with restrictions. Certificate Revocation Lists (CRLs), for example, are not supported.

You can find more information on X.509 certificates and CRLs on the Internet (https://www.rfc-editor.org/rfc/rfc5280).

Creating or assigning certificates in the TIA Portal

You create certificates for various applications in STEP 7 for devices with security properties, such as an S7-1500 CPU as of firmware V2.0.

The following areas in the Inspector window of the CPU allow the creation of new certificates or the selection of existing ones:

- "Web server > Security" - for the generation and assignment of Web server certificates.
- "Protection & Security > Access control" - for the assignment of user management server certificates (UMC server certificates - from TIA Portal V20).
- "Protection & Security > Connection mechanisms" - for the generation or assignment of PLC communication certificates (Secure PG/HMI communication, as of TIA Portal V17).
- "Protection & Security > Certificate manager" - for generating and assigning all types of certificates.
- "Protection & Security > Syslog" - for managing syslog client and server certificates (as of TIA Portal V19).
- "OPC UA > Server > Security" - for the generation or assignment of OPC UA server certificates.

You can find the areas listed above in the following places in the CPU properties.

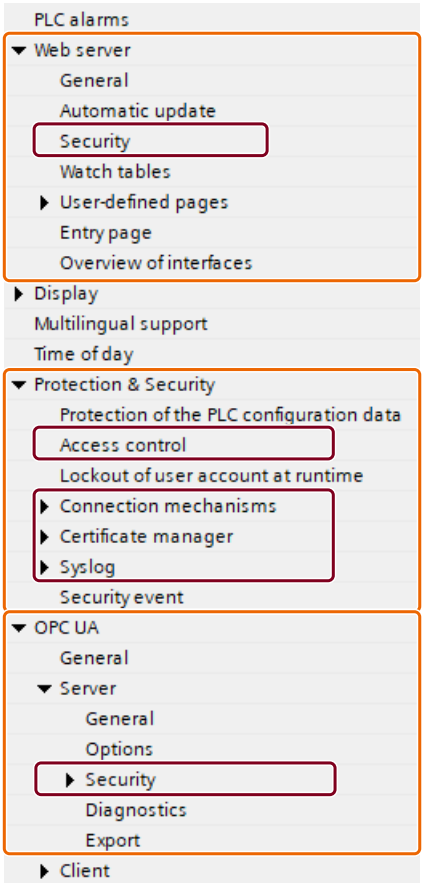


Figure 3-106 Certificate management in the properties of an S7-1500 CPU in STEP 7

Certificates have a validity period

⚠ WARNING

Certificates have a limited period of validity
If you generate certificates or adopt existing certificates in the TIA Portal when configuring devices and networks, then the limited validity period of the certificates is not obvious at this point in time.
For certificates generated automatically in the TIA Portal, the validity period expires well in the future. Once the validity period has expired, a secure connection from an HMI device or programming device to the CPU can no longer be established.
The system informs the operator or integrator of the system about the validity periods of the certificates used. This allows precautions to be taken for updating certificates.
To transfer certificates with an updated validity period to the CPU, either reload the TIA Portal project or use the certificate management at runtime. Not all services support certificate management at runtime.
If certificates with short validity periods are required, check whether automated certificate management, which provides certificates at runtime (OPC UA GDS Push methods), is an option.

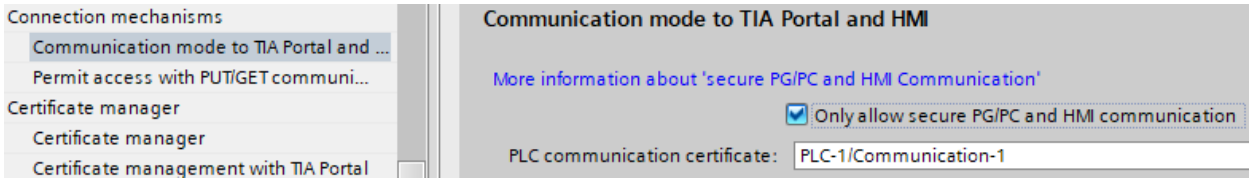
Example

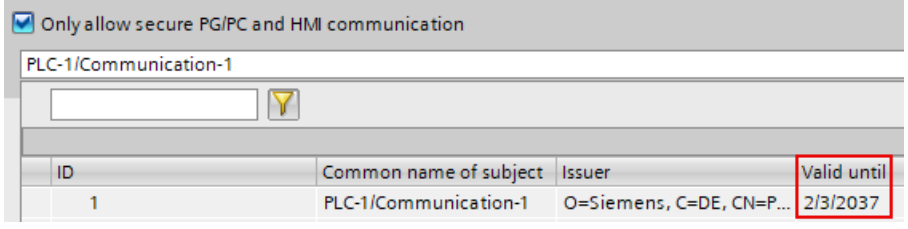
Settings in the "Protection & Security > Connection mechanisms > Communication mode to TIA Portal and HMI" area of the CPU:

A certificate for a protected connection is automatically created in the "Communication mode to TIA Portal and HMI" area. The properties of this initial certificate, including the validity period, are selected by the TIA Portal.

To see the validity period, open the extended display.

Depending on the client (connection partner), a connection establishment is rejected if the PLC communication certificate has expired.





You can easily set the validity period when creating new certificates. If the global security settings for the certificate manager are activated, you can change the validity period using the "Renew" function, e.g. move it further into the future.

You cannot update the PLC communication certificate shown in the example via the certificate management at runtime.

Special case: Expiration of the certificate while the protected connection is established

As the expiration date in the certificate is checked when the connection is established, an existing connection remains active even if the certificate expires in the meantime. When the connection is re-established, e.g. after a disconnection or temporary failure of the communication partner, the validity period of the certificate is checked and a connection is rejected.

Within an OPC UA session, a periodic connection establishment is enforced over the lifetime of the SecureChannel. This prevents certificate expiration or revoked certificates from remaining ineffective or undetected for long periods of time.

Special features of the section "Protection & Security > Certificate manager"

In this area of the Inspector window, you can switch between the global, i.e. project-wide, and local, i.e. device-specific, certificate manager (option "Use global security settings for certificate manager"). The option decides whether you have access to all the certificates in the project or not. The option determines which certificates you have access to as follows:

- If you **do not** use the certificate manager in the global security settings, you only have access to the local certificates of the CPU. You do not have access to imported certificates or root certificates. Without these certificates, only limited functionality is available: You can only generate self-signed certificates.
- If you use the certificate manager in the global security settings, you have access to the global, project-wide certificates. You can assign imported certificates or root certificates to the CPU. You can also create new certificates that are issued and signed by the project CA (certification authority of the project).
  A user requires a role with the following engineering rights for certificate handling in the certificate manager in the global security settings:
  - View configuration of security modules
  - Edit configuration of security modules

The following requirements must be met to access the global certificate manager:

- The project must be protected.
- The logged-in user must be assigned a role with the above-mentioned engineering rights.

The following figure shows the "Global security settings" in the project navigation after the option "Use global security settings for certificate manager" has been activated in the Inspector window of the CPU.

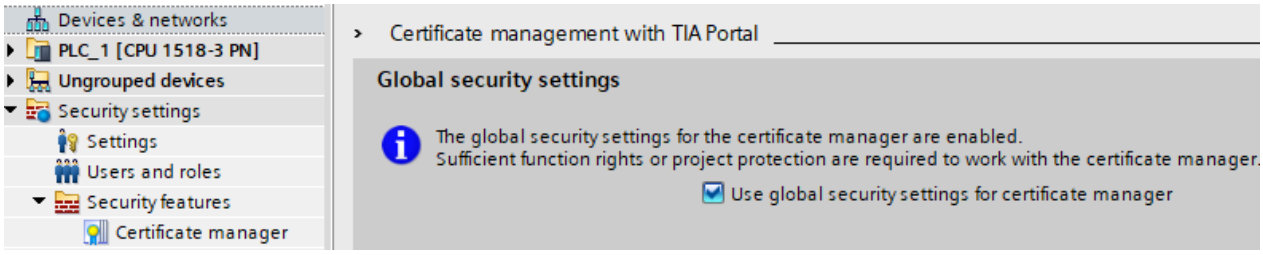


Figure 3-107 Use global security settings for certificate manager

When you double-click the "Certificate manager" line, you obtain access to all the certificates in the project, divided into the tabs "CA" (certificate authorities), "Device certificates" and "Trusted certificates and root certificate authorities".

Private keys

With asymmetric encryption, the confidentiality of private keys must be guaranteed. Private keys are used to decrypt or encrypt messages or to create digital signatures.

STEP 7 generates private keys when creating device certificates for client or server applications (end-entity certificates). The location where the private key is stored encrypted depends on the use of the global security settings for the certificate manager:

- If you use global security settings, the private key is stored encrypted in the global (project-wide) certificate memory.
- If you do not use global security settings, the private key is stored encrypted in the local (CPU-specific) certificate memory.

The existence of the private key is displayed in the "Private key" column in the "Device certificates" tab of the certificate manager in the global security settings.

When loading the hardware configuration, all certificates assigned to this CPU and the corresponding private keys are loaded into the CPU.

NOTICE
Enabling the "Use global security settings for certificate manager" option - Consequences The "Use global security settings for certificate manager" option influences the previously used private key: If you have already created certificates without using the certificate manager in the global security settings and then change the option for using the certificate manager, the private keys are lost and the certificate ID can change. All self-signed certificates in the device-specific certificate manager are removed from the configuration. The self-signed certificates in the global security settings remain unaffected. A warning draws your attention to this fact. Therefore specify at the beginning of the project configuration which option is required for the certificate manager.

More information

You can find more information on handling certificates in the application example "Using certificates with TIA Portal" (https://support.industry.siemens.com/cs/ww/en/view/109769068).

5.6.2.3 Examples for the management of certificates.

As explained in the preceding sections, certificates are required for every type of secure communication. The following section shows as an example how you handle the certificates with STEP 7 so that the requirements for Secure Open User Communication are fulfilled.

The devices which are involved at the respective communication partners are differentiated below. The respective steps for supplying the required certificates to the communications participants are described. An S7-1500 CPU or an S7-1500 Software Controller as of firmware version 2.0 is always required.

The general rule is:

While establishing a secure connection ("handshake"), the communication partners only transmit their end-entity certificates (device certificates).

Therefore the CA certificates required to verify the transmitted device certificate must be located in the certificate memory of the respective communication partner.

NOTE
The current date/time must be set in the CPU. The same date/time must be set for all communication partners involved.
When using secure communication (for example, HTTPS, secure OUC, OPC UA), make sure that the corresponding modules have the current time of day and the current date. Otherwise, the modules evaluate the used certificates as invalid and secure communication does not work.

Secure Open User Communication between 2 S7-1500 CPUs

Two S7-1500 CPUs PLC_1 and PLC_2 are to exchange data with each other via Secure Open User Communication.

You generate the required device certificates with STEP 7 and assign them to the CPUs as described below.

STEP 7 project certificate authorities (CA of the project) are used to sign the device certificates.

The certificates are to be referenced by their certificate ID in the user program (TCON communication instruction in combination with the associated system data type, for example TCON_IPV4_SEC). STEP 7 assigns the certificate ID automatically during the generation or creation of certificates.

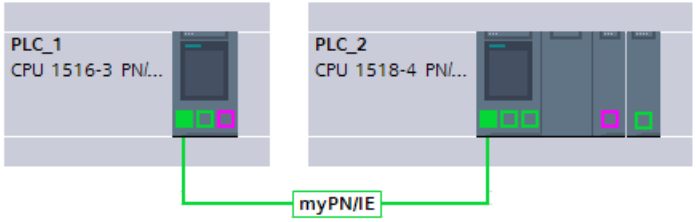


Figure 3-108 Secure OUC between two S7-1500 CPUs

Procedure

STEP 7 automatically loads the required CA certificates together with the hardware configuration to the participating CPUs so that the requirements for certificate verification exist for both CPUs. You therefore only have to generate the device certificates for the respective CPU; STEP 7 does the rest for you.

1. Mark PLC_1 and activate the "Use global security settings for certificate manager" option in the "Protection & Security" section.
2. Log in as a user in the project tree in the "Global security settings" section. For a new project, the "Administrator" role is planned for the first login.
3. Return to the PLC-1 in the "Protection & Security" section. Click in an empty line in the "Certificate subject" column in the "Device certificates" table to add a new certificate.
4. In the drop-down list for selecting a certificate click the "Add" button.
   The "Create Certificate" dialog opens.

5. Leave the default settings in this dialog. They are tailored to the usage of Secure Open User Communication (usage: TLS).

   Tip: Supplement the default name of the certificate subject, in this case the CPU name. In order to differentiate you better leave the default CPU name in case you have to manage a large number of device certificates.

   Example: PLC_1/TLS becomes PLC_1-SecOUC-Chassis17FactoryState.
6. Compile the configuration.

   The device certificate and the CA certificate are part of the configuration.
7. Repeat the steps described above for PLC_2.

In the next step you have to create the user programs for the data exchange and load the configurations together with the program.

Using self-signed certificates instead of CA certificates

When creating device certificates you can select the "Self-signed" option. You can create self-signed certificates without being logged in for the global security settings. This procedure is not recommended because the resulting certificates do not exist in the global certificate memory and can therefore not be assigned directly to a partner CPU.

As described above, you should select the name of the certificate subject with care so that the right certificate can be assigned to a device without any doubt.

Verification with the CA certificates of the STEP 7 project is not possible for self-signed certificates. To ensure that self-signed certificates can be verified you have to include the self-signed certificates of the communication partner into the list of trusted partner devices for each CPU. To this purpose you must have activated the "Use global security settings for certificate manager" option and be logged in as a user in the global security settings.

Proceed as follows to add the self-signed certificate of the communication partner of the CPU:

1. Mark PLC_1 and navigate to the "Certificates of partner devices" table in the "Protection & Security" section.
2. Click in an empty line in the "Certificate subject" column in the "Device certificates" table to add a new certificate.
3. Select the self-signed certificate of the communication partner from the drop-down list and confirm the selection.

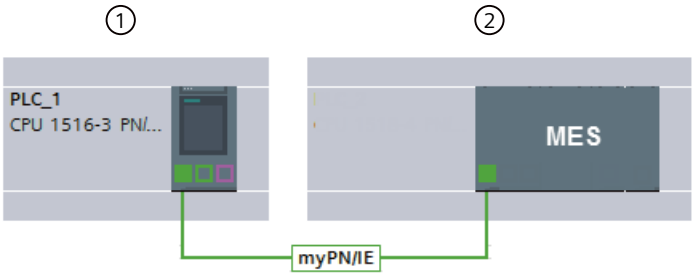
In the next step you have to create the user programs for the data exchange and load the configurations together with the program.

Secure Open User Communication between S7-1500 CPU as a TLS client and an external device as a TLS server

Two devices are to exchange data with each other via TLS connection or TLS session, for example, exchanging recipes, production data or quality data:

- An S7-1500-CPU (PLC_1) as TLS client; the CPU uses Secure Open User Communication
- An external device (for example a Manufacturing Execution System (MES)) as TLS server

The S7-1500 CPU establishes the TLS connection / session to the MES system as TLS client.



① TLS client
② TLS server

Figure 3-109 Secure OUC between S7-1500 CPU and a third-party device

The S7-1500 CPU requires the CA certificates of the MES system to authenticate the TLS server: The root certificate and, if appropriate, the intermediate certificates for verifying the certificate path.

You have to import these certificates into the global certificate memory of the S7-1500 CPU.

Proceed as follows to import certificates of the communication partner:

1. Open the certificate manager in the global security settings in the project tree.
2. Select the appropriate table (trusted certificates and root certificate authorities) for the certificate to be imported.
3. Right-click in the table to open the context menu. Click "Import" and import the required certificate or the required CA certificates.

   As a result of the import, the certificate has a certificate ID assigned to it and can be assigned to a module in the next step.
4. Mark PLC_1 and navigate to the "Certificates of partner devices" table in the "Protection & Security" section.
5. Click in an empty line in the "Common name of subject" column to add the imported certificates.
6. Select the required CA certificates of the communication partner from the drop-down list and confirm the selection.

Optionally the MES system can also request a device certificate of the CPU to authenticate the CPU (i.e., the TLS client). In this case, the CA certificates of the CPU must be made available to the MES system. The prerequisite for importing the certificates into the MES system is a preceding export of the CA certificates from the STEP 7 project of the CPU. Follow these steps:

1. Open the certificate manager in the global security settings in the project tree.
2. Select the matching table (CA certificate) for the certificate to be exported.
3. Right-click the selected certificate to open the context menu.
4. Click "Export".
5. Select the export format of the certificate.

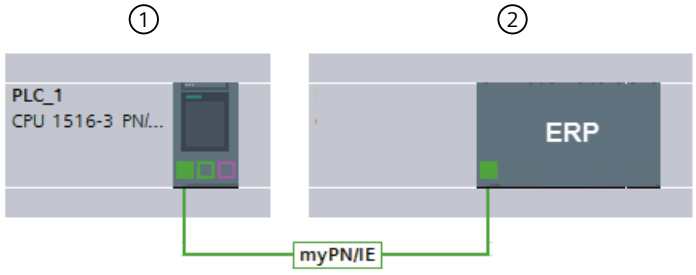
In the next step you have to create the user programs for the data exchange and load the configurations together with the program.

Secure Open User Communication between an S7-1500 CPU as TLS server and an external device as TLS client

If the S7-1500 CPU acts as TLS server and the external device, for example an ERP system (Enterprise Resource Planning System) establishes the TLS connection / session, you require the following certificates:

- For the S7-1500 CPU, you generate a device certificate (server certificate) with a private key and download it with the hardware configuration into the S7-1500 CPU. You use the "Signed by certificate authority" option when generating the server certificate.

  The private key is required for the key exchange as explained in the figure for the example "HTTP over TLS (Page 72)".
- You have to export the CA certificate of the STEP 7 project for the ERP system and import / load it into the ERP system. With the CA certificate the ERP system verifies the server certificate of the S7-1500 that was transferred from the CPU to the ERP system during the establishment of the TLS connection / session.



① TLS server
② TLS client

Figure 3-110 Secure OUC between an S7-1500 CPU and ERP system

You can find the description of the necessary steps in the previous sections.

Secure Open User Communication to a mail server (SMTP over TLS)

An S7-1500 CPU can establish a secure connection to an e-mail server with the communication instruction TMAIL-C.

The system data types TMail_V4_SEC and TMail_QDN_SEC allow you to determine the partner port of the e-mail server and thus to reach the e-mail server via "SMTP over TLS".

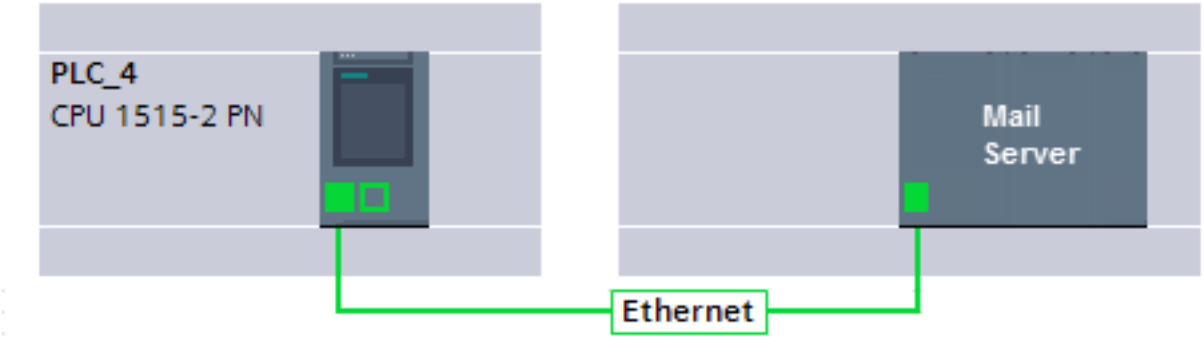


Figure 3-111 Secure OUC between a S7-1500 CPU and a mail server

Requirement for secure email connection is the importing of the root certificate and the intermediate certificates of the mail server (provider) into the global certificate memory of the S7-1500 CPU. By means of these certificates the CPU can check the server certificate that is sent by the mail server during the establishment of the TLS connection / session.

Proceed as follows to import certificates of the mail server:

1. Open the certificate manager in the global security settings in the project tree.
2. Select the appropriate table (trusted certificates and root certificate authorities) for the certificate to be imported.
3. Right-click in the table to open the context menu. Click "Import" and import the required certificate or the required CA certificates.

   As a result of the import, the certificate has a certificate ID assigned to it and can be assigned to a module in the next step.
4. Mark PLC_1 and navigate to the "Certificates of partner devices" table in the "Protection & Security" section.
5. Click in an empty line in the "Common name of subject" column to add the imported certificates.
6. Select the required CA certificates of the communication partner from the drop-down list and confirm the selection.

In the next step you have to create the user programs for the email client function of the CPU and load the configurations together with the program.

5.6.2.4 How communication with certificates works: HTTP over TLS

The following paragraphs show how the mechanisms described are used to establish a secure communication between a Web browser and the Web server of an S7-1500 CPU.

Initially the changes for the "Permit access only with HTTPS" option in STEP 7 are described. As of STEP 7 V14 you have the possibility to influence the server certificate of the Web server of an S7-1500 CPU as of firmware V2.0: The server certificate is generated as of these versions with STEP 7.

In addition it illustrates the processes that are executed when a website of the CPU Web server is called with a Web browser of a PC through an encrypted HTTPS connection.

Using Web server certificates for S7-1500 CPUs, FW V2.0 or higher

For S7-1500 CPUs with a firmware version before V2.0, you were able to set "Permit access only with HTTPS" when setting the Web server properties, without specific requirements applying.

You did not have to handle certificates for these CPUs; the CPU automatically generates the certificates required for the Web server.

For S7-1500 CPUs as of firmware V2.0, STEP 7 generates the server certificate (end-entity certificate) for the CPU. You assign a server certificate to the Web server in the properties of the CPU (Web server > Security).

Because a server certificate name is always preset, there is no change to the easy configuration of the Web server: You activate the Web server. The "Permit access only with HTTPS" option is enabled by default - STEP 7 generates a server certificate with the default name during compiling.

Irrespective of whether you use the certificate manager in the global security settings or not: STEP 7 has all the information required to generate the server certificate.

In addition, you have the possibility to determine the properties of the server certificate, for example, the name or the validity period.

NOTE

The current date/time must be set in the CPU.

When using secure communication (for example, HTTPS, secure OUC, OPC UA), make sure that the corresponding modules have the current time of day and the current date. Otherwise, the modules evaluate the used certificates as invalid and secure communication does not work.

Loading the Web server certificate

The server certificate generated by STEP 7 is then automatically also loaded to the CPU when the hardware configuration is loaded.

- If you use the certificate manager in the global security settings, the certificate authority of the project (CA certificate) signs the server certificate of the Web server: During loading the CA certificate of the project is loaded as well automatically.
- If you do not use the certificate manager in the global security settings, STEP 7 generates the server certificate as a self-signed certificate.

When you address the Web server of the CPU over the IP address of the CPU, a new server certificate (end-entity certificate) must be generated and loaded with each change in the IP address of an Ethernet interface of the CPU. This is necessary because the identity of the CPU changes with the IP address – and the identity requires a signature in accordance with the PKI rules.

You can avoid this problem by addressing the CPU with a domain name instead of its IP address, for example "myconveyer-cpu.room13.myfactory.com". For this purpose, you have to manage the domain names of the CPU via a DNS server.

Supplying a Web browser with a CA certificate of the Web server

In the Web browser the user who accesses the websites of the CPU through HTTPS should install the CA certificate of the CPU. If no certificate is installed, a warning is output recommending that you do not use the page. To view this page, you must explicitly "Add an exception".

The user receives the valid root certificate for download from the "Intro" Web page of the CPU Web server under "Download certificate".

STEP 7 offers a different possibility: Export the CA certificate of the project with the certificate manager into the global security settings in STEP 7. Subsequently import the CA certificate into the browser.

Course of the secure communication

The figure below shows, in simplified terms, how communication is established ("handshake") focusing on the negotiation of keys used for data exchange (here with HTTP over TLS).

However, the procedure can be applied to all communication options that are based on the usage of TLS, i.e. also to Secure Open User Communication (see Basics for secure communication (Page 51)).

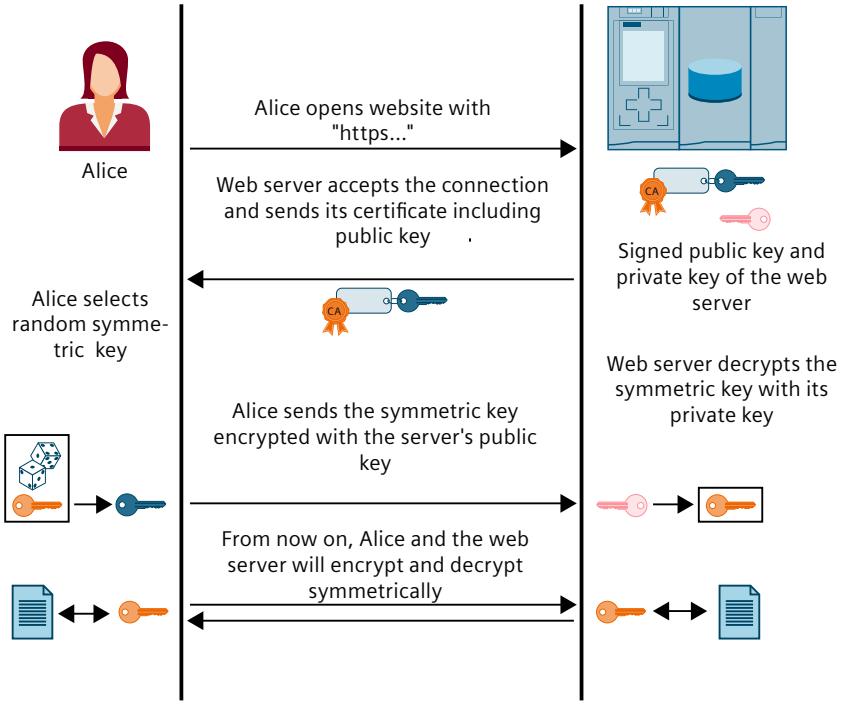


Figure 3-112 Handshake with https

The figure does not show the measures taken at Alice's end (browser) to verify the certificate sent by the Web server. Whether Alice can trust the Web server certificate received and therefore the identity of the Web server, and can accept the exchange of data, depends on positive verification.

The steps for verifying the authenticity of the Web server:

1. Alice must know the public keys of all relevant certificate authorities, which means she requires the complete certificate chain to verify the Web server certificate (i.e. the end-entity certificate of the Web server):

   Alice will generally have the required root certificate in her certificate memory. When a Web browser is installed, a range of trusted root certificates is also installed. If she does not have the root certificate, she must download it from the certificate authority and install it in the certificate authority of the browser. The certificate authority can also be the device on which the Web server is located.

   You have the following options for obtaining the intermediate certificates:

   – The server itself sends the required intermediate certificates to Alice along with its end-entity certificate – in the form of a signed message so that Alice can verify the integrity of the certificate chain.
   – The certificates often contain the URLs of the certificate issuer. Alice can load the required intermediate certificates from these URLs.

When you work with certificates in STEP 7 it is always assumed that you have imported the intermediate certificates and the root certificate into the project and assigned them to the module.

2. Alice validates the signatures in the certificate chain with the public keys of the certificates.
3. The symmetric key must be generated and transferred to the Web server.
4. If the Web server is addressed by its domain name, Alice also verifies the identity of the Web server in accordance with the Internet PKI rules defined in RFC 2818. She is able to do this because the URL of the Web server, in this case the "Fully Qualified Domain Name" (FQDN), is saved in the end-entity certificate of the Web server. If the certificate entry in the "Subject Alternative Name" field corresponds to the entry in the address bar of the browser, everything is fine.

The process continues with the exchange of data with the symmetric key, as shown in the figure above.

See also

Examples for the management of certificates. (Page 67)

5.6.2.5 Tip: Updating loaded certificates in RUN

As of TIA Portal V19 and firmware version V3.1 of the S7-1500 CPUs (incl. R/H-CPUs) you have the possibility to update certificates during runtime, i.e. in RUN mode of the CPU.

These are certificates that were configured through the TIA Portal and downloaded.

This allows this you, for example, to renew or replace expired certificates without interrupting the running process.

Requirements

- Project protection is activated.
- The project administrator (Engineering-Administrator) is logged on with the corresponding security rights.
- No further changes to the hardware configuration are present. These changes would require a STOP of the CPU to be loaded.

Rule

The existing ID of the certificate to be updated must not change.

Procedure

1. In TIA Portal (project navigation), navigate to the certificate manager (Security settings > Security functions).
2. Select the "Certificate authority (CA)" tab or the "Device certificates" tab - depending on which certificate you want to update.
3. Select the certificate to be updated.

4. In the context menu, select the "Renew" or "Replace" command, depending on whether you want to replace the existing certificate with a certificate from the file system or only update the validity data of the existing certificate, for example.
   When CA certificates are replaced, all derived device certificates are automatically digitally signed with the renewed CA certificate.
5. Load the changes to the CPU (Load to device > Hardware configuration).

5.6.3 Requirements for secure communication

5.6.3.1 Protection of confidential configuration data

As described in the basic information on secure communication, the proper functioning of certificate-based protocols requires private keys that must be protected as best as possible.

As of STEP 7 V17, you can use a password to protect these keys and other data worth protecting: The password to protect confidential PLC configuration data.

As of STEP 7 V21 and a CPU FW version V4.1, you can choose whether you also want to protect the entire configuration of the CPU in addition to protecting the configuration data. The data is stored encrypted in the SIMATIC.S7S folder on the SIMATIC Memory Card and can only be decrypted with the password for protection of confidential configuration data.
If you revoke or add the setting for protection of all data, the contents of the SIMATIC.S7S folder on the SIMATIC Memory Card will be deleted at the next download to the CPU. Other files, such as recipes or backup files on the SIMATIC Memory Card, are not deleted. After the deletion, the CPU performs a restart.

If you have activated protection for the entire configuration, you will need the assigned password to upload from a SIMATIC memory card to STEP 7. Without a password, uploading from a SIMATIC memory card to STEP 7 is no longer possible.

It is possible to do without the password if you have implemented measures to prevent unauthorized access to the TIA Portal project and the configuration of the CPU.

independently of whether you assign a password or not: The TIA Portal generates a key information that provides for the protection of the confidential PLC configuration data. This password has no influence on the secure communication process. However, the complexity of the password for the protection of confidential PLC configuration data determines how well the private keys, for example, are protected.

The presence of key information is a prerequisite for secure communication such as TLS-based secure PG/HMI communication: The CPU can handle certificates which are required for Secure Communication only if this key information is available.

The following figure shows the described contexts.

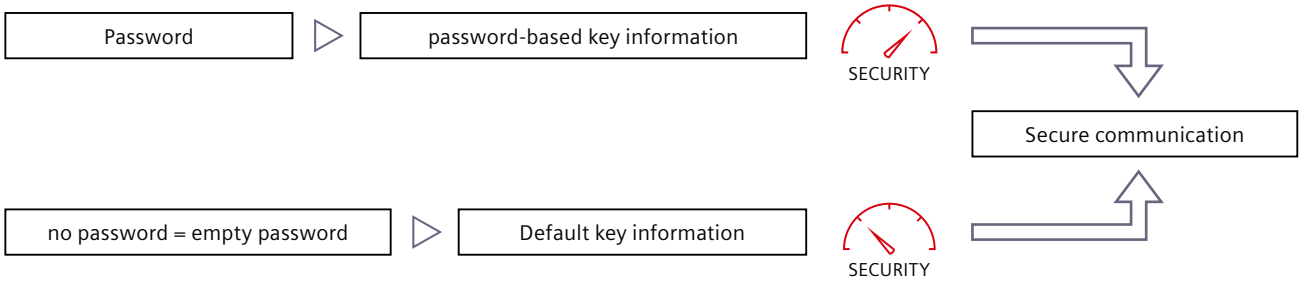


Figure 3-113 Contexts for protecting confidential configuration data

Security settings wizard

When you add a CPU to the project that supports secure PG/HMI communication in the TIA Portal from the hardware catalog, a wizard starts for the security settings of the CPU. The wizard guides you step-by-step through the security settings of the CPU.

Each of these settings is explained in detail in the wizard. At the end, all settings are once again summarized in an overview.

The wizard also starts, for example, when you replace a module in the network view of the TIA Portal and the new CPU, unlike the replaced CPU, supports secure PG/HMI communication.

All settings in the wizard are applied in the Inspector window (CPU properties).

You can start the wizard at any time using a Start button in the "Protection & Security" area of the CPU properties.

Requirement

- TIA Portal as of version V17
- CPU supports secure PG/HMI communication (for S7-1500 CPUs as of firmware version 2.9)
- The CPU is not yet loaded or the CPU is reset to factory settings with the option "Delete password for protection of confidential PLC configuration data"

Procedure

1. Open the CPU properties in the network view or in the device view.
2. Navigate to the area "Protection & Security > Protection of the PLC configuration data".
   Result: The "Protect confidential PLC configuration data" option is enabled first and the empty field for password entry is highlighted in red.
3. Configure the password (recommended) via the "Set" button or disable the "Protect confidential PLC configuration data" option.
4. Complete the configuration and create the user program.
5. Load the CPU.
   When loading the hardware configuration, you will be asked once to re-enter the password.
   Background: The configured password is used in the TIA Portal to generate the key information to protect confidential configuration data and thus to protect this data. For security reasons, however, neither the password nor the key information is saved in the project. In order for the key information to reach the CPU, it is re-generated when the hardware configuration is loaded, so that the password must be entered once at this point.

Certificate-based communication also between PG/HMI and CPU

Because, as of TIA Portal version V17 and CPU firmware version V2.9 (S7-1500) or V4.5 (S7-1200), the PG/HMI communication is also certificate-based, you will be prompted to accept the server certificate in the course of the commissioning.

Tips and rules for password management

- Manage your passwords in a password manager.
- To check the newly entered passwords for compliance and, for example, prevent trivial passwords, use the settings for checking the password policies in the TIA Portal:
  - In the project tree, navigate to the area "<Project name> > Security settings > Settings" area and select the "Password policies" area.
  - Specify, for example, the minimum number of characters the password must have or the minimum number of special characters.
- You do not have to assign different passwords for each CPU in a system or machine. If the requirements are met, you can also define the same password for a group of CPUs. This strategy also has advantages in the replacement parts scenario: If the group password is also assigned to the replacement CPU, the workload of replacing the CPU is reduced.

  Note here the risk that if the password of one of these CPUs is compromised, all CPUs with the same password are vulnerable.
- The definition of passwords also has an impact on the replacement part case, as the password for confidential PLC configuration data must be transferred to the new (replacement) CPU in addition to the configuration (see Rules for the replacement parts scenario (Page 87)).
- With **S7-1500R/H CPUs**, the password for confidential PLC configuration data is only loaded onto one of the two CPUs during loading. In order that the sync-up process works and that the partner CPU also works properly, the password must be transferred to the partner CPU before the sync-up, using the Online and Diagnostics editor:
  - In the Online and diagnostics view, you specify the area "Password to protect confidential PLC configuration data".
  - Enter the required password and click the "Set" button.

    If the correct password has been entered, the partner CPU can use the protected PLC configuration data and start the sync-up process.

5.6.3.2 Useful information for the protection of confidential PLC configuration data

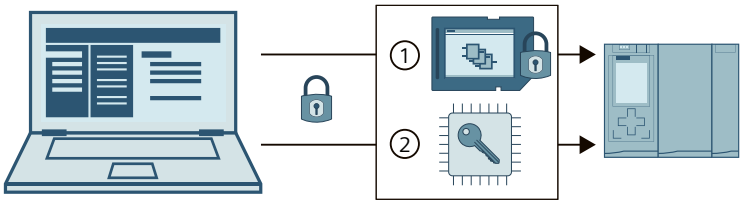
The concept for Secure Communication protected by security standards comprises the following components:

- A password-based key information that is used for protecting confidential configuration data (e.g. private keys for certificates, passwords).
- A standardized log (TLS) that ensures communication between the participants (e.g. programming device and CPU).

Principle of "Protection of confidential configuration data" and "Additional protection of downloadable configuration data"

The following simplified illustration shows how confidential configuration data, e.g. of a standard S7-1500 CPU, is protected: The two components project and key information are placed in different memory areas when loaded for the first time. The project in the load memory (memory card), the key information in a memory area in the CPU.

For other target systems (e.g. S7-1200 CPU, software controller) with different storage concepts, the implementation is adapted to the corresponding storage concepts, but the principle is the same.



① Project with password-protected confidential configuration data (here: in load memory = memory card)

② Key information (generated from password) to use the protected confidential configuration data (here: in the memory area in the CPU)

Figure 3-114 Principle for protection of confidential configuration data

Two memory areas for more security

The charged components are related to each other like two matching puzzle pieces: The project is bound to the loaded key information, the loaded key information is bound to the password that was assigned during configuration.

Project and key information must match, otherwise the CPU will not start.

The principle of two separate memory areas also applies to the S7-1200 CPUs and to S7-1500 CPU variants without a memory card, such as the SW controller or PLCSIM/PLCSIM Advanced. In the versions without memory card, two separate partitions are used so that the two items of information can be managed independently of one another.

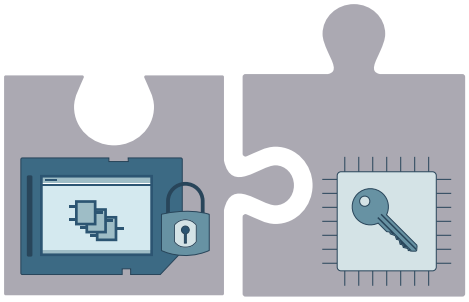


Figure 3-115 Principle of two separate memory areas

5.6.3.3 Changing your password

It makes a difference whether the CPU has already been loaded or not. If the CPU has already been loaded, it has the key information with which the password-protected PLC configuration data can be used.

Change password - configuration not yet loaded

As long as you have not yet loaded a configuration into the CPU, you can change an entered password or you can revoke the activation of the password protection.

Requirement

- The CPU is not yet loaded

Procedure

1. Open the CPU properties in the network view or in the device view.
2. Navigate to the area "Protection & Security > Protection of the PLC configuration data".
3. Click the "Change" button or deactivate the option "Protect confidential PLC configuration data".
4. Enter the previously valid password in the dialog. In case of a password change, also enter the new password and confirm the new password.

As long as you have not yet loaded a configuration into the CPU, the CPU is in a provisioning phase (see CPU behavior from loading to operational readiness (Page 110)) and you can load any valid configuration with your configured password.

Change password - configuration is already loaded

If the CPU has already been loaded with a configuration and the configuration is protected with a password for confidential PLC configuration data, you must first either reset the CPU to the factory settings and delete the password for confidential PLC configuration data in the CPU or delete it directly online and then set it.

Requirements

- You have write access to the CPU
- The CPU must be in STOP mode.

Procedure

1. Select the CPU in the network view.
2. Select the "Online & Diagnostics" command from the shortcut menu.
3. If you also change the project on the memory card, i.e. then want to reload the configuration:
   - Select the "Reset to factory settings" area in the opened online and diagnostics view.
   - Activate the option "Delete password to protect confidential PLC configuration data". To avoid a repeated start-up of the CPU, also select the "Format memory card" option.
   - Then load the project with the changed configuration and the desired password.

4. If you do not have to change the project on the memory card, i.e. only the wrong password is set:
   - In the Online and diagnostics view, you specify the area "Password for the protection of confidential PLC configuration data".
   - Click the "Delete" button. If the "Delete" button is not available, no password has been set in the CPU yet.
   - Enter the required password and click the "Set" button.

   If the correct password has been entered, the CPU can use the protected PLC configuration data.

No write access to the CPU
If you do not have write access to the load memory (read access level), remove the memory card from the CPU or delete the memory card externally, e.g. in your computer, before you reset to factory settings with the option "Delete password to protect confidential PLC configuration data".

NOTE
Reset to factory settings via the mode switch/mode selector keys of the CPU
Restoring the factory settings of the CPU via the mode switch/mode selector keys also deletes the IP address of the CPU, but not the password for protecting confidential PLC configuration data.

NOTE
Reset to factory settings via the display of the CPU
Resetting the CPU to factory settings via the display deletes the password for the protection of confidential PLC configuration data.

More information

Information on how to proceed in case of a spare part can be found in section Rules for the replacement parts scenario (Page 87).

5.6.3.4 Resetting the password

The protection of the confidential PLC configuration data can be reset. This may be necessary, for example, if you want to change the password but no longer know the current password.

Password lost - configuration not yet loaded

Since you have to enter the password when loading the CPU via TIA Portal for the first time, the CPU configuration for this CPU can no longer be used. To change the password in the CPU properties, you must also enter the previously valid password. If you forget your password, do the following:

Requirement
- The CPU is not yet loaded

Procedure

1. Open the CPU properties in the network view or in the device view.
2. Navigate to the area "Protection & Security > Protection of the PLC configuration data".
3. Click "Reset".

   Please note that the certificates of the CPU (e.g. certificates for web server, for OPC UA server, for PG/PC communication and HMI communication) may no longer be used after the reset and may have to be created again and reassigned.

   – If you use the global security settings for the certificate manager, you must reassign the certificates from the certificate manager.
   – If you do not use the global security settings for the certificate manager, you must recreate and reassign the certificates.
4. Confirm the reset of the password.

The option for the protection of confidential PLC configuration data is still activated.

Delete password – Configuration is already loaded

If the CPU has already been loaded with a configuration and the configuration is protected with a password for confidential PLC configuration data, you can, for loading a new project, delete the password for confidential PLC configuration data online and then specify a new password.

Requirements

- You have write access to the CPU
- The CPU must be in STOP mode.

Procedure

1. Select the CPU in the network view.
2. Select the "Online & Diagnostics" command from the context menu.
3. In the area "Password to protect confidential PLC configuration data", click the "Delete" button.
   If the "Delete" button is not available, no password has been set in the CPU yet.

NOTICE
Deleting the password for confidential configuration data If a loaded project is password-protected and the password is deleted, this project may no longer work without a password. The CPU also generates a corresponding entry in the diagnostics buffer.

4. If required, now enter a new password via the "Set" button.
5. Perform a restart of the CPU.

NOTE

Password for protecting confidential configuration data after resetting the CPU to factory settings

- **Via the mode switch / mode selector keys (SIMATIC Memory Card is not inserted):** The password for protection of confidential configuration data is retained.
- **Using the display:** The password for protection of confidential configuration data is deleted.
- **Using STEP 7:** The password for protection of confidential configuration data is retained. The password is only deleted when the "Delete password for protection of confidential PLC configuration data" option is set.

More information

Information on changing the password can be found in section Changing your password (Page 80).

5.6.3.5 Assign password via SIMATIC Memory Card

If you want to transfer the password to protect confidential PLC configuration data to a CPU without using TIA Portal, you can also use a SIMATIC memory card for this function.

The use of a SIMATIC memory card is suitable for the following purposes:

- Preparing a new CPU

  If a CPU is set up again, it should be configured with a password to protect the confidential PLC configuration data. After this configuration is completed, it is possible to use another SIMATIC memory card with the desired project.

  (S7-1200 CPU: A "transfer" card with transfer job can also be used to install the program on the CPU).
- CPU has a password to protect confidential PLC configuration data, but the password does not match the project

  If the passwords are not identical, you can set the correct password with the memory card in the CPU.

  (S7-1200 CPU: equipped either with SIMATIC "transfer" card or with SIMATIC "Program" card).
- reset the password for the protection of confidential PLC configuration data in the CPU

  As preparation for a disposal of the CPU or as preparation for a new project for the CPU.

Requirement

- TIA Portal as of version V17

Basic procedure

1. Creating a SIMATIC memory card with "SET PASSWORD" job

   This action creates a folder and file structure following a special pattern and writes a password for the protection of the confidential PLC configuration data as plain text to a special file on the SIMATIC memory card. See description below.
2. Insertion of a prepared SIMATIC memory card in the CPU and switch on the CPU.

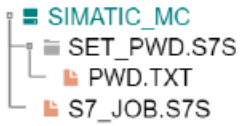
   The PLC reads the password, processes it and stores the result in the internal memory. Any existing entry is overwritten.
3. Remove the SIMATIC memory card and restart the CPU.

   Results (S7-1500): While the CPU is reading the SIMATIC memory card, the LED shows the same behavior as with a firmware update. The RUN/STOP LED flashes while the CPU is setting the password. After the process has been completed successfully, the RUN/STOP LED lights up yellow and the MAINT LED flashes yellow.

The result of the operation is displayed in the diagnostics buffer as success or error message. If the password could not be set, the error LED flashes together with the other LEDs.

Creating a SIMATIC memory card with "SET PASSWORD" job

1. Create a folder in the root directory named "SET_PWD.S7S".
2. Create a text file named "PWD.TXT" with the password as text-only in the folder just created on the memory card.
3. Create a text file named "S7_JOB.S7S" in the root directory of the memory card with the content "SET_PWD".
   This file is the "Job file" for assigning a password for the protection of the confidential PLC configuration data of the PLC.
4. The file structure on the SIMATIC memory card then looks as follows:



NOTE
Safe storage of the SIMATIC memory card
Store the SIMATIC memory card in a safe location to which only authorized persons have access.

Rules and recommendations

- Setting the password must be done in a secure environment.
- The content of the text file "PWD.TXT" defines the password for the protection of confidential PLC configuration data. It must match the password that you have also assigned in the CPU configuration.
- To reset an existing password of a PLC, the text file "PWD.TXT" must be empty, i.e. the file size is 0 bytes.
- Use any text editor to create the text file. The recommended text format is "UTF-8".
- The folder and file names are not case-sensitive. However, the password itself is case-sensitive.
- Do not enter a CR/LF character at the end (PWD.TXT or S7_JOB.S7S).

5.6.3.6 Special features when backing up and restoring a CPU

You can back up a functional configuration of a CPU in the TIA Portal and access it at a later time; this means you can then restore the originally backed-up configuration. This allows you to load a modified configuration, for example, to test product enhancements, to change programs for troubleshooting in the system or you can replace components on a test basis. You can then restore the originally backed-up configuration of the CPU.

Backing up the configuration

In backing up a CPU ("Online" menu, "Load backup from online device" in TIA Portal), the password for the protection of confidential PLC configuration data is backed up as well.

Restoring the backup

When restore the backup of a CPU (menu "Online", command “Download to device” with marked backup in TIA Portal) the CPU can only communicate with a PG/PC or HMI if the following condition is fulfilled:

- After the restoration of a configuration protected with a password to protect confidential PLC configuration data, exactly this password must be present in the CPU.
  Otherwise the CPU cannot access the configuration data. As a result, the CPU cannot restore the backup.
- With a CPU as of FW version V4.1, the password for protecting confidential PLC configuration data when restoring the backup must be the same as that used when the backup was created. Otherwise, the backup cannot be restored.

Possible causes of errors when restoring the backup
For CPUs as of FW version 4.1:
You must set the correct password to protect confidential PLC configuration data before restoring the project. Otherwise, a successful recovery process cannot be guaranteed.
For CPUs with FW version lower than V4.1:
You can also restore a backup if the password entered to protect confidential PLC configuration data does not match the password stored in the CPU. In this case, the CPU performs a restart, but cannot evaluate the contents of the SIMATIC Memory Card. Consequently, the CPU remains in STOP and displays an error.

Remedy
If one of these errors occurs, you must delete the password for protecting confidential PLC configuration data in the CPU and then set the correct password. After a restart the CPU, the backup is functional.

5.6.3.7 Tips for error avoidance and error handling

The following description lists some use cases that may result in CPU error messages.

Diagnostic buffer provides information

The CPU detects when the password protecting confidential configuration data and the loaded configuration do not match. A message in the diagnostic buffer indicates possible causes and remedies and usually leads to a solution of the problem.

Typical "pitfalls"

You should pay attention to the following circumstances in order to avoid or correct errors:

- Configuration loaded?
  Regardless of whether you protect your confidential configuration data with a password or not: without a loaded configuration, the CPU does not leave the provisioning phase.
- You are trying to load the CPU with a configured password and the CPU has already received another password.
  Example: CPU is exchanged for another CPU from the stock. The replacement CPU was not completely reset (reset to factory settings with option "Delete password for protection of confidential PLC configuration data").
  Solution:
  - Always prepare replacement CPUs with the appropriate option (password deleted).
  - For the configuration to be loaded, use the same password that was already used for the configuration already loaded.
  - It is also possible that the wrong project / CPU configuration was loaded. Check whether the correct CPU configuration is available.
  - Use the online function "Set password to protect confidential PLC configuration data" to delete the password or to set the same password as in the CPU configuration. Then, restart the device.
- The same error occurs if your CPU configuration does not use a password and the already loaded configuration requires a user-defined password.
  Solution:
  - Use the online function "Set password to protect confidential PLC configuration data" to delete the password or to set the same password as in the CPU configuration. Then, restart the device.

5.6.3.8 Rules for the replacement parts scenario

The assignment of passwords to protect confidential PLC configuration data also has an impact on the replacement parts scenario.

Rules for the replacement parts scenario

Observe the following rules for the replacement parts scenario:

Configuration of the replacement CPU via TIA Portal

- A CPU as replacement for an existing CPU should not have a configuration or a configured password to protect confidential PLC configuration data.
  Advantage: You can load the project into the replacement CPU without any further preparation - regardless of whether a password is configured or not.
- If the replacement CPU has already been configured, you must reset the CPU to the factory settings with the following options set:
  - "Delete password for protection of confidential PLC configuration data"
  - "Format memory card"

Replacement CPU is supplied with configuration data via memory card

- If you have **not** assigned a password to a CPU in your project to protect confidential PLC configuration data, you can insert the memory card of the CPU to be replaced into a brand-new, unused CPU without any further action needed.
  If the replacement CPU has already been configured with a password to protect confidential PLC configuration data, you must first reset this CPU to the factory settings using the option "Delete password for protection of confidential PLC configuration data".
- If you have assigned the same password to a group of CPUs, you can also assign the group password to the replacement CPU via the TIA Portal or via an appropriately prepared memory card (see Protection of confidential configuration data (Page 76)).
  In this case you can, for example, insert a memory card with the current project into the CPU and put it into operation without any further password handling.
- If you assign different passwords to each CPU in your project, you must first set the password valid for the respective CPU with the online and diagnostics editor when using the replacement CPU (area "Set password for protection of confidential PLC configuration data", see Changing your password (Page 80)).

More information

In section Assign password via SIMATIC Memory Card (Page 84) you can read how to use the SIMATIC Memory Card to assign the password to protect confidential PLC configuration data.

5.6.4 Secure Open User Communication

5.6.4.1 Secure OUC of an S7-1500 CPU as TLS client to an external PLC (TLS server)

The following section describes how you can set up Open User Communication via TCP from an S7-1500 CPU as TLS client to a TLS server.

Setting up a secure TCP connection from an S7-1500 CPU as TLS client to a TLS server

S7-1500 CPUs as of firmware version V2.0 support secure communication with addressing via a Domain Name System (DNS).

For secure TCP communication over the domain name you need to create a data block with the TCON_QDN_SEC system data type yourself, assign parameters and call it directly at one of the instructions TSEND_C, TRCV_C or TCON.

Requirements:

- Current date and time are set in the CPU.
- Your network includes at least one DNS server.
- You have configured at least one DNS server for the S7-1500 CPU.
- TLS client and TLS server have all the required certificates.

To set up a secure TCP connection to a TLS server, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_QDN_SEC in the global data block.
   The example below shows the global data block "Data_block_1" in which the tag "DNS ConnectionSEC" of the data type TCON_QDN_SEC is defined.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	DNS Connection SEC	TCON_QDN_SEC		
3	ConnPara	TCON_QDN		parameter of the TCP connection
4	InterfaceId	HW_ANY	0	not relevant
5	ID	CONN_OUC	5	connection reference / identifier
6	ConnectionType	Byte	11	type of connection: 16#0B=11=TCP/IP, 16#13
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteQDN	String[254]	'plc_1.factory127.'	fully or partially qualified domain name of rem
9	RemotePort	UInt	4000	remote UDP / TCP port number
10	LocalPort	UInt	0	local UDP / TCP port number
11	ActivateSecureConn	Bool	true	activate the security functionality of that conn
12	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a
13	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 a
14	TLSServerCertRef	UDInt	7	for Server side: Reference to own X.509 V3 se
15	TLSClientCertRef	UDInt	0	for Client side: add id of own X.509 V3 client c

Figure 3-116 Data type TCON_QDN_SEC

3. Set the connection parameters of the TCP connection in the "Start value" column. Enter the fully qualified domain name (FQDN) of the TLS server, for example, for "RemoteQDN".
4. Set the parameters for secure communication in the "Start value" column.
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "ExtTLSCapabilities": If you enter the value 1, the client validates the subjectAlternateName in the X.509v3 certificate of the server to verify the identity of the server. This validation is executed in the context of the instruction.

– "TLSServerCertRef": ID of the X.509v3 certificate (usually a CA certificate) that is used by the TLS client to validate the TLS server authentication. If this parameter is 0, the TLS client uses all (CA) certificates currently loaded in the client certificate store to validate the server authentication.

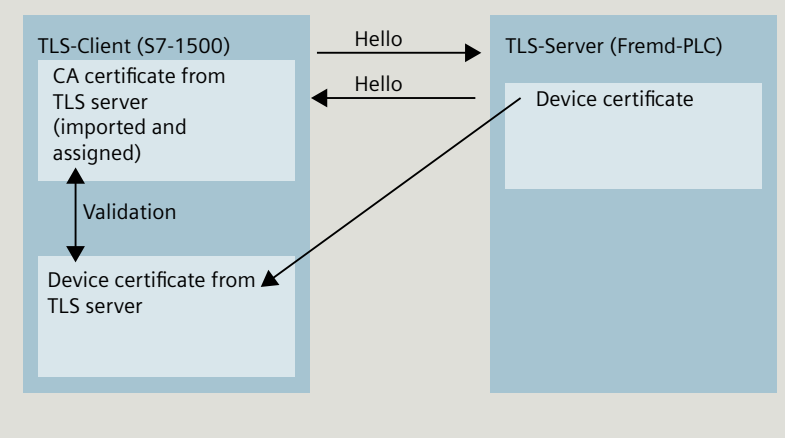


Figure 3-117 Certificate handling from the perspective of the S7-1500 as a TLS client

– "TLSClientCertRef": ID of your own X.509v3 certificate.

5. Create one of the instructions TSEND_C, TRCV_C or TCON in the program editor.
6. Interconnect the CONNECT parameter of one of the instructions TSEND_C, TRCV_C or TCON with the tags of the data type TCON_QDN_SEC.

   In the example below, the CONNECT parameter of the TCON instruction is interconnected with the tag "DNS connectionSEC" (data type TCON_QDN_SEC).

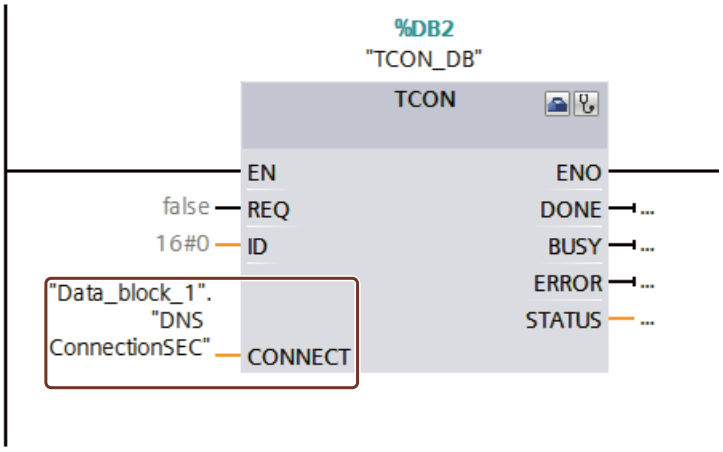


Figure 3-118 TCON instruction

Additional information

You can find more information on the TCON_QDN_SEC system data type in the STEP 7 online help.

For additional information on secure communication, refer to the section Secure Communication (Page 51).

5.6.4.2 Secure OUC of an S7-1500 CPU as TLS server to an external PLC (TLS client)

The following section describes how you can set up Open User Communication via TCP from an S7-1500 CPU as TLS server to a TLS client.

Setting up a secure TCP connection via the domain name of the communication partner

S7-1500 CPUs as of firmware version V2.0 support secure communication with addressing via a Domain Name System (DNS).

For secure TCP communication over the domain name you need to create a data block with the TCON_QDN_SEC system data type yourself, assign parameters and call it directly at one of the instructions TSEND_C, TRCV_C or TCON.

Requirements:

- Current date and time are set in the CPU.
- Your network includes at least one DNS server.
- You have configured at least one DNS server for the S7-1500 CPU.
- TLS client and TLS server have all the required certificates.

To set up a secure TCP connection to a TLS client, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_QDN_SEC in the global data block.
   The example below shows the global data block "Data_block_1" in which the tag "DNS ConnectionSEC" of the data type TCON_QDN_SEC is defined.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	DNS Connection SEC2	TCON_QDN_SEC		
3	ConnPara	TCON_QDN		parameter of the TCP connection
4	InterfaceId	HW_ANY	0	not relevant
5	ID	CONN_OUC	8	connection reference / identifier
6	ConnectionType	Byte	11	type of connection: 16#0B=11=TCP/IP, 16#13
7	ActiveEstablished	Bool	false	active/passive connection establishment
8	RemoteQDN	String[254]	''	fully or partially qualified domain name of rem
9	RemotePort	UInt	0	remote UDP / TCP port number
10	LocalPort	UInt	2010	local UDP / TCP port number
11	ActivateSecureConn	Bool	true	activate the security functionality of that conn
12	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a
13	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 a
14	TLSServerCertRef	UDInt	5	for Server side: Reference to own X.509 V3 se
15	TLSClientCertRef	UDInt	0	for Client side: add id of own X.509 V3 client c

Figure 3-119 TCON_QDN_SEC_Server

3. Set the connection parameters of the TCP connection in the "Start value" column. Enter, for example, the local ID of the TCP connection for "ID".
4. Set the parameters for secure communication in the "Start value" column.
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "TLSServerReqClientCert": Request for an X.509v3 certificate from the TLS client.

– "TLSServerCertRef": ID of your own X.509v3 certificate.

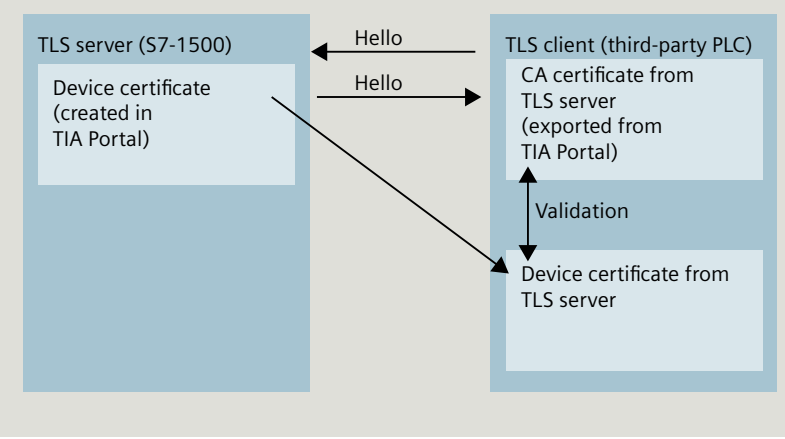


Figure 3-120 Certificate handling from the perspective of the S7-1500 as TLS server

– "TLSClientCertRef": ID of the X.509v3 certificate (or a group of X.509v3 certificates) that is used by the TLS server to validate TLS client authentication. If this parameter is 0, the TLS server uses all (CA) certificates currently loaded in the server certificate store to validate the client authentication.

5. Create one of the instructions TSEND_C, TRCV_C or TCON in the program editor.
6. Interconnect the CONNECT parameter of one of the instructions TSEND_C, TRCV_C or TCON with the tags of the data type TCON_QDN_SEC.

   In the example below, the CONNECT parameter of the TCON instruction is interconnected with the tag "DNS connectionSEC" (data type TCON_QDN_SEC).

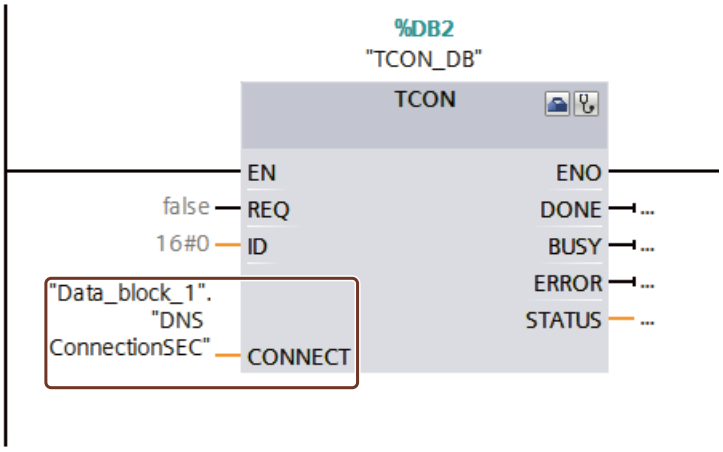


Figure 3-121 TCON instruction

More information

You can find more information about the system data types TCON_QDN_SEC in the STEP 7 online help.

For more information on secure communication, refer to the section Secure Communication (Page 51).

5.6.4.3 Secure OUC between two S7-1500 CPUs

The following section describes how you can set Secure Open User Communication via TCP between two S7-1500 CPUs. In the process one S7-1500 CPU acts as TLS client (active establishing of the connection) and the other S7-1500 CPU as TLS server (passive establishing of the connection).

Setting up a secure TCP connection between two S7-1500 CPUs

For secure TCP communication between two S7-1500 CPUs you need to create a data block with the TCON_IP_V4_SEC system data type yourself in every CPU, assign parameters and call it directly at one of the instructions TSEND_C, TRCV_C or TCON.

Requirements:

- The current date and time are set in the CPUs.
- Both S7-1500 CPUs have at least firmware version V2.0
- TLS client and TLS server have all the required certificates.

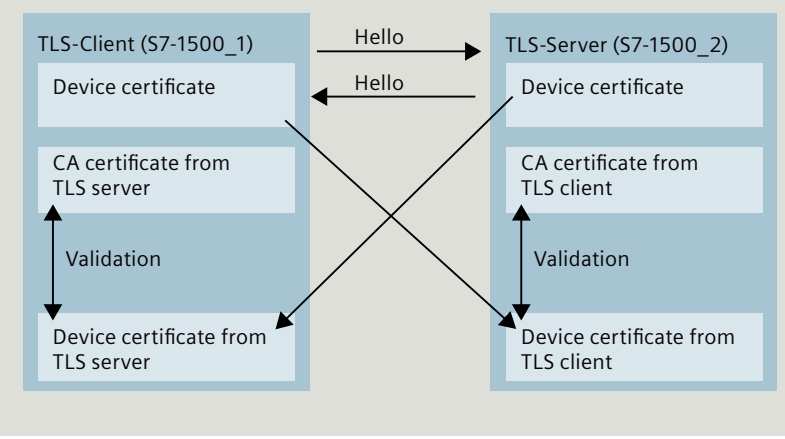


Figure 3-122 Certificate handling for Secure OUC between two S7-1500 CPUs

Settings at the TLS client

To set up a secure TCP connection in the TLS client, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_IP_V4_SEC in the global data block.
   The example below shows the global data block "Data_block_1" in which the tag "SEC connection 1 TLS-Client" of the data type TCON_IP_V4_SEC is defined.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Client	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	72	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	100	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against th
19	TLSServerCertRef	UDInt	1	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	5	for Client side: add id of own X.509 V3 client certificate; for Serv

Figure 3-123 IP_V4_SEC_Client

3. Set the connection parameters of the TCP connection in the "Start value" column. For example, enter the IPv4 address of the TLS server for "RemoteAddress".

NOTE

Connection parameter Interface ID

Note that you can enter the value "**0**" for the interface ID in the data type TCON_IP_V4_SEC. In this case, the CPU itself searches for a suitable local CPU interface.

4. Set the parameters for secure communication in the "Start value" column.
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "TLSServerCertRef": Enter the value 2 (reference to the CA certificate of the TIA Portal project (SHA256)) or the value 1 (reference to the CA certificate of the TIA Portal project (SHA1)). If you use a different CA certificate, enter the corresponding ID from the certificate manager of the global security settings.
   - "TLSClientCertRef": ID of your own X.509v3 certificate.
5. Create one of the instructions TSEND_C, TRCV_C or TCON in the program editor.
6. Interconnect the CONNECT parameter of one of the instructions TSEND_C, TRCV_C or TCON with the tags of the data type TCON_IP_V4_SEC.

Settings at the TLS server

To set up a secure TCP connection in the TLS server, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_IP_4_SEC in the global data block.
   The example below shows the global data block "Data_block_1" in which the tag "SEC connection 1 TLS-Server" of the data type TCON_IP_V4_SEC is defined.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Server	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	120	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	false	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	10	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	true	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against the
19	TLSServerCertRef	UDInt	6	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	1	for Client side: add id of own X.509 V3 client certificate; for Serv

Figure 3-124 IP_V4_SEC_Server

3. Set the connection parameters of the TCP connection in the "Start value" column. For example, enter the IPv4 address of the TLS client for "RemoteAddress".
4. Set the parameters for secure communication in the "Start value" column.
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "TLSServerReqClientCert ": Request for an X.509v3 certificate from the TLS client. Enter the value "true".
   - "TLSServerCertRef": ID of your own X.509v3 certificate.
   - "TLSClientCertRef": Enter the value 2 (reference to the CA certificate of the TIA Portal project (SHA256)) or the value 1 (reference to the CA certificate of the TIA Portal project (SHA1)). If you use a different CA certificate, enter the corresponding ID from the certificate manager of the global security settings.
5. Create one of the instructions TSEND_C, TRCV_C or TCON in the program editor.

6. Interconnect the CONNECT parameter of one of the instructions TSEND_C, TRCV_C or TCON with the tags of the data type TCON_IP_V4_SEC.
   In the example below, the CONNECT parameter of the TSEND_C instruction is interconnected with the "SEC connection 1 TLS server" tag (data type TCON_IP_4_SEC).

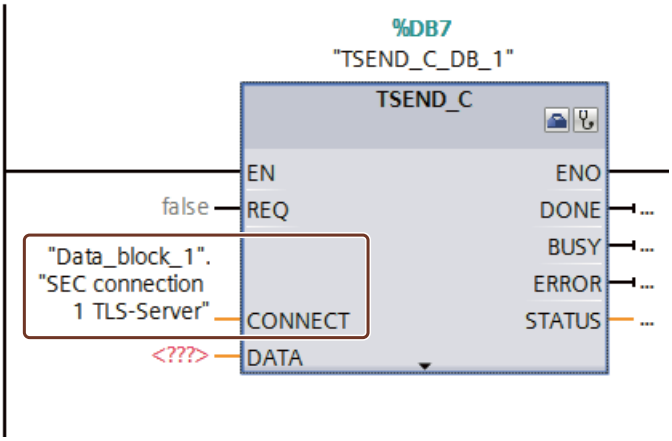


Figure 3-125 TSEND_C

More information

You can find more information about the system data types TCON_IP_4_SEC in the STEP 7 online help.

For additional information on secure communication, refer to the section Secure Communication (Page 51).

5.6.4.4 Secure OUC via CP interface

The following sections describes the particular points to be taken into consideration in the case of Secure Open User Communication via a CP interface. At least one station is an S7-1500 station with the following modules:

- S7-1500 CPU as of firmware version V2.0 (except for S7-1500 Software Controller)
- CP
  - CP 1543-1 as of firmware version V2.0
  - CP 1545-1 as of firmware version V1.0
  - CP 1543SP-1 as of firmware version V1.0

The CP acts in an S7-1500 station as a TLS client (active connection establishment) or a TLS server (passive connection establishment).

The fundamental procedure and the concept for using secure communication via a CP interface is similar to that of secure communication via the interfaces of the S7-1500 CPUs. Essentially, you have to assign the certificates to the CPU in the role of a TLS server or TLS client and not to the CPU. Other rules and procedures therefore apply. These are described below.

Handling certificates for CPs

The following applies in general: You have to be logged on at the certificate manager in the global security settings. The generation of self-signed certificates also requires logon for the global security settings. You have to have sufficient rights as a user (administrator or user with the "Standard" role with the right to "Configure security").

The starting point for the generation or assignment of certificates at the CP is the section "Security > Security properties". In this section, you log on for the global security settings.

Procedure:

1. In the network view of STEP 7, mark the CP and select the section "Security > Security properties" in the Inspector window.
2. Click on the "User logon" button.
3. Log on using your user name and password.
4. Enable the "Activate security functions" option.
   The security properties are initialized.
5. Click in the first line of the "Device certificates" table to generate a new certificate or select an existing device certificate.
6. If the communication partner is also an S7-1500 station, you also have to assign a device certificate to the communication partner with STEP 7 as described here or for the S7-1500 CPU.

Example: Setting up a secure TCP connection between two S7-1500 CPUs via CP interfaces

In order to establish secure TCP communication between two S7-1500 CPs you have to create a data block with the system data type TCON_IP_V4_SEC in each CPU, carry out the parameter assignment and call it directly at the instruction.

Requirements:

- Both S7-1500 CPUs have one of the firmware versions specified above.
- The CPs have one of the firmware versions specified above.
- TLS client and TLS server have all the required certificates.
  - A device certificate (end-entity certificate) for the CP must be generated and be located in the certificate memory of the CP. If a communication partner is an external device (for example an MES or ERP system), a device certificate also has to exist for this device.
  - The root certificate (CA certificate) with which the device certificate of the communication partner is signed must also be located in the certificate memory of the CP or in the certificate memory of the external device. If you use intermediate certificates, you have to ensure that the complete certificate path exists in the validating device. A device uses these certificates to validate the device certificate of the communication partner.
- The communication partner must always be addressed via its IPv4 address, not via its domain name.

The following figure shows the different certificates in the devices for a scenario in which both communication partners communicate via one CP. In addition, the figure shows the transfer of the device certificates during establishment of the connection ("Hello").

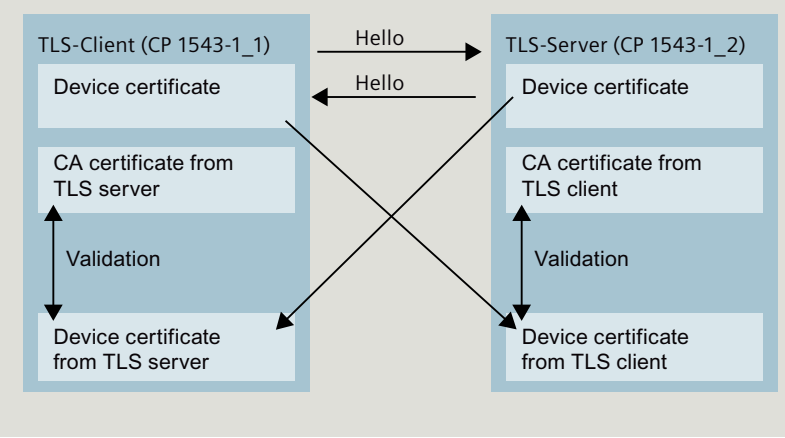


Figure 3-126 Certificate handling in secure OUC between two S7-1500 CPUs via CP interfaces.

Settings at the TLS client

To set up a secure TCP connection in the TLS client, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_IP_4_SEC in the global data block. To do so, enter the string "TCON_IP_V4_SEC" in the "Data type" field.

   The example below shows the global data block "Data_block_1" in which the tag "SEC connection 1 TLS-Client" of the data type TCON_IP_V4_SEC is defined.

   The Interface ID has the value of the HW identifier of the IE interface of the local CP (TLS client).

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Client	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	258	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	100	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against th
19	TLSServerCertRef	UDInt	1	for Server side: Reference to own X.509 V3 server certificate; fc
20	TLSClientCertRef	UDInt	5	for Client side: add id of own X.509 V3 client certificate; for Sen

Figure 3-127 IP_V4_SEC_Client

3. Set the connection parameters of the TCP connection in the "Start value" column. For example, enter the IPv4 address of the TLS server for "RemoteAddress".
4. Set the parameters for secure communication in the "Start value" column.
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "TLSServerCertRef": Enter the value 2 (reference to the CA certificate of the TIA Portal project (SHA256)) or the value 1 (reference to the CA certificate of the TIA Portal project (SHA1)).
   - "TLSClientCertRef": ID of your own X.509v3 certificate.
5. Create a TCON instruction in the program editor.
6. Connect the CONNECT parameter of the TCON instruction with the variable of data type TCON_IP_V4_SEC.

Settings at the TLS server

To set up a secure TCP connection in the TLS server, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_IP_4_SEC in the global data block.
   The example below shows the global data block "Data_block_1" in which the tag "SEC connection 1 TLS-Server" of the data type TCON_IP_V4_SEC is defined.
   The interface ID has the value of the HW identifier of the IE interface of the local CP (TLS server).

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC connection 1 TLS-Server	TCON_IP_V4_SEC		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	260	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	10	connection reference / identifier
6	ConnectionType	Byte	11	type of connetion: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	false	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of Byte		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	1	IPv4 address
13	ADDR[4]	Byte	10	IPv4 address
14	RemotePort	UInt	4711	remote UDP/TCP port number
15	LocalPort	UInt	4711	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	true	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	16#0	Bit 0: Just for client side: validate given IPv4 address against the
19	TLSServerCertRef	UDInt	6	for Server side: Reference to own X.509 V3 server certificate; fo
20	TLSClientCertRef	UDInt	1	for Client side: add id of own X.509 V3 client certificate; for Serv

Figure 3-128 IP_V4_SEC_Server

3. Set the connection parameters of the TCP connection in the "Start value" column. For example, enter the IPv4 address of the TLS client for "RemoteAddress".
4. Set the parameters for secure communication in the "Start value" column.
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "TLSServerReqClientCert": Request for an X.509v3 certificate from the TLS client. Enter the value "true".
   - "TLSServerCertRef": ID of your own X.509v3 certificate.
   - "TLSClientCertRef": Enter the value 2 (reference to the CA certificate of the TIA Portal project (SHA256)) or the value 1 (reference to the CA certificate of the TIA Portal project (SHA1)).
5. Create a TCON instruction in the program editor.
6. Connect the CONNECT parameter of the TCON instruction with the variable of data type TCON_IP_V4_SEC.

Upload device as new station

When you upload a configuration with certificates and configured secure Open User Communication as a new station into your STEP 7 project, the certificates of the CP are not uploaded, in contrast to the certificates of the CPU. After the device has been loaded as a new station, no more certificates are contained in the corresponding tables of the CPs for the device certificates.

You have to perform configuration of certificates again after the upload. Otherwise, renewed loading of the configuration results in the certificates that originally exist in the CP being deleted so that secure communication does not function.

Secure OUC connections via CPU and CP interfaces - similarities

- Connection resources:
  No differences between OUC and secure OUC. A programmed secure OUC connection uses a connection resource just like an OUC connection, irrespective of which IE/PROFINET interface communicates with the station.
- Connection diagnostics:
  No differences between OUC and secure OUC connection diagnostics.
- Loading of projects with secure OUC connections into the CPU:
  Only possible in STOP of the CPU, if certificates are loaded as well. For information on the requirements for updating loaded certificates in RUN mode, see Tip: Updating loaded certificates in RUN (Page 75).
  Recommendation: Load to device > Hardware and software. Reason: Ensuring consistency between programs with secure OUC, hardware configuration and certificates.
  The reloading of blocks that utilize further secure OUC connections is only possible in RUN mode if the certificates required for this purpose are already located on the module.

5.6.4.5 Secure OUC with Modbus TCP

For secure Modbus TCP connection you need to create a data block with one of the system data types TCON_IP_V4_SEC or TCON_QDN_SEC yourself, assign parameters and call it directly at the MB_Server or MB_CLIENT instruction.

Requirements

- S7-1500 CPU CPU firmware version V2.5 or higher
- The Modbus client (TLS client) can reach the Modbus server (TLS server) over IP communication in the network.
- TLS client and TLS server have all the required certificates.

Example: Setting up a secure Modbus TCP connection to a Modbus TCP server

The following section describes how you can set up a Secure Open User Communication over Modbus TCP from a Modbus TCP client to a Modbus TCP server.

To set up a secure connection from a Modbus TCP client (TLS client) to a Modbus TCP server (TLS server), proceed as follows:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_IP_V4 SEC in the global data block.

Data_block_1

	Name	Data type	Start value	Comment
1	Static			
2	SEC_ModbusTCP_1	TCON_IP_V4...		
3	ConnPara	TCON_IP_v4		parameter of the TCP connection
4	InterfaceId	HW_ANY	64	HW-identifier of IE-interface submodule
5	ID	CONN_OUC	15	connection reference / identifier
6	ConnectionType	Byte	11	type of connection: 11=TCP/IP, 19=UDP (17=TCP/IP)
7	ActiveEstablished	Bool	true	active/passive connection establishment
8	RemoteAddress	IP_V4		remote IP address (IPv4)
9	ADDR	Array[1..4] of B...		IPv4 address
10	ADDR[1]	Byte	192	IPv4 address
11	ADDR[2]	Byte	168	IPv4 address
12	ADDR[3]	Byte	10	IPv4 address
13	ADDR[4]	Byte	100	IPv4 address
14	RemotePort	UInt	502	remote UDP/TCP port number
15	LocalPort	UInt	502	local UDP/TCP port number
16	ActivateSecureConn	Bool	true	activate the security functionality of that connection in general
17	TLSServerReqClientCert	Bool	false	Just for server side: The TLS server requests a client certificate
18	ExtTLSCapabilities	Word	0	Bit 0: Just for client side: validate given IPv4 address against the subjectAlt
19	TLSServerCertRef	UDInt	2	for Server side: Reference to own X.509 V3 server certificate; for Client side:
20	TLSClientCertRef	UDInt	7	for Client side: add id of own X.509 V3 client certificate; for Server side: add

Figure 3-129 TCON_IP_V4_SEC

3. Set the connection parameters of the TCP connection in the "Start value" column. For example, enter the IPv4 address of the communication partner in "RemoteAddress".
4. Set the parameters for secure communication in the "Start value" column as follows:
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. In this case you can set up an unsecured Modbus TCP connection.
   - "TLSServerCertRef": Reference to the X.509v3 (CA) certificate of the Modbus TCP server, which is used by the TLS client to validate the authentication of the Modbus TCP server.
5. Create an MB_CLIENT instruction in the program editor.
6. Interconnect the CONNECT parameter of the MB_Client instruction with the tags of the data type TCON_IP_4_SEC.

5.6.4.6 Secure OUC via e-mail

Setting up a secure connection to a mail server over the CPU interface

For secure communication to a mail server you need to create a data block with one of the system data types TMAIL_V4_SEC, TMAIL_QDN_SEC yourself, assign parameters and call it directly at the TMAIL_C instruction.

Requirements

- TMAIL_C instruction version V5.0 or higher
- STEP 7 V15 and higher
- S7-1500 CPU V2.5 and higher
- You have assigned all the CA certificates of the mail server (TLS server) to the CPU (TLS client) and have downloaded the configuration to the CPU.
- Current date and time are set in the CPU.

Process for establishing a secure connection to the mail server

You can choose between two processes for establishing the secure connection to the mail server:

- SMTPS: The client attempts to immediately establish a TLS connection to the mail server ("handshake" process). If the mail server does not support TLS, then no connection is established.
- STARTTLS: Client establishes a TCP connection to the mail server. The client sends a request to "upgrade" the existing connection to a secure TLC connection over the TCP connection. If the mail server supports TLS, the client sends the command to establish a secure connection. The mail server uses the SMTP command "STARTTLS" to do this. The client then establishes a secure connection to the mail server. Advantage: If the mail server does not support TLS, client and mail server can communicate unsecured with each other.

You use the "Remote Port" setting in the data types at the block parameter "MAIL_ADDR_PARAM" to define which process is used for the communication.

Table 3-19 Port numbers for the SMTPS and STARTTLS processes

Process	Port
SMTPS:	465[1]
STARTTLS	Any (≠465)[2]

1 The TMAIL_C instruction uses SMTPS only for port 465. For all other ports STARTTLS is used.

2 According to RFC, mail servers use ports 25 and 587 for secure connections with STARTTLS. The use of other port numbers for SMTP is not RFC-compliant, successful communication with such a mail server is not guaranteed.

Example: Setting up a secure connection to a mail server over IPv4

The following section describes how to set up a secure connection to an IPv4 mail server with the TMAIL_C communication instruction.

To set up a secure connection via the IP4 address of the mail server, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TMAIL_V4_SEC in the global data block.
   The example below shows the global data block "MailConnDB" in which the tag "MailConnectionSEC" of the data type TMAIL_V4_SEC is defined.

MailConnDB

Name	Datentyp	Startwert	Kommentar
Static			
MailConnectionSEC	TMail_V4_SEC		
InterfaceId	HW_ANY	"Local~CP_1543-1_1~Ethernet-Schnittstelle_1"	Use HW-identifier of the IE-interface to specify th
ID	CONN_OUC	100	connection reference / identifier
ConnectionType	Byte	16#20	type of connection 16#20=32=TMail_V4 or TMai
ActiveEstablished	Bool	true	active / passive connection establishment
WatchDogTime	Time	T#5000ms	watchdog time to monitor SMTP server associa
MailServerAddress	IP_V4		IPv4 address of mail server
ADDR	Array[1..4] of Byte		IPv4 address
ADDR[1]	Byte	144	IPv4 address
ADDR[2]	Byte	145	IPv4 address
ADDR[3]	Byte	2	IPv4 address
ADDR[4]	Byte	20	IPv4 address
UserName	String[254]	'myName'	user name which is necessary to login into the
PassWord	String[254]	'myPW'	user password which is necessary to login into
From	EMAIL_ADDR		source mail address
LocalPartPlusAt...	String[64]	'Mustermann@'	local part of e-mail address plus "@" sign
FullQualifiedD...	String[254]	'siemens.com'	full qualified domain name part of e-mail addre
RemotePort	UInt	587	remote TCP port number
ActivateSecureConn	Bool	TRUE	activate the security functionality of that conne
ExtTLSCapabilities	Byte	16#0	for further capability extensions of the TLS hand
TLSServerCertRef	UDInt	7	Reference to the X.509 V3 (CA-) certificate of the

Figure 3-130 Data type TMAIL_V4_SEC

3. Set the connection parameters of the TCP connection in the "Start value" column. For example, enter the IPv4 address of the mail server for the "MailServerAddress".

NOTE

Connection parameter Interface ID

As of instruction version V5.0 of TMAIL_C instruction in the TMAIL_V4_SEC data type, note that you need to enter the value "**0**" for the Interface ID. In this case, the CPU itself searches for a suitable local CPU interface.

4. Set the parameters for secure communication in the "Start value" column as follows:
   - "ActivateSecureConn": Activation of secure communication for this connection. If this parameter has the value FALSE, the subsequent security parameters are irrelevant. You can set up a non-secure TCP or UDP connection in this case.
   - "TLSServerCertRef": Reference to the X.509v3 (CA) certificate of the mail server, which is used by the TLS client to validate the authentication of the mail server.
5. Create a TMAIL_C instruction in the program editor.

6. Interconnect the MAIL_ADDR_PARAM parameter of the TMAIL_C instruction with the tag of the data type TMAIL_V4_SEC.
   In the following example, the MAIL_ADDR_PARAM parameter of the TMAIL_C instruction is interconnected with the tag "MailConnectionSEC" (data type TMAIL_V4_SEC).

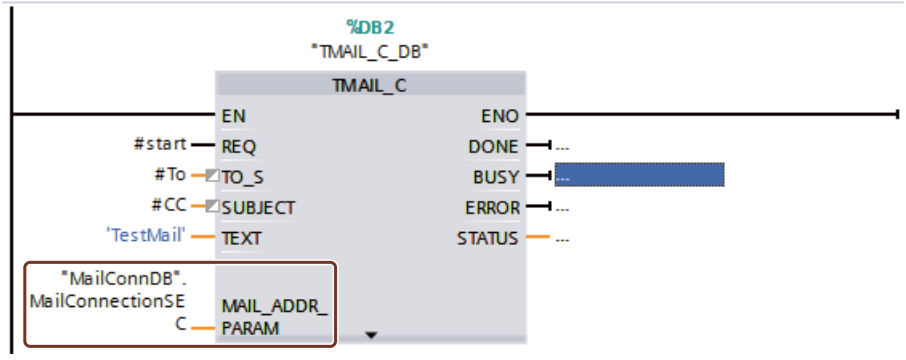


Figure 3-131 TMAIL_C instruction

Setting up a secure connection to a mail server over the interface of a communication module

For secure communication to a mail server over a communications module, you need to create a data block with one of the system data types TMAIL_V4_SEC, TMAIL_QDN_SEC or TMAIL_V6_SEC (CP only), assign parameters and call it directly in the TMAIL_C instruction.

Requirements:

- TMAIL_C instruction with version **V4.0**
- S7-1500 CPU as of firmware version V2.0 with communication module CP 1543-1 as of firmware version V2.0
- ET 200SP CPU as of firmware version V2.0 with communication module CP 1542SP-1 (IRC) as of firmware version V1.0
- You have assigned all the CA certificates of the mail server (TLS server) to the CP (TLS client) and have downloaded the configuration to the CPU.
- Current date and time are set in the CPU.

The STEP 7 online help describes how to set up a secure connection to a mail server over the interface of a communications module.

Application example

This application example (https://support.industry.siemens.com/cs/ww/en/view/46817803) shows how you can use the CP of an S7-1500 or S7-1200 station to set up a secure connection to an email server and send an email with the default application "TMAIL_C" from the S7 CPU.

More information

You can find more information about the system data types TMAIL_V4_SEC and TMAIL_QDN_SEC in the STEP 7 online help.

For additional information on secure communication, refer to the section Secure Communication (Page 51).

5.6.5 Secure PG/HMI communication

5.6.5.1 PG/HMI communication based on standardized security mechanisms

With the central components of the TIA Portal, STEP 7 and WinCC, an innovative and standardized Secure PG/PC and HMI Communication - PG/HMI communication for short - is implemented starting with version V17 together with the latest controllers and latest HMI devices.

The following CPU families are referred to in detail:

- S7-1500 controller family as of firmware version V2.9
- S7-1200 controller family as of firmware version V4.5
- Software controllers as of firmware version V21.9
- SIMATIC Drive controllers as of firmware version V2.9
- PLCSIM and PLCSIM Advanced Version V4.0

Furthermore, HMI components have been updated to support Secure PG/HMI Communication:

- Panels or PCs configured with WinCC Basic, Comfort and Advanced
- PCs with WinCC RT Professional
- WinCC Unified PCs and Comfort Panels

Also updated are SINAMICS RT SW as of version V6.1 and STARTDRIVE as of version V17.

Properties of PG/HMI communication

One characteristic of PG communication and HMI communication above all is their simplicity: Establishing an online connection from a programming device with installed TIA Portal to a CPU, for example, to load a program, requires little effort. This online connection also meets criteria such as confidentiality and integrity - based on a proven SIMATIC communication standard.

In the course of integrating machines and systems into an open IT environment, however, it must be ensured that the communication between the programming device / HMI device and the CPU is not only secure in the sense of maintaining integrity and confidentiality for sensitive data but also that this security meets generally accepted standards and is thus ready for the challenges of the future.

With TIA Portal version V14, the "Open User Communication" procedure for communication based on user programs has already been extended by the "**Secure** Open User Communication" variant. Other certificate-based communication mechanisms have become established (HTTPS, Secure SMTP over TLS or OPC UA). As of TIA Portal Version V17, PG/HMI communication has also been upgraded: Here, too, the TLS (Transport Layer Security) protocol is used to secure PG/HMI communication using standardized security mechanisms.

What has changed

Additional optional password for more security
The most noticeable change in the frame of the configuring of the above devices is the ability to assign a password to protect sensitive configuration data of the respective CPU. This refers to data such as private keys that are required for the proper functioning of certificate-based protocols (Secure Communication) - as of TIA Portal V17 also for PG/HMI communication. You can use a policy setting to check the assigned passwords as they are entered into the TIA Portal. This will ensure that your company complies with prescribed password policies.

If your machine or system does not require this protection based on the Siemens Industrial Defense-in-Depth concept, you can dispense with password assignment, for example, because another equivalent protection is present. It is possible to do without the password if you have implemented measures to prevent unauthorized access to the TIA Portal project and the configuration of the CPU.

⚠ WARNING
Without password, weak protection of private keys Note that without a password to protect trusted configuration data, the private keys for certificates required for secure communication are only weakly protected.

Certificate-based communication between PG/HMI and CPU
Because PG/HMI communication is certificate-based, you will be asked to accept the server certificate during commissioning.

Additional parameter assignment options allow you to determine the behavior of the CPU during operation: For example, you can specify that the CPU also allows connection to devices that do not support Secure PG/HMI communication.

Maintenance / replacement parts scenario
For the problem-free exchange of the CPU in replacement parts scenario, you must observe specific rules (see Rules for the replacement parts scenario (Page 87)).

More information

An overview of how to protect confidential configuration data can be found in section Protection of confidential configuration data (Page 76).

5.6.5.2 Additional settings for the secure PG/HMI communication

In addition to the assignment of a password to protect confidential PLC configuration data, you have further setting options for the behavior of the CPU during operation.

PG/PC and HMI communication mode

You can set how the CPU can communicate with programming devices and HMI devices:

- Only via secure PG/HMI communication
- Both via Secure PG/HMI communication and via the previously used PG/HMI communication, "Legacy PG/HMI communication" for short.

Procedure

1. In the CPU properties, navigate to the area "Protection & Security > Connection mechanisms".
2. Select the option you want to use.

Select certificate or generate a new certificate

If you select the connection mechanism for PG/HMI communication, you can select a PLC communication certificate for the protection of the connection in the same context or have it generated by the TIA Portal. If you have assigned a password or if you have deactivated the option to protect confidential PLC configuration data (i.e. no password has been set), then a certificate with suitable settings and a valid default name is already preset in the "Protection & Security > Connection mechanisms" area.

Procedure

If you want to have a new certificate generated by the TIA Portal or if you want to select another existing certificate:

1. In the "PLC communication certificate" field, click the three points to expand the field.
2. Select the certificate you want or click the "Add" button.
3. When adding a certificate, a dialog appears with setting options for the certificate. The purpose is set to "TLS server", you can change other parameters (such as name, hash algorithm).

The general rules for certificate management apply. For example, if you want to generate a CA certificate, the option "Global settings for the certificate manager" must be selected. You also have the option of generating a self-signed PLC certificate.

More information

Basic information on the subject of certificate management can be found in section Certificate management with TIA Portal (Page 63).

5.6.5.3 Tip for certificate-based communication between PG and CPU

The certificate-based PG/PC communication (Secure PG/PC communication) means that the communication partner of the CPU – the programming device with installed TIA Portal – must trust the device certificate of the CPU so that a connection can be loaded.

To put it simply, from the TIA Portal perspective you have the following options to trust the certificate of a CPU:

- The PG with TIA Portal is in possession of the device certificate of the CPU because it was, for example, created or imported in the project. In this case, the certificate check runs automatically and without prompting.
- The PG with TIA Portal is not in possession of the device certificate of the CPU, because the CPU was determined via "Accessible stations", for example, and is not available in the project. In this case, the TIA Portal asks the TIA Portal user whether the certificate can be trusted. This may be possible only with great effort because the CPU is not in sight, for example, and the authenticity can therefore not be checked immediately.
- The PG with TIA Portal is in possession of the CA certificate (certification authority) and all CPUs that can be reached in the network from the TIA Portal have device certificates issued by this CA certificate.

  Advantage of this solution: TIA Portal can check device certificates automatically, even if the device certificates of the communication partners are not available in TIA Portal.

The solution with a CA certificate (certification authority) is explained in more detail below.

Requirement

You can use the certification authority of the TIA Portal to create device certificates for a CPU and use the existing CA certificates to sign the device certificates. However, you can also import another certification authority into TIA Portal and use it.

Enabling the global security policies for the certificate manager is a requirement. Only with this setting you can generate CA-signed certificates.

See also here: Certificate management with TIA Portal (Page 63)

Exporting CA certificate for programming devices

To export the corresponding CA certificate after creating and assigning a certificate, follow these steps:

1. Open the certificate manager in the global security settings in the project tree.
2. Select the table "CA certificates" for the certificate to be exported.
3. Right-click to open the shortcut menu of the selected certificate.
4. Click "Export".
5. Select the export format of the certificate and the storage location.

Store CA certificate in the TIA Portal

To make the exported certificate known to a PG with TIA Portal and thus enable automatic certificate checking, follow these steps:

1. Copy the CA certificate exported in the previous step to the following directory:
   C:\ProgramData\Siemens\Automation\Certstore\Trusted
2. Start TIA Portal.
   In the "Info" tab of the Inspector window, a message appears for each CA certificate which provides information on whether the CA certificate could be successfully transferred to the CA store of TIA Portal.
   However, no detailed causes are output in case of failure.

Adding device certificates to the TIA Portal certificate revocation list (CRL)

You have the option to add individual device certificates to a certificate revocation list (CRL), for example, because the associated key is no longer considered secure.

When the TIA Portal establishes a connection to a CPU whose device certificate is in the certificate revocation list, a dialog appears in the TIA Portal asking whether you still want to trust the certificate. If you decline, the connection will not be established.

To add a device certificate to the certificate revocation list, follow these steps:

1. Copy the device certificate to the following directory:
   C:\ProgramData\Siemens\Automation\Certstore\CRL
2. Start TIA Portal.
   In the "Info" tab of the Inspector window, a message appears for each certificate which provides information about whether the certificate could be successfully transferred to the CRL store of TIA Portal.
   However, no detailed causes are output in case of failure.

5.6.5.4 CPU behavior from loading to operational readiness

To ensure that communication between the CPU and a programming device or HMI device is secure, it must first have a certificate. However, the certificate for productive operation is only issued when the project is loaded into the CPU.

To ensure that the initial loading is also secured, the CPU first creates a self-signed certificate. The following description explains the different phases of establishing a connection.

Requirement for the initial establishment of connection to load the CPU

- No password for confidential PLC configuration data available in the CPU.
  If the CPU has already been loaded and therefore already has a password for confidential PLC configuration data, this password must then match the project that is to be loaded.
- Project with CPU configuration (including password for confidential PLC configuration data) and user program is available.

- The CPU is in STOP mode.
- Programming device and CPU are directly connected to each other and are located in a protected environment, i.e. you can identify the CPU to be loaded and control the connection between CPU and programming device.

Initial establishment of connection to the CPU - provisioning phase

The first connection establishment for loading the CPU is secured by the TLS procedure in terms of Secure PG/HMI Communication.

However, the CPU uses its manufacturer device certificate (if available) or a self-signed certificate to establish this connection. The CPU can only be used to a limited extent in this phase. In this phase, the CPU waits for the provision of the password-based key information - or more simply stated, it is expecting the password for confidential PLC configuration data. This phase is referred to below as the provisioning phase. A message in the diagnostic buffer indicates that the CPU is in the provisioning phase.

When a project is loaded into the CPU, the CPU receives the project data:

- Hardware configuration including configured certificates for secure communication (OPC UA, HTTPS, Secure OUC, Secure PG/HMI Communication)
- User program

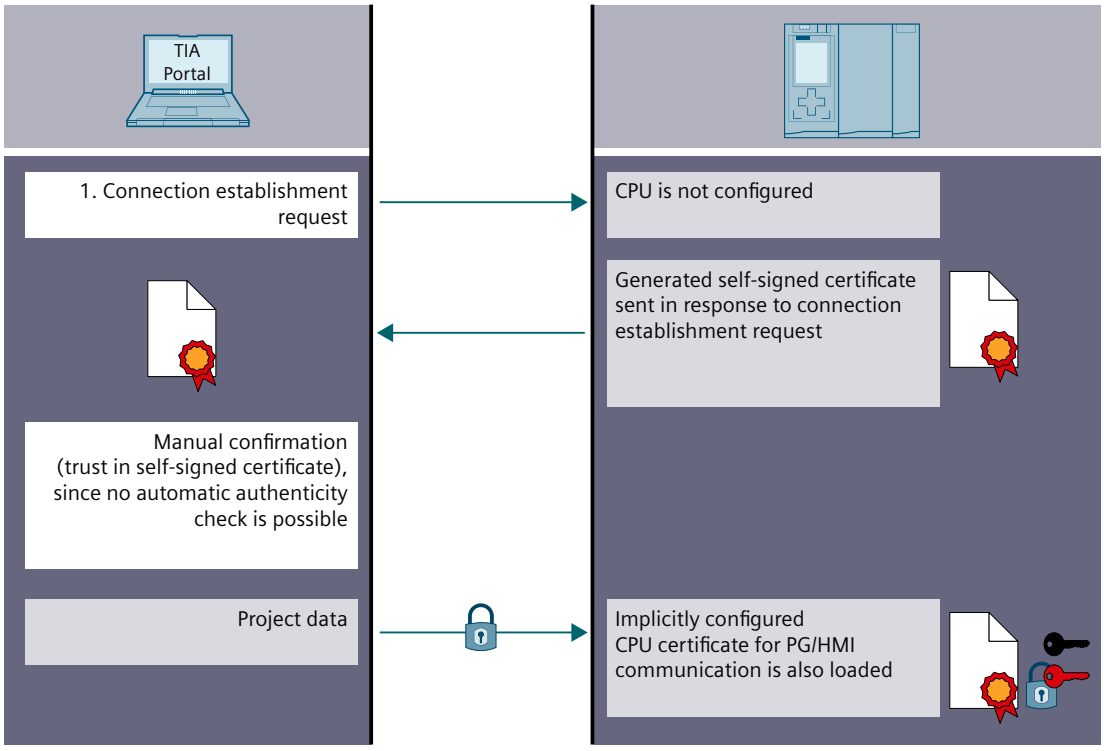


Figure 3-132 Connection establishment, provisioning phase

WARNING

Potential security risks during commissioning
During commissioning, the CPU provides a manufacturer device certificate (if available) or a self-signed certificate that you must trust in order to establish a connection. Only trust this certificate if the programming device and the CPU are in a protected network and are directly connected to each other. In an unprotected environment, these certificates can be manipulated and allow attackers to access the communication between the programming device/HMI and CPU (e.g. through man-in-the-middle attacks).

Ending the provisioning phase

TIA Portal does not store the password for confidential PLC configuration data itself or the key information generated from the password in the project.

Therefore, the password is requested in a dialog when loading the project for the first time or when loading a new project and transferred to the CPU as key information. Only after this step the CPU is able to use the protected PLC configuration data - this completes the provisioning phase and the CPU can start operating.

If you do not protect the confidential PLC configuration data with a password, there is no need to enter the password when loading the CPU for the first time. This has no influence on the flow of the PG/HMI communication but you have to consider that the confidential PLC configuration data (e.g. private keys) offer almost no protection against unauthorized access in this case.

Startup of PG/HMI communication

When the CPU is loaded and has received the CPU certificate for Secure PG/HMI Communication, the programming device connects again - this time based on the loaded CA certificate.

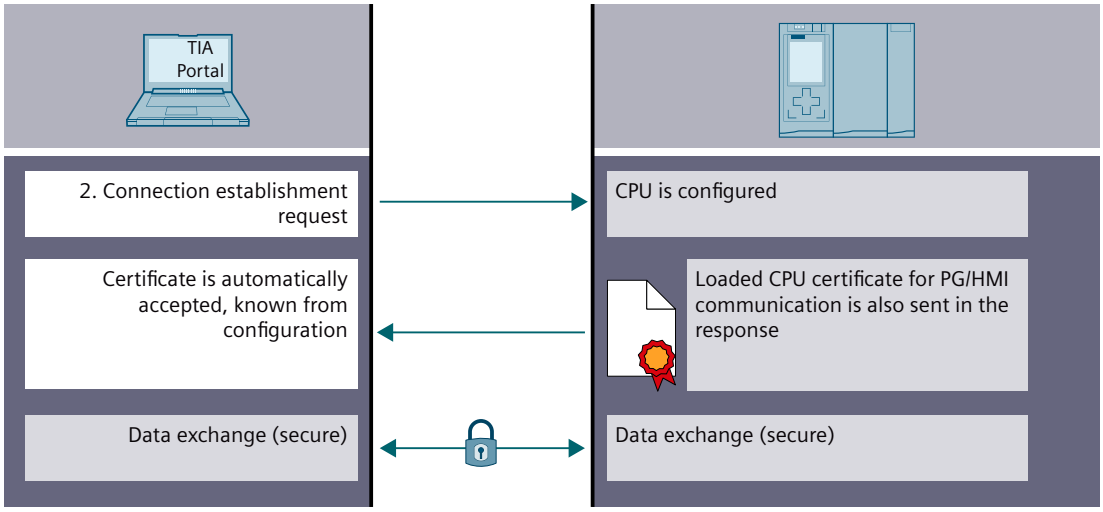


Figure 3-133 Startup of PG/HMI communication

5.6.5.5 Using secure HMI communication

As of TIA Portal version V17, the CPU and the HMI device communicate via secure HMI communication if both devices meet the requirements for this type of communication.

The basis of secure HMI communication is that the HMI device can verify the authenticity of the CPU, using the PLC communication certificate that the CPU sends when establishing communication, and considers the CPU to be "trustworthy". Secure HMI communication is only possible when this turns out to be the case.

This section describes the measures you must take for the various HMI devices to manually label the PLC communication certificate as "trustworthy".

Requirement

- CPU and HMI device support secure HMI communication.
- A current project is available on the CPU (TIA Portal V17 and higher).

Configuring secure HMI communication

1. Configure the HMI device with an alarm view.

   NOTE
   Without an alarm view you cannot identify the errors during connection establishment.

2. Configure the CPU with the required security settings. Select a PLC communication certificate to protect the HMI connection or have the TIA Portal generate a PLC communication certificate.

3. Configure the HMI connection between the CPU and the HMI device.
4. Download the project to the CPU and the HMI device. During the project transfer, the PLC communication certificate and, if necessary, a CA (Certificate Authority) certificate is transferred to the CPU and the HMI device.

NOTE

Updating and loading the CPU configuration requires reloading into the HMI device
If you change the CPU configuration and this change causes a change to the PLC communication certificate (e.g. when changing the IP address of an interface), you must also reload the PLC communication certificate of the connected HMI device.
Otherwise, communication between the HMI device and CPU is not possible.

Trusting the PLC communication certificate

During connection setup, the CPU transfers the PLC communication certificate to the HMI device.

- When the PLC communication certificate is already available on the HMI device with the "trustworthy" status, a secure HMI communication is automatically set up between the CPU and the HMI device.
- When the PLC communication certificate is not available with the "trusted" status on the HMI device, you will see an alarm in the alarm view of the HMI device informing you that the CPU is not trusted along with an error code.

NOTE

For HMI devices (Runtime V17 to V20), it is not possible to manually trust the PLC communication certificate, unless the "ChangeConnection" system function is used.

Depending on the type of your HMI device, follow these steps.

Basic Panels 2nd Generation

1. In the Start Center, select "Settings > Internet Settings > Certificate store".
2. In the "Available certificates in Device" list, select the PLC communication certificate of the CPU.
3. Press "Trust".
4. Restart the HMI runtime software.

Unified Comfort Panels

1. Open the Control Panel.
2. Select "Security > Certificates".
3. In the "Certificate store" selection list, select the entry "Other Certificates".
4. In the "Other certificates" list, select the PLC communication certificate of the CPU.
5. Press "Trust".
6. Restart the HMI runtime software.

Comfort Panels, Mobile Panels 2nd Generation

1. Open the file manager via the Windows CE desktop icon "My Device".
2. Navigate to the directory "\flash\simatic\SystemRoot\OMS\Untrusted". There you will find the PLC communication certificate of the CPU.
3. Copy the PLC communication certificate of the CPU to the directory "\flash\simatic\SystemRoot\OMS\Trusted".
4. Restart the HMI runtime software.

When the PLC communication certificate is already available on the HMI device with the "trustworthy" status, secure HMI communication can be set up. You can find more information in the operating instructions of the HMI device.

More information

You can find more information on handling certificates in the application example Application example: Using certificates with TIA Portal (https://support.industry.siemens.com/cs/ww/en/view/109769068).

5.6.5.6 Using Legacy PG/PC communication for TIA Portal

As of TIA Portal version V17, the TIA Portal and the S7-1200/S7-1500 CPU as of firmware version V4.5/V2.9 automatically communicate "securely" - the connection partners set their connection mechanisms automatically to the highest possible security method.

Only special circumstances (see Information about compatibility (Page 116)) cause a fallback to the old PG/PC communication, called "Legacy PG/PC communication".

There may be some cases in which the higher security is not desirable because it can impact the transmission rate of CPUs with weak communication performance.

Requirement

- There may be no online connections to the CPUs.
- For CPUs that are to be reached online, the option "Only permit secure PG/PC and HMI communication" must be disabled (CPU parameters in the area "Connection mechanisms").
- The communication partners are in a protected environment, for example, during the commissioning phase.

Setting the Legacy PG/PC communication

1. In the "Online" menu, select the command "Use only Legacy PG/PC communication".
2. Select the check box in front of the menu command.

Result: All online connections are set up as for TIA Portal versions < V17.

The setting remains active for the duration of the session. When you open a project, the option "Use only legacy PG/PC communication" is not set.

Behavior with enabled option "Use only Legacy PG/PC communication"

- A password to protect confidential PLC configuration data cannot be specified, modified or deleted online for CPUs. These functions require disabling the "Use only Legacy PG/PC communication" option.
- A CPU that is set to only permit secure PG/PC and HMI communication can no longer be reached online.

5.6.5.7 Information about compatibility

The following description provides information about the interaction between different TIA Portal versions with different CPU firmware versions and the effects on the type of PG/HMI connection.

Projects created with TIA Portal < V17

For example, if you have created a project with TIA Portal version V16 for an S7-1500 CPU (e.g. version V2.8), then the corresponding configuration with TIA Portal V17 can also be loaded into an S7-1500 CPU V2.9, e.g. in a spare part scenario - with the same behavior as a configuration on an S7-1500 CPU V2.8.

Even projects created with TIA Portal < V17 and transferred to a memory card work without problems in an S7-1500 CPU V2.9.

However, the concept of protecting confidential PLC configuration data applies as soon as you open the project with TIA Portal ≥ V17, update the firmware version of the CPU via a device replacement and thus save it as a CPU with a firmware version ≥ V2.9 (see Useful information for the protection of confidential PLC configuration data (Page 78)). The project can no longer be edited with previous versions of TIA Portal V17.

PG/HMI and CPU connected differently

As explained in the previous sections, the secure PG/HMI connection as of V17 between the PG/HMI device and CPU (current version) is characterized by the employed standardized communication procedure, TLS (Transport Layer Security).

You have the option of connecting a V2.9 CPU to a current programming device with TIA Portal V17 or higher and additionally, for example, to an HMI device with a runtime from the previous version: The devices automatically adjust their connection mechanisms accordingly. In order to be able to better differentiate between the two connection mechanisms, we call the previous procedure, which is based on a variant of S7 communication, "Legacy procedure".

In summary ("PG" here stands for a programming device with TIA Portal):

- PG/HMI and CPU come with the V17 (or subsequent version): TLS procedure is used.
- PG/HMI comes from a predecessor version (< V17): Legacy procedure is used - provided that you have deactivated the option "Only allow secure PG/PC and HMI communication" in the CPU properties.
- CPU comes with V17 (or higher), several PGs/HMIs are connected and come from both V17 (or higher) and previous versions: TLS + legacy procedures are used - provided that you have deactivated the option "Only allow secure PG/PC and HMI communication" in the CPU properties.

When the CPU state changes
The diagnostics buffer provides you with information if its status changes due to events in connection with the Secure PG/HMI Communication.

Examples:

- After successfully loading a configuration with a configured password, the diagnostics buffer reports that the CPU is changing from the provisioning phase to Secure Mode (TLS procedure).
- You have connected a PG with TIA Portal V17 to a CPU V2.9. If "Use only Legacy PG/PC communication" is deactivated in the Online menu, the Secure PG/HMI Communication (TLS procedure) is established automatically.

More information

Information on device or firmware-specific features such as the TLS version used can be found in section Device-dependent security features (Page 54).

5.7 SNMP

5.7.1 Activating and deactivating SNMP

The network management protocol SNMP (Simple Network Management Protocol) is used for performing monitoring and diagnostics of the network topology. SNMP uses the transport protocol UDP and knows two roles: the SNMP manager (client) and SNMP agent (server).

- The SNMP manager monitors the network nodes:
- The SNMP agents collect the various network-specific information in the individual network nodes and store it in structured form in the MIB (Management Information Base). Various services and tools (as SNMP manager) can run detailed network diagnostics with the help of these data.

SNMP is also used in a PROFINET IO system for managing the network infrastructure and the IO controller/IO devices.

NOTE
If SNMP is deactivated for a device, various options for diagnostics of the network topology (for example, using the PRONETAtool) are no longer available to you.
Example: For the topology comparison Online-Offline, the TIA Portal determines which ports are actually connected and uses SNMP for this function.

Default settings depending on the firmware version

S7-1500 CPUs have an integrated SNMP agent. Depending on the firmware version, different defaults apply to SNMP (SNMP activated or deactivated).

With S7-1500 CPUs with a FW version < V3.0, the SNMP agent is **activated** by default and can only be deactivated via a data record in the user program.

Under certain conditions, it may be useful to deactivate SNMP. Examples:

- The security guidelines in your network do not allow the use of SNMP.
- You use your own SNMP solution, e.g. with your own communications instructions.

With S7-1500 CPUs as of FW version V3.0, the SNMP agent is **deactivated** by default. The default setting "disabled" is also in effect if no configuration has been loaded or if no memory card is plugged in. STEP 7 V18 offers the following options for changing the SNMP settings for S7-1500 CPUs as of FW version V3.0:

- Configure SNMP in the CPU properties of TIA Portal.
- Activate/deactivate SNMP in the use program by transferring a data record to a PROFINET interface.

NOTE

Replacement part scenario
For compatibility reasons, an S7-1500 CPU as of firmware version V3.0 with a loaded predecessor project (CPU firmware < V3.0) behaves like the CPU in the predecessor project: SNMP is activated and "public" and "private" community strings are in effect.

Configuring SNMP

As of CPU firmware version V3.0 and TIA Portal version V18, you can change the following settings for SNMP in the CPU properties:

- Activate SNMP (default: deactivated)
- Read-only community string (default: "public")
- Read-write community string (default: "private")

You can find the settings in the "Advanced configuration > SNMP" area.

As of CPU firmware version V3.1 and TIA Portal version V19, you can additionally enable write-protected access for SNMP when SNMP is activated.

Meaning and properties of community strings

An SNMP community string, also referred to as a "community name", is like an ID or a password, which allows access to information/statistics of a device such as a router.
In this respect, to increase the security, you should change the default community strings in the CPU properties. An SNMP manager authenticates itself with the SNMP agent by transferring the community strings when there is a request.

The community strings are transferred as plain text.

- The default community string for SNMP read-only operations (GET) is "public".
- The default community string for SNMP read-write operations (SET) is "private".

Number of characters for the community string: 1-240.

You can use the following characters for the community string:

- a-z
- A-Z
- 0-9
- -
- .

Activating/deactivating SNMP in the user program

In addition to the configuration in the CPU properties, you can also activate or deactivate SNMP in the user program. To do this, transfer a data record 0xB071 to a PROFINET interface of the CPU. In this data record, it is encoded whether SNMP is to be enabled/disabled. No matter to which PROFINET interface you transfer the data record, the data record applies to all interfaces of the CPU.

One way to transfer the 0xB071 data record: Define the data set structure in a data block and transfer it in the program cycle OB (e.g. OB 1) with the "WRREC" (write record) instruction to a PROFINET interface of the CPU.

To do this, follow these steps:

1. In STEP 7, create a data block that contains the structure of data record 0xB071.
   The following table shows the structure of the data record 0xB071.

Byte	Element	Code	Explanation
0-1	BlockID	0xF003	Header
2-3	BlockLength	8	The data record length is counted starting at byte 4 "Version".
4	Version	0x01	
5	Subversion	0x00	
6-7	Reserved	-	-
8-11	SNMP controller	0.1	0: Deactivate SNMP. 1: Activate SNMP.

2. Transfer the record 0xB071 to an organization block (OB) with the "WRREC" (write record) instruction to the CPU. As a hardware identifier, use an integrated PROFINET interface of the CPU.

Interplay of SNMP configuration and user program

- The SNMP setting "activated/deactivated" via the user program is not stored permanently in the CPU. The configured setting takes effect again, for example, after each POWER OFF/POWER ON transition, loading of a new hardware configuration, or resetting to factory settings.
- When loading the configuration from the CPU ("Upload device as new station"), the configured SNMP setting (activated/deactivated) is taken into consideration. An SNMP setting previously set by data record in the user program is ignored.

- The community strings can only be changed in the configuration; the community strings cannot be set through a data record in the user program.
  However, you can activate the configured community strings by data record.
  Example:
  You have set SNMP to deactivated in the configuration of an S7-1500 CPU. You change the default community strings in the CPU properties and then load the configuration into the CPU.
  Then, you activate SNMP via data record transfer.
  Result: The changed community strings take effect.
- For S7-1500 CPUs with a firmware version < V3.0, the preset community strings ("public" and "private") are always in effect when SNMP is activated.

5.7.2 Activating/deactivating SNMP by data record transfer: Example for a CPU 1516-3 PN/DP

Introduction

You need to activate the SNMP for a CPU 1516-3 PN/DP to manage your network infrastructure, CPUs and IO devices with SNMP. The example below shows the 0xB071 data record being transferred to a PROFINET interface for this purpose.

Requirement

- CPU 1516-3 PN/DP as of FW version V2.0
- STEP 7 version V14 or higher

Solution

Transfer the data record 0xB071 to a PROFINET interface of the CPU. As a result, SNMP is enabled in all PROFINET interfaces of the CPU.

The following example shows how you can create the data record in a global data block and transfer it in a program cycle OB (for example, OB 1) to the PROFINET interface (Local~PROFINET_interface_1).

To activate SNMP for the addressed PROFINET interface of the CPU 1516-3 PN/DP, follow these steps:

1. Create a global data block.
2. Assign a name, for example, "ActivateSnmp".

3. Under "Static", create the structure of the 0xB071 data record (in the figure: "snmpRecord") and other variables for transferring the data record. The following figure shows the data block structure "ActivateSnmp".

ActivateSnmp

	Name	Data type	Start value	Re...	Ac...	Wr...	Vis...	Comment
1	Static			☐	☐	☐	☐	
2	snmpWrite	Bool	TRUE	☐	☑	☑	☑	Start writing Data record 16#B071
3	snmpRecord	Struct		☐	☑	☑	☑	Data record 16#B071
4	blockID	UInt	16#F003	☐	☑	☑	☑	Data record ID
5	blockLength	UInt	8	☐	☑	☑	☑	Length of block
6	version	USInt	1	☐	☑	☑	☑	Byte 1 of blockversion
7	subversion	USInt	0	☐	☑	☑	☑	Byte 2 of blockversion
8	reserved	UInt	0	☐	☑	☑	☑	Reserverd for future usage
9	snmpControl	UDInt	1	☐	☑	☑	☑	0: deactivate SNMP, 1: activate SNMP
10	snmpWrDone	Bool	false	☐	☑	☑	☑	writing done
11	snmpWrError	Bool	false	☐	☑	☑	☑	error while writing
12	snmpWrStatus	DWord	16#0	☐	☑	☑	☑	status of writing

Figure 3-134 Structure of the global data block "ActivateSnmp"

4. Transfer the 0xB071 data record in an OB program cycle (for example, OB 1), with the "WRREC" (write data record) instruction to the CPU 1516-3 PN/DP. You can find an example program in the next section.

Programming example for the data record transfer in OB 1

The data record 0xB071 is transferred in the following program code:

```
//----------------------------------------
// Start writing SNMP settings
//----------------------------------------
IF "ActivateSnmp".snmpWrite THEN
 IF (NOT "ActivateSnmp".snmpWriteDone)
 AND (NOT "ActivateSnmp".snmpWriteError) THEN
 "instWrrec_1"(REQ := "ActivateSnmp".snmpWrite,
 ID := "Local~PROFINET-Schnittstelle_1",
 INDEX := 16#B071,
 DONE => "ActivateSnmp".snmpWriteDone,
 ERROR => "ActivateSnmp".snmpWriteError,
 STATUS => "ActivateSnmp".snmpWriteStatus,
 RECORD := "ActivateSnmp".snmpRecord);
 END_IF;
 IF "ActivateSnmp".snmpWriteError THEN
 ; // add error handling
 END_IF;
 IF "ActivateSnmp".snmpWriteDone THEN
 "ActivateSnmp".snmpWrite := FALSE;
 END_IF;
END_IF;
```

Deactivating SNMP again

You can use the program code used above, with small changes, to deactivate SNMP. Assign the value "0" to the tag "ActivateSnmp".snmpRecord.snmpControl in the user program:

```
"ActivateSnmp".snmpRecord.snmpControl := 0;
```

The next time the "WRREC" instruction is called, SNMP will be deactivated again.

5.7.3 Activating/deactivating SNMP by data record transfer with S7-1500R/H CPUs

In S7-1500R/H systems, activate/deactivate SNMP in the user program as with standard CPUs. However, the PROFINET interfaces (X1, X2,...) of both CPUs have different hardware IDs. The PROFINET interface X1 of the left CPU, for example, has a different hardware ID as the PROFINET interface X1 of the right CPU. The S7-1500R/H system does not automatically synchronize the SNMP status (activated/deactivated) for both CPUs. An SNMP status (activated/deactivated) set by the "WRREC" instruction only affects the CPU whose PROFINET interface addresses the "WRREC" instruction.

Example:

The S7-1500R/H system is in the "RUN redundant" system state. If a PROFINET interface of the left CPU is addressed with the "WRREC" instruction, for example, the SNMP status of the left CPU is changed. The SNMP status of the right CPU remains unchanged. If the left CPU fails or is replaced, the unchanged SNMP status is in place after the SYNCUP.

Solution:

Call the "WRREC" instruction 2 times. In the first call of "WRREC", address the hardware ID of a PROFINET interface of the left CPU. Call the "WRREC" instruction again. This time, address the hardware ID of a PROFINET interface of the right CPU.

Hardware IDs for PROFINET interface X1:

- The PROFINET interface X1 of the left CPU has the hardware ID 65164 (default name: Local1~PROFINET-interface_1).
- The PROFINET interface X1 of the right CPU has the hardware ID 65364 (default name: Local2~PROFINET-interface_1).

The addressing by means of the respective hardware IDs of the PROFINET interfaces X1 is also used in the following example for calling the "WRREC" instruction for both R/H CPUs.

NOTE

Transferring the data record to the backup CPU

Call the "WRREC" instruction for the addressed PROFINET interface of the backup CPU only when the S7-1500R/H system has reached the "RUN REDUNDANT" system state. Otherwise, the data record cannot be transferred to the addressed PROFINET interface of the backup CPU.

The S7-1500R/H system signals changes to its system state, e.g. the change to "Run REDUNDANT", by calling the CPU redundancy error OB (OB 72) with the corresponding "Fault_ID".

Example: WRREC calls for both R/H CPUs

To activate/deactivate SNMP for the addressed PROFINET interface of both the CPUs by transferring data records, proceed as follows:

1. Create a global data block.
2. Assign a name, for example, "ActivateSnmp".

3. Under "Static", create the structure of the 0xB071 data record (in the figure: "snmpRecord") and other tags for transferring the data record. The following figure shows the structure of the data block "ActivateSnmp".

ActivateSnmp

	Name	Data type	Start value	Re...	Ac...	Wr..	Vis...	Comment
1	Static							
2	snmpWrite	Bool	TRUE					Start writing Data record 16#B071
3	snmpRecord	Struct						Data record 16#B071
4	blockID	UInt	16#F003					Data record ID
5	blockLength	UInt	8					Length of block
6	version	USInt	1					Byte 1 of blockversion
7	subversion	USInt	0					Byte 2 of blockversion
8	reserved	UInt	0					Reserverd for future usage
9	snmpControl	UDInt	1					0: deactivate SNMP, 1: activate SNMP
10	plcLeft	Struct						Writing status of left plc
11	snmpWrDone	Bool	false					writing done
12	snmpWrError	Bool	false					error while writing
13	snmpWrStatus	DWord	16#0					status of writing
14	plcRight	Struct						Writing status of right plc
15	snmpWrDone	Bool	false					writing done
16	snmpWrError	Bool	false					error while writing
17	snmpWrStatus	DWord	16#0					status of writing

Figure 3-135 Structure of the global data block "ActivateSnmp"

4. Add the organization block "CPU redundancy error" (OB 72) to your user program. You can find a program example for OB 72 in the next paragraph.
5. Open the program cycle OB (OB 1).
6. In OB 1, execute two "" instructions for transferring the data record to the respective addressed PROFINET interface of both CPUs. You can find a program example for OB 1 in the next paragraph.

   Result: The 0xB071 data record was transferred to the PROFINET interface of both the CPUs addressed in each case.

Programming example for the organizational blocks OB 72 and OB 1

Open the added OB 72. With the following program code, determine whether the R/H system has assumed the "RUN-REDUNDANT" state and set the starting command for the "WRREC" instructions:

```
//-----------------------------------------
// Check redundancy state and set "snmpWrite"
//-----------------------------------------
IF #Fault_ID = B#16#03 OR #Fault_ID = B#16#06 THEN
 "ActivateSnmp".snmpWrite := TRUE;
END_IF;
```

Open the program cycle OB (OB 1). With the following program code, you can run 2 "WRREC" instructions for transferring the data record to the respective addressed PROFINET interface of both the CPUs:

```
//---------------------------------------
// Start writing SNMP settings
```

```
//----------------------------------------
IF "ActivateSnmp".snmpWrite THEN
 IF (NOT "ActivateSnmp".plcLeft.snmpWrDone)
 AND (NOT "ActivateSnmp".plcLeft.snmpWrError) THEN
 // write SNMP settings for the left PLC
 "instWrrec_1"(REQ := "ActivateSnmp".snmpWrite,
 ID := "Local1~PROFINET_interface_1",
 INDEX := 16#B071,
 DONE => "ActivateSnmp".plcLeft.snmpWrDone,
 ERROR => "ActivateSnmp".plcLeft.snmpWrError,
 STATUS => "ActivateSnmp".plcLeft.snmpWrStatus,
 RECORD := "ActivateSnmp".snmpRecord);
 END_IF;
 IF "ActivateSnmp".plcLeft.snmpWrError THEN
 ; // add error handling for left plc
 END_IF;
 IF (NOT "ActivateSnmp".plcRight.snmpWrDone)
 AND (NOT "ActivateSnmp".plcRight.snmpWrError) THEN
 // write SNMP settings for the right PLC
 "instWrrec_2"(REQ := "ActivateSnmp".snmpWrite,
 ID := "Local2~PROFINET_interface_1",
 INDEX := 16#B071,
 DONE => "ActivateSnmp".plcRight.snmpWrDone,
 ERROR => "ActivateSnmp".plcRight.snmpWrError,
 STATUS =>
 "ActivateSnmp".plcRight.snmpWrStatus,
 RECORD := "ActivateSnmp".snmpRecord);
 END_IF;
 IF "ActivateSnmp".plcRight.snmpWrError THEN
 ; // add error handling for right plc
 END_IF;
 IF "ActivateSnmp".plcLeft.snmpWrDone
 AND "ActivateSnmp".plcRight.snmpWrDone THEN
 "ActivateSnmp".snmpWrite := FALSE;
 END_IF;
END_IF;
```

Deactivating SNMP again

You can use the program code used above, with small changes, to deactivate SNMP. Assign the value "0" to the tag "ActivateSnmp".snmpRecord.snmpControl in the user program:

```
"ActivateSnmp".snmpRecord.snmpControl := 0;
```

The next time the "WRREC" instructions are called, SNMP will be deactivated again.

PG communication

6

Properties

Using PG communication, the CPU or another module capable of communication exchanges data with an engineering station (for example PG, PC). The data exchange is possible via PROFIBUS and PROFINET subnets. The gateway between S7 subnets is also supported.

PG communication provides functions needed to load programs and configuration data, run tests, and evaluate diagnostic information. These functions are integrated in the operating system of the module capable of communication.

NOTE

As of TIA Portal version V17, the TLS (Transport Layer Security) protocol is supported for programming device/HMI communication to secure the data exchange between programming device/PC and CPU using standardized security mechanisms.

For more information, refer to the following sections:

- Requirements for secure communication (Page 76)
- Secure PG/HMI communication (Page 106)

Requirements

- The PG/PC is physically connected to the communication-capable module.
- If the communication-capable module is to be reached via S7 routing, the hardware configuration has to be loaded in the participating stations (S7 router and end point).

Procedure for connecting online

You must establish an online connection to the CPU for the programming device communication:

1. Select the CPU in the project tree in STEP 7.
2. Select the "Online > Go online" menu command.
3. In the "Go online" dialog, make the following settings for your online connection:
   - In the "Type of the PG/PC interface" drop-down menu, select the interface type (e.g. PN/IE)
   - In the "PG/PC interface" drop-down menu, select the PG/PC interface (e.g. ind. Ethernet card) via which you want to establish the online connection.
   - Select the interface or the S7 subnet with which the programming device/PC is physically connected from the "Connection to interface/subnet" drop-down menu.
   - If the communication-capable module is accessible via an S7 router (gateway), select the S7 router that connects the affected subnets to one another in the "1st gateway" drop-down menu.

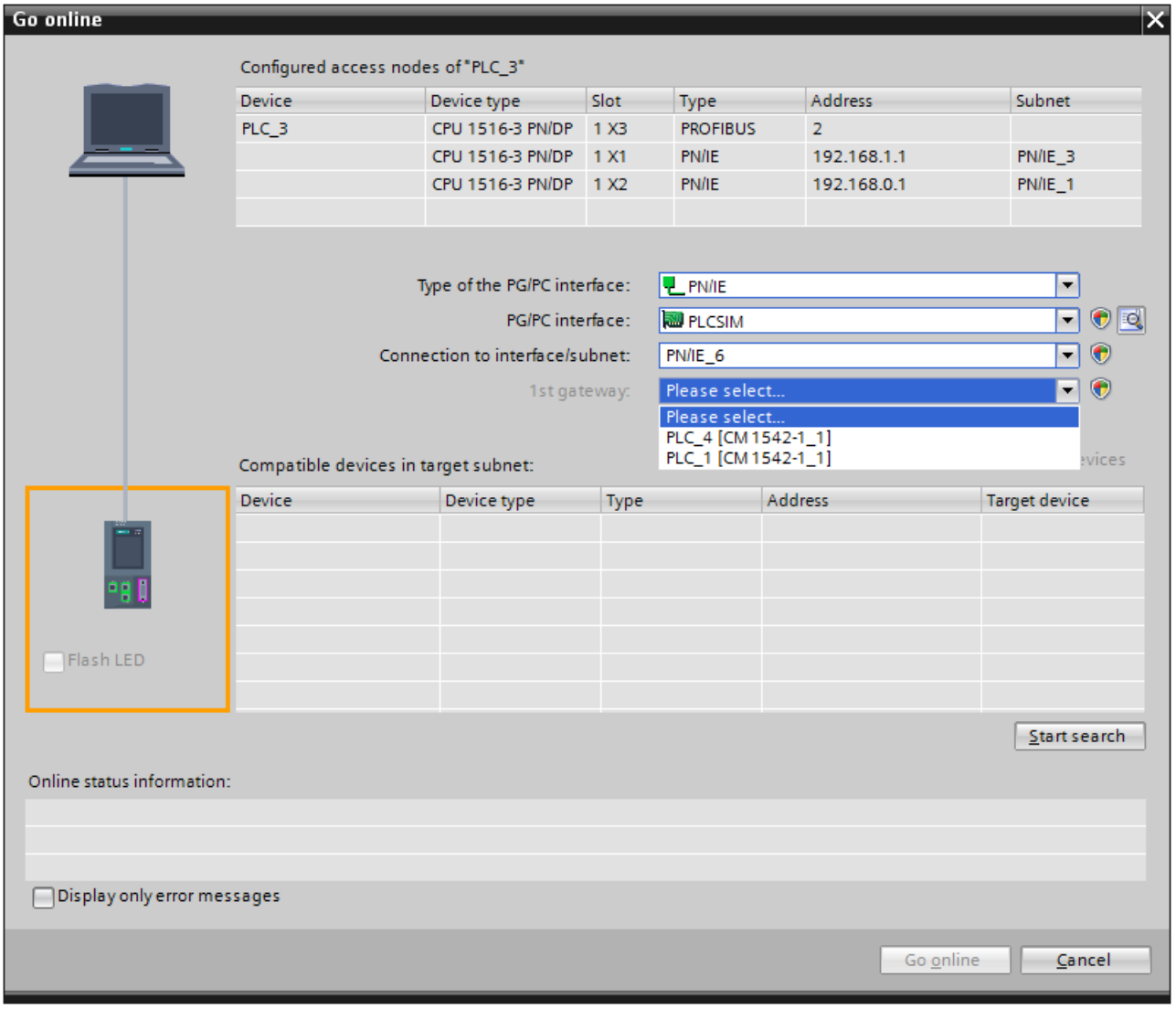


Figure 3-136 Setting up PG communication

4. Click "Start search".
   All devices that you can address with PG communication appear shortly thereafter in the table "Compatible devices in target subnet".
5. In the "Compatible devices in target subnet" table, select the relevant CPU and confirm with "Go online".

More information

You can find more information on "Go online" in the STEP 7 online help.

For information on how to protect your CPU against manipulation during loading and unauthorized access, refer to the "Protection" section in the relevant system manual, e.g. S7-1500/ET 200MP System Manual (https://support.industry.siemens.com/cs/ww/en/view/59191792).

HMI communication

7

Properties

Using HMI communication, one or more HMI devices (for example HMI Basic/Comfort/Mobile Panel) exchanges data with a CPU for operator control and monitoring with via the PROFINET or PROFIBUS DP interface. The data exchange is via HMI connections.

If you want to set up several HMI connections to a CPU, use for example:

- The PROFINET and PROFIBUS DP interfaces of the CPU
- CPs and CMs with the relevant interfaces

NOTE

As of TIA Portal version V17, the TLS (Transport Layer Security) protocol is supported for programming device/HMI communication to secure the data exchange between programming device/PC and CPU using standardized security mechanisms.

For more information, refer to the following sections:

- Requirements for secure communication (Page 76)
- Secure PG/HMI communication (Page 106)

Procedure for setting up HMI communication

As soon as you drag-and-drop a tag, for example a tag from a global data block into an HMI screen or into the HMI tag table, STEP 7 automatically sets up an HMI connection. Alternatively, you can also set up the HMI connection yourself.

To set up an HMI connection, follow these steps.

1. Configure the HMI device in an existing configuration with a CPU in the network view of the Devices & networks editor of STEP 7.
2. Select the "Connections" button and then "HMI connection" from the drop-down list.
3. Drag-and-drop a line between the end points of the connection (HMI device and CPU). The end points are highlighted in color. If the required S7 subnet does not yet exist, it is created automatically.

4. In the "Connections" tab, select the row of the HMI connection.
   In the "General" area of the "Properties" tab, you see the properties of the HMI connection, some of which you can change.

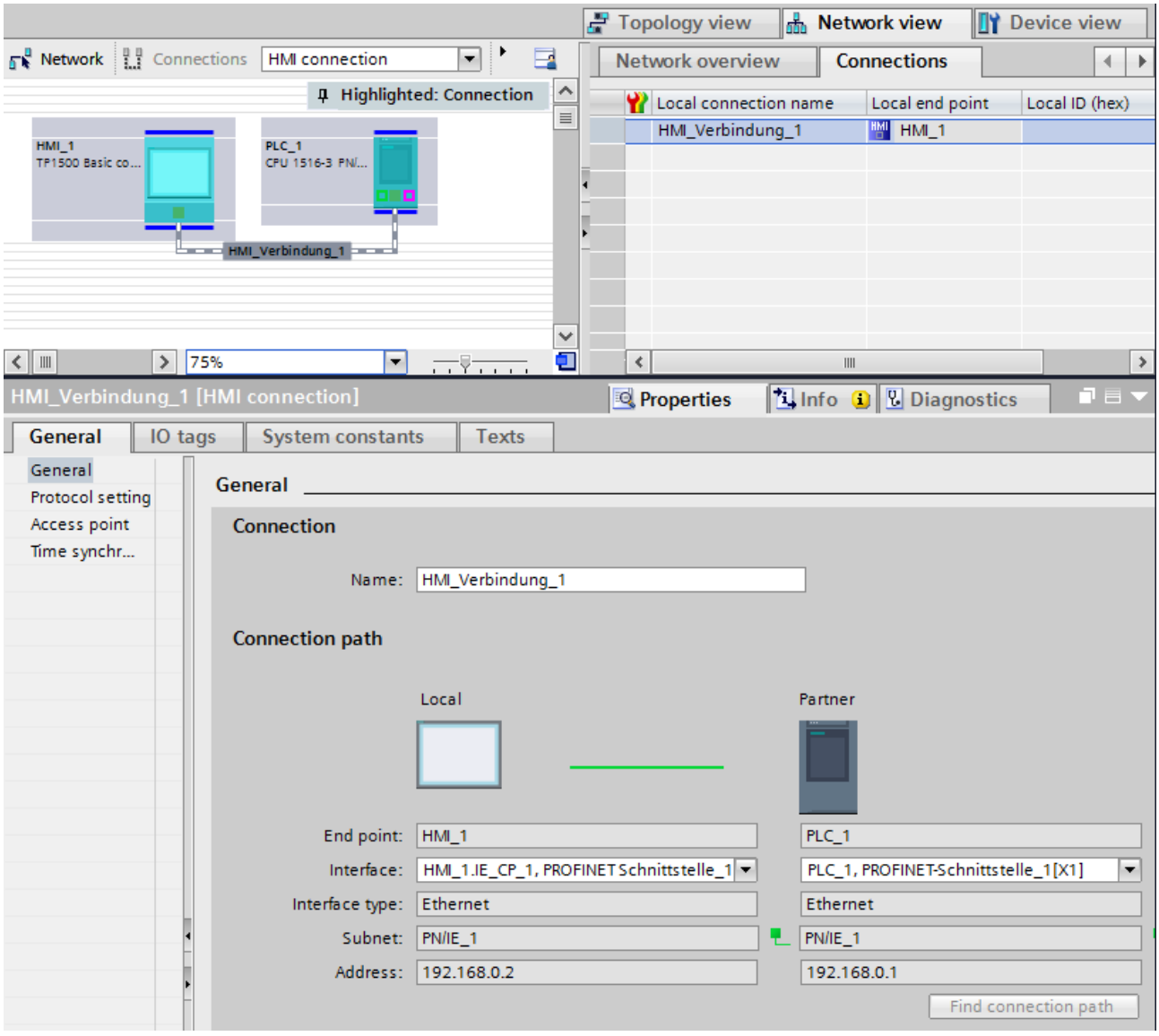


Figure 3-137 Setting up HMI communication

5. Download the hardware configuration to the CPU.
6. Download the hardware configuration to the HMI device.

More information

You can find information on S7 routing for HMI connections in the section S7 Routing (Page 397).

You can find more information on setting up HMI connections in the STEP 7 online help.

Open User Communication 8

8.1 Overview of Open User Communication

Features of Open User Communication

Through Open User Communication, also called "open communication", the CPU exchanges data with another device capable of communication. Open User Communication has the following features and characteristics:

- Open standard (communication partners can be two SIMATIC CPUs or a SIMATIC CPU and a suitable third-party device).
- Communication via various protocols (in STEP 7 known as "Connection types")
- High degree of flexibility in terms of the data structures transferred; this allows open data exchange with any communications devices as long as these support the connection types available.
- Secure Communication: To protect your automation system, you can exchange data securely over Open User Communication. With Secure Open User Communication, the data is sent signed and encrypted, see also Secure Open User Communication (Page 88).
- Open User Communication is possible in various automation systems, see technical specifications of the respective manuals.
  Examples:
  - Integrated PROFINET / Ind. Ethernet interfaces of CPUs (S7-1500, ET 200SP CPU, S7-1500 Software Controller, CPUs 1513/1516pro 2 PN)
  - PROFINET / Ind. Ethernet interfaces of communications modules (for example CP 1543-1, CM 1542-1, CP 1543SP-1)

Information on Secure Open User Communication is available in the section Secure Communication (Page 51).

Information on S7-1500R/H

You can find information on Open User Communication with the S7-1500R/H redundant system in section Communication with the redundant system S7-1500R/H (Page 435).

8.2 Protocols for Open User Communication

Protocols for Open User Communication

The following protocols are available for open communication:

Table 3-20 Transport protocols for open communication

Transport protocol	Via interface
TCP according to RFC 793	PROFINET/Industrial Ethernet
ISO-on-TCP according to RFC 1006 (Class 4)	PROFINET/Industrial Ethernet
ISO according to ISO/IEC 8073	Industrial Ethernet (only CP 1543-1)
UDP according to RFC 768	PROFINET/Industrial Ethernet
FDL	PROFIBUS

Table 3-21 Application protocols for open communication

Application protocol	Used transport protocol
Modbus TCP	**TCP** according to RFC 793
E-mail	**TCP** according to RFC 793
FTP	**TCP** according to RFC 793

TCP, ISO-on-TCP, ISO, UDP

Prior to data transfer, these protocols (except UDP) establish a transport connection to the communication partner. Connection-oriented protocols are used when potential loss of data needs to be avoided.

The following is possible with UDP:

- Unicast to one device or broadcast to all devices on PROFINET via the PROFINET interface of the CPU or the Industrial Ethernet interface of the CP 1543-1
- Multicast to all receivers of a multicast group via the PROFINET interface of the CPU or the PROFINET/Industrial Ethernet interface of the CP 1543-1

Maximum number of supported multicast groups and maximum user data lengths: See technical specifications of the respective Equipment Manuals.

Protocol for communication via PROFIBUS: FDL

Data transfer via an FDL connection (Fieldbus Data Link) is suitable for the transfer of related blocks of data to a communication partner on PROFIBUS that supports the sending and receiving of data according to the FDL service SDA (Send Data with Acknowledge) according to EN 50170, Vol 2. Both partners have the same rights; in other words, each partner can initiate sending and receiving event-driven.

In keeping with the FDL service SDN (Send Data with No Acknowledge) according to EN 50170, Vol 2, the following is possible with FDL:

- Broadcast to all devices on PROFIBUS via the PROFIBUS interface of the CM 1542-5
- Multicast to all recipients of a multicast group via the PROFIBUS interface of the CM 1542-5

Modbus TCP

The Modbus protocol is a communication protocol with linear topology based on a master/slave architecture. In the Modbus TCP (Transmission Control Protocol), the data is transmitted as TCP/IP packets.

Communication is controlled solely by suitable instructions in the user program.

E-mail and FTP

You can use email to send for example, data block contents (e.g. process data) as an attachment.

You can use the FTP connection (FTP = File Transfer Protocol) to transmit files to and from S7 devices.

The communication is controlled by instructions in the user program at the client end.

Application example: MQTT Publisher for the SIMATIC S7-1500 CPU

The "Message Queue Telemetry Transport" (MQTT) is a simple protocol on the TCP/IP level. It is suitable for the exchange of messages between devices with lower functionality and for the transfer via unreliable networks.

The application example provides a function block with which you can implement the MQTT protocol into the SIMATIC S7-1500.

You can find the application example on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109772284).

See also

SYSLOG (https://support.industry.siemens.com/cs/ww/en/view/51929235)

8.3 Instructions for Open User Communication

Introduction

You set up Open User Communication via the corresponding connection (for example, TCP connection) as follows:

- By programming in the user programs of the communications partners or
- By configuring the connection in STEP 7 in the hardware and network editor

Regardless of whether you set up the connection by programming or configuring, instructions are always required in the user programs of both communications partners for sending and receiving the data.

Setting up the connection via the user program

If the connection is set up by programming, the connection establishment and termination is implemented using instructions in the user program.

In certain application areas, it is advantageous not to set up the communication connections statically via hardware configuration, but via the user program instead. You can set up the connections via a specific application program-controlled and therefore when necessary. Programmed connection setup also allows connection resources to be released following data transfer.

A data structure is necessary for each communications connection that contains the parameters for establishing the connection (for example system data type "TCON_IP_v4" for TCP).

The system data types (SDT) are provided by the system and have a predefined structure that cannot be changed.

The various protocols have their own data structures (see table below). The parameters are stored in a data block ("connection description DB") for example of the system data type TCON_IP_v4.

There are two ways in which you can specify the DB with the data structure:

- Recommendation: Have the data block created automatically in the properties in the program editor during parameter assignment of the connection for the TSEND_C, TRCV_C and TCON instructions.
- Create the data block manually, assign parameters to it and write it directly to the instruction
  Necessary for:
  - Secure OUC
  - Connection over DNS
  - E-mail
  - FTP

You can modify the connection parameters in the "connection description DB".

This FAQ (https://support.industry.siemens.com/cs/ww/en/view/58875807) describes how to program the TCON instruction to set up a connection for Open User Communication between two S7-1500 CPUs.

Protocols, system data types and employable instructions for programmed setup

The following table shows the protocols of the Open User Communication and the matching system data types and instructions.

Table 3-22 Instructions for programmed setup of the connection

Protocol	System data type	Instructions
TCP	• TCON_QDN • TCON_IP_v4	Establish connection and send/receive data via: • TSEND_C/TRCV_C or • TCON, TSEND/TRCV or • TCON, TUSEND/TURCV (connection can be terminated via TDISCON)
ISO-on-TCP	• TCON_IP_RFC	
ISO according to ISO/IEC 8073 (Class 4)	• TCON_ISOnative[1] • TCON_Configured	

[1] This protocol can only be used with the CM 1542-5

[2] This protocol can only be used with the CP 1543-1

[3] User-defined data type

Protocol	System data type	Instructions
UDP	• TCON_IP_v4 • TADDR_Param • TADDR_SEND_QDN • TADDR_RCV_IP	Establish connection and send/receive data via: • TSEND_C/TRCV_C • TUSEND/TURCV/TRCV (connection can be terminated via TDISCON)
FDL[1]	• TCON_FDL	Establish connection and send/receive data via: • TSEND_C/TRCV_C or • TCON, TSEND/TRCV or • TCON, TUSEND/TURCV (connection can be terminated via TDISCON)
Modbus TCP	• TCON_IP_v4 • TCON_QDN • TCON_Configured	• MB_CLIENT • MB_SERVER
Email	• TMAIL_v4 • TMAIL_v6 • TMAIL_FQDN	• TMAIL_C
FTP[2]	• FTP_CONNECT_IPV4[3] • FTP_CONNECT_IPV6[3] • FTP_CONNECT_NAME[3]	• FTP_CMD

[1] This protocol can only be used with the CM 1542-5

[2] This protocol can only be used with the CP 1543-1

[3] User-defined data type

The following table shows you the different connections of the Secure Open User Communication and the matching system data types and instructions.

Secure OUC connection	System data type	Instructions
Secure TCP connection from an S7-1500 CPU as TLS client to a third-party PLC (TLS server) Secure TCP connection from an S7-1500 CPU as TLS server to a third-party PLC (TLS client)	• TCON_QDN_SEC	• TSEND_C/TRCV_C • TCON, TSEND/TRCV
Secure TCP connection between two S7-1500 stations	• TCON_IP_V4_SEC[1]	
Secure connection to a mail server[2]	• TMAIL_V4_SEC • TMAIL_QDN_SEC	• TMAIL_C (V5.0 or higher)
Secure Modbus TCP connection	• TCON_IP_V4_SEC[1] • TCON_QDN_SEC	• MB_Client • MB_Server

1 Also possible for CP 1543-1

2 Secure connection to a mail server also possible with CP1543-1 und TMAIL_C (V4.0)

Setting up the connection with connection configuration

When setting up through the configuration of the connection, the address parameters of the connection are specified in the hardware and network editor of STEP 7.

To send and receive the data, use the same instructions as when the connections are set up by programming:

Table 3-23 Instructions for sending/receiving with configured connections

Protocol	Send/receive with configured connections
Supported instructions:	
TCP	Send/receive data via: • TSEND_C/TRCV_C or • TSEND/TRCV or • TUSEND/TURCV
ISO-on-TCP	
ISO according to ISO/IEC 8073 (Class 4)	
UDP	Send/receive data via: • TSEND_C/TRCV_C or • TUSEND/TURCV
FDL	Send/receive data via: • TSEND_C/TRCV_C or • TSEND/TRCV or • TUSEND/TURCV
Modbus TCP	Not supported
Email	Not supported
FTP	Not supported

Additional instructions for open communication

You can use the following instructions for connections set up in the user program as well as for configured connections:

- T_RESET: Terminating and establishing a connection
- T_DIAG: Check the connection

Basic examples for Open User Communication

The Siemens Online Support offers you function blocks (FBs) that facilitate the handling of the instructions of the Open User Communication. You can find the function block with corresponding examples on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109747710).

More information

The STEP 7 online help describes:

- The user and system data types
- The instructions for open communication
- The connection parameters

You will find information about the allocation and release of connection resources in the section Allocation of connection resources (Page 424).

Information about the Secure Open User Communication is available in the section Secure Open User Communication (Page 88).

8.4 Open User Communication with addressing via domain names

As of firmware version V2.0, S7-1500 CPUs, ET 200SP CPUs and the CPUs 1513/1516pro-2 PN support Open User Communication with addressing via Domain Name System (DNS). A DNS client is integrated in the CPU. In the case of communication via DNS, you use domain names as an alias for IP addresses to address communication partners. Addressing of the communication partners via domain names is possible for open communication via TCP and UDP.

At least one DNS server must be located in your network as a requirement for communication via DNS.

The S7-1500 software controller supports communication via DNS for all interfaces that are assigned to the software controller.

Setting up communication via DNS

The DNS client of the CPU must know the IPv4 address of at least one DNS server so that a CPU can establish a connection to a communication partner via its domain name. The CPU supports up to 4 different DNS servers.

To set up communication via domain names for an S7-1500 CPU, follow these steps:

1. Select the CPU in the network view of STEP 7.
2. In the Inspector window, navigate to "Properties" > "General" > "Advanced configuration" > "DNS configuration".

3. Enter the IPv4 address of a DNS server in the "DNS server addresses" column of the "Server list" table.
   You can enter up to 4 IPv4 addresses of DNS servers.

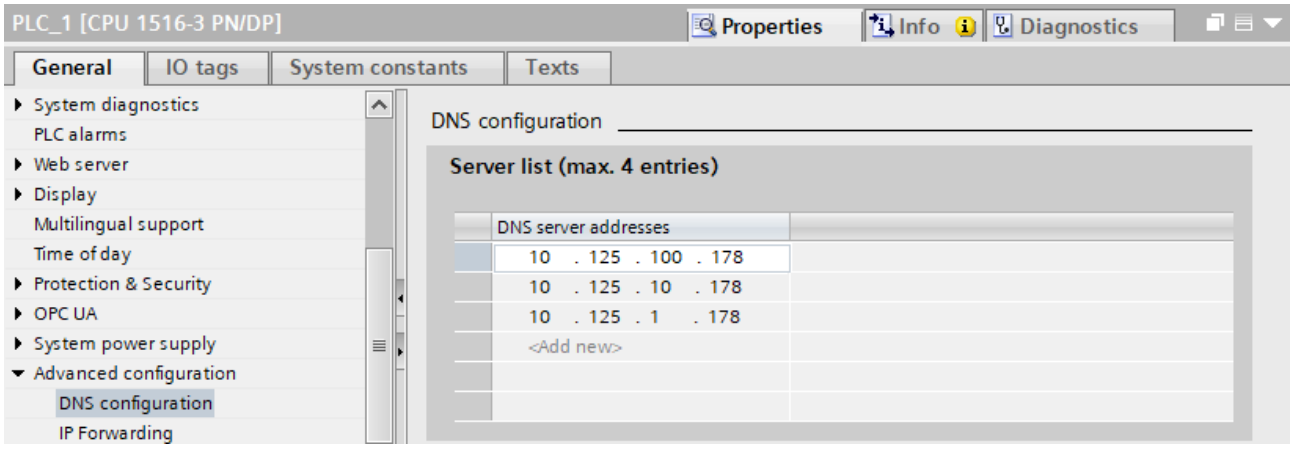


Figure 3-138 Entering DNS server addresses using a CPU 1516-3 PN/DP as an example

Setting up a TCP connection via the domain name of the communication partner

For TCP communication via the domain name you need to create a data block with the TCON_QDN system data type yourself, assign parameters and call it directly at the instruction. The TCON, TSEND_C and TRCV_C instructions support the system data type TCON_QDN:
To set up a TCP connection via the domain name of the communication partner, follow these steps:

1. Create a global data block in the project tree.
2. Define a tag of the data type TCON_QDN in the global data block.
   The example below shows the global data block "Data_block_1" in which the tag "DNS Connection1" of data type TCON_QDN is defined.

Data_block_1

		Name	Datentyp	Startwert	Kommentar
1		Static			
2		DNS Connection1	TCON_QDN		
3		InterfaceId	HW_ANY	0	not relevant
4		ID	CONN_OUC	16#0	connection reference / identifier
5		ConnectionType	Byte	16#0B	type of connection: 16#0B=11=TCP/IP, 16#13=19=UDP
6		ActiveEstablished	Bool	false	active/passive connection establishment
7		RemoteQDN	String[254]	''	fully or partially qualified domain name of remote partner
8		RemotePort	UInt	0	remote UDP / TCP port number
9		LocalPort	UInt	0	local UDP / TCP port number

Figure 3-139 Data type TCON_QDN

3. Program the parameters of the TCP connection (for example the fully qualified domain name (FQDN)) in the tag of data type TCON_QDN.
4. Create a TCON instruction in the program editor.

5. Interconnect the CONNECT parameter of the TCON instruction with the tag of the data type TCON_QDN.
   In the example below, the CONNECT parameter of the TCON instruction is interconnected with the tag "DNS connection1" (data type TCON_QDN).

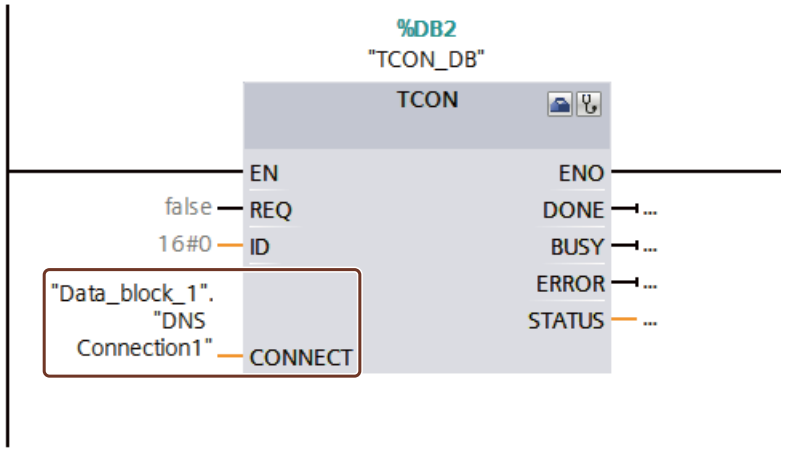


Figure 3-140 TCON instruction

Addressing a UDP connection via the domain name of the communication partner

For S7-1500 CPUs as of firmware version V2.0, you can address the recipient with its fully qualified domain name (FQDN) when sending data via UDP. With the instruction TUSEND at the parameter ADDR, you hereby reference a structure of the type TADDR_SEND_QDN.

The receiver can return an IPv4 or an IPv6 address. With the TURCV instruction at the ADDR parameter, you therefore reference a structure of the TADDR_RCV_IP type. Only this structure can include both IP address types.

NOTE

Network load

In contrast to the TCP the UDP protocol does not work connection-oriented. For every edge at the block parameter REQ, the TUSEND or TURCV command performs queries of the DNS server. This can lead to high network load or load on the DNS server.

Additional information

You can find more information about the system data types TCON_QDN, TADDR_SEND_QDN and TADDR_RCV_IP in the STEP 7 online help.

How to set up a secure TCP connection via the domain name of the communication partner is described in the section Secure Open User Communication (Page 88).

8.5 Setting up Open User Communication via TCP, ISO-on-TCP, UDP and ISO

Configuring a connection for the TSEND_C, TRCV_C or TCON instructions

Requirement: A TSEND_C, TRCV_C or TCON instruction is created in the programming editor.

1. Select a TCON, TSEND_C or TRCV_C block of Open User Communication in the program editor.
2. Open the "Properties > Configuration" tab in the inspector window.
3. Select the "Connection parameters" group. Until you select a connection partner, only the empty drop-down list for the partner end point is enabled. All other input options are disabled.

   The connection parameters already known are displayed:

   – Name of the local end point
   – Interface of the local end point

– IPv4 address of the local end point

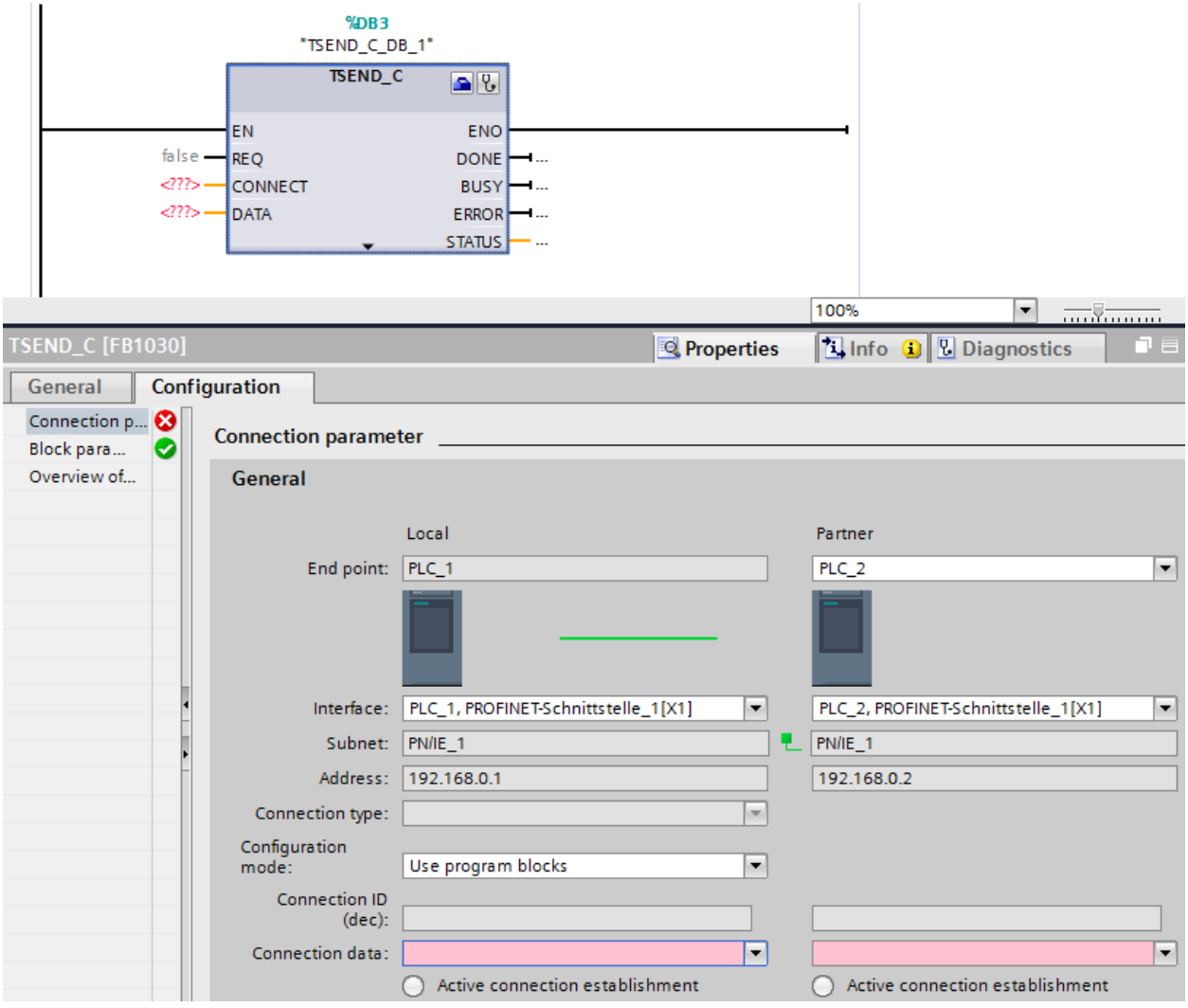


Figure 3-141 Connection parameters for TSEND_C

4. In the drop-down list box of the partner end point, select a connection partner. You can select an unspecified device or a CPU in the project as the communication partner. Certain connection parameters are then entered automatically.

   The following parameters are set:

   – Name of the partner end point
   – Interface of the partner end point
   – IPv4 address of the partner end point

   If the connection partners are networked, the name of the subnet is displayed.

5. In the "Configuration type" drop-down list, select between using program blocks or configured connections.

6. Select an existing connection description DB in the "Connection data" drop-down list or for configured connections select an existing connection under "Connection name". You can also create a new connection description DB or a new configured connection. Later, you can still select other connection description DBs or configured connections or change the names of the connection description DBs in order to create new data blocks:
   - You can also see the selected data block at the interconnection of the CONNECT input parameter of the selected TCON, TSEND_C or TRCV_C instruction.
   - If you have already specified a connection description DB for the connection partner using the CONNECT parameter of the TCON, TSEND_C or TRCV_C instruction, you can either use this DB or create a new DB.
   - If you edit the name of the displayed data block in the drop-down list, a new data block with the changed name but with the same structure and content is generated and used for the connection.
   - Changed names of a data block must be unique in the context of the communication partner.
   - A connection description DB must have the structure TCON_Param, TCON_IP_v4 or TCON_IP_RFC, depending on CPU type and connection.
   - A data block cannot be selected for an unspecified partner.

   Additional values are determined and entered after the selection or creation of the connection description DB or configured connection.

   The following is valid for specified connection partners:
   - ISO-on-TCP connection type
   - Connection ID with default of 1
   - Active connection establishment by local partner
   - TSAP ID
     for S7-1200/1500: E0.01.49.53.4F.6F.6E.54.43.50.2D.31

   The following is valid for unspecified connection partners:
   - TCP connection type
   - Partner port 2000

   The following applies for a configured connection with a specified connection partner:
   - TCP connection type
   - Connection ID with default of 257
   - Active connection establishment by local partner
   - Partner port 2000

   The following applies for a configured connection with an unspecified connection partner:
   - TCP connection type
   - Local port 2000
7. Enter a connection ID as needed for the connection partner. No connection ID can be assigned to an unspecified partner.

NOTE

You must enter a unique value for the connection ID at a known connection partner. The uniqueness of the connection ID is not checked by the connection parameter settings and there is no default value entered for the connection ID when you create a new connection.

8. Select the desired connection type in the relevant drop-down list. Default values are set for the address details depending on the connection type. You can choose between the following:
   - TCP
   - ISO-on-TCP
   - UDP
   - ISO (only with Configuration mode "Use configured connection")

   You can edit the input boxes in the address details. Depending on the selected protocol, you can edit the ports (for TCP and UDP) or the TSAPs (for ISO-on-TCP and ISO).
9. Use the "Active connection establishment" check box to set the connection establishment characteristics for TCP, ISO and ISO-on-TCP. You can decide which communication partner establishes the connection actively.

Changed values are checked immediately for input errors by the connection configuration and entered in the data block for the connection description.

NOTE

Open User Communication between two communication partners can only work when the program section for the partner end point has been downloaded to the hardware. To achieve fully functional communication, make sure that you load not only the connection description of the local CPU on the device but also that of the partner CPU as well.

Configuring connections, e.g. for TSEND/TRCV

If you want to use the instructions for TSEND/TRCV for open communication, for example, you first need to configure a connection (e.g. TCP connection).

To configure a TCP connection, follow these steps:

1. Configure the communications partners in the network view of the Devices & networks editor of STEP 7.
2. Click the "Connections" button and select the "TCP connection" connection type from the drop-down list.
3. Using drag-and-drop, connect the communication partner with each other (via an interface or local end point). If the required S7 subnet does not yet exist, it is created automatically.

   You can also set up a connection to unspecified partners.
4. Select the created connection in the network view.
5. Set the properties of the connection in the "Properties" tab in the "General" area, for example the name of the connection and the interfaces of the communications partner that will be used.

   For connections to an unspecified partner, set the address of the partner.
   You can find the local ID (reference of the connection in the user program) in the "Local ID" area.
6. In the Project tree, select the "Program blocks" folder for one of the CPUs and open OB1 in the folder by double-clicking on it. The program editor opens.
7. Select the required instruction from the "Instructions" task card, "Communication" area, "Open user communication", for example TSEND and drag it to a network of OB1.

8. At the ID parameter of the instruction, assign the local ID of the configured connection to be used for the transmission of data.
9. Interconnect the "DATA" parameter of the TSEND instruction with the user data, for example in a data block.
10. Download the hardware configuration and user program to the CPU.

Based on the procedure described above, set up the connection on the partner CPU with the instruction for receiving, TRCV, and download it to the CPU.

Point to note with ISO connections with CP 1543-1

If you use the "ISO connection" connection type, you will need to select the "Use ISO protocol" check box in the properties of the CP so that addressing using MAC addresses will work.

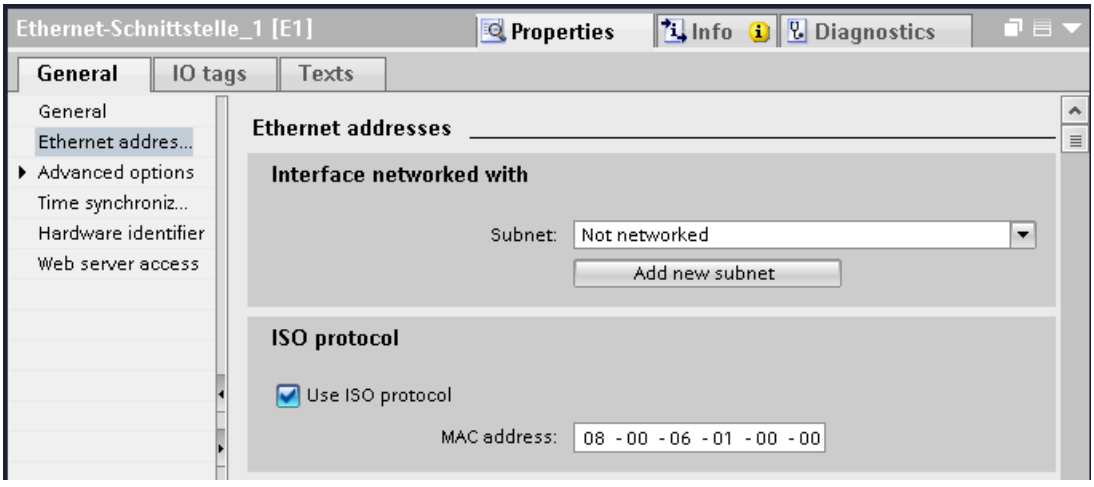


Figure 3-142 Select CP 1543-1 ISO protocol

Additional information

The STEP 7 online help describes:

- The instructions for open communication
- The connection parameters

This FAQ (https://support.industry.siemens.com/cs/ww/en/view/109479564) describes how the instructions TSEND_C and TRCV_C behave in the S7-1500.

8.6 Setting up communication over FDL

Requirements

- Configuration software: STEP 7 Professional V14
- End point of the connection: CPU S7-1500 firmware version V2.0 or higher with communication module CM 1542-5 with firmware version V2.0

Setting up a configured FDL connection

Proceed as follows to set up a configured FDL connection in STEP 7:

1. Create a TSEND_C instruction in the program editor.
2. Select the TSEND_C instruction and go to "Properties" > "General" > "Connection parameters" in the Inspector window.
3. Under End point, select the partner end point. Use one of the two partner end points below:
   - CPU S7-1500 with CM 1542-5
   - Unspecified
4. Under Configuration type, select "Use configured connection".
5. Under Connection type, select "FDL".
6. Under Interface, select the following interfaces:
   - Local: PROFIBUS interface of CM 1542-5
   - Specified partner: PROFIBUS interface of CM 1542-5
7. Under Connection data, select the setting <new>.

The figure below shows a fully configured FDL connection in STEP 7.

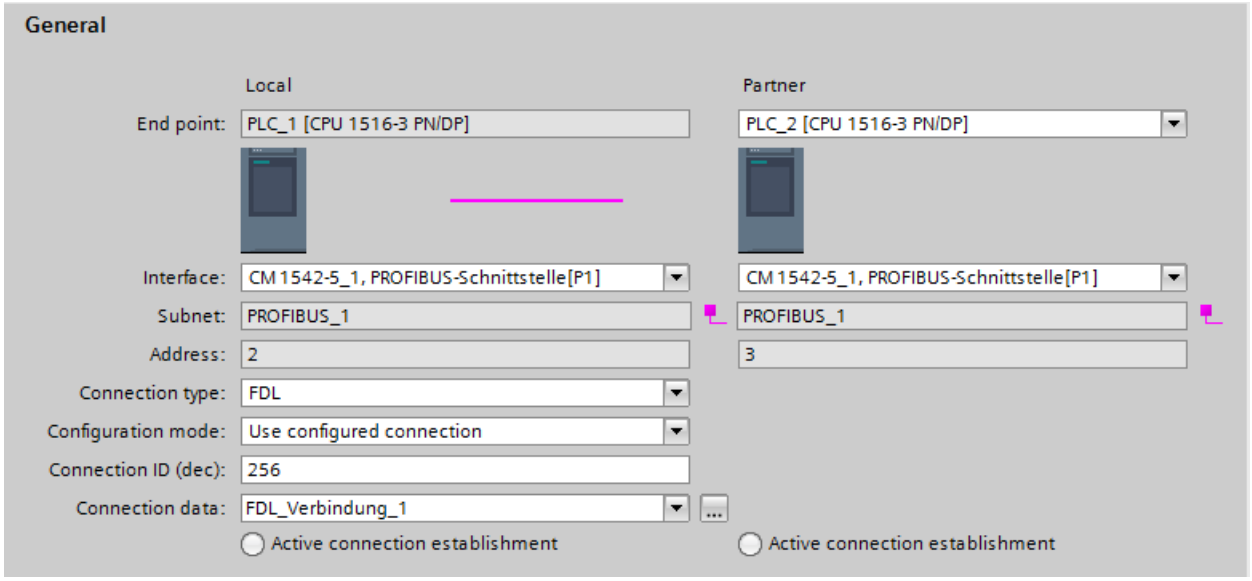


Figure 3-143 Configuring the FDL connection

Setting up an FDL connection in the user program

For communication via FDL, you need to create the data block of the TCON_FDL system data type yourself in each case, assign parameters and call it directly at the instruction. Follow these steps:

1. Create a global data block in the project tree.
2. In the global data block, define a tag of the data type TCON_FDL.
   The example below shows the global data block "FDL_connection" in which the tag "FDL_connection" of the data type TCON_FDL is defined.

FDL_connection

	Name	Data type	Start val..	R...	A...	...	V...	S...	Super...	Comment
1	Static			☐	☐	☐	☐	☐		
2	FDL_connection	TCON_FDL		☐	☑	☑	☑	☐		
3	InterfaceId	HW_ANY	0	☐	☑	☑	☑	☐		HW identifier of PB interface submodule
4	ID	CONN_OUC	16#0	☐	☑	☑	☑	☐		connection reference / identifier
5	ConnectionType	Byte	16#15	☐	☑	☑	☑	☐		type of connection: 21= FDL connection
6	ActiveEstablished	Bool	false	☐	☑	☑	☑	☐		active/passive connection establishment
7	ServiceId	Byte	16#0	☐	☑	☑	☑	☐		service id: 0 – default, 1 – SDA, 2 – SDN
8	RemotePBAddress	Byte	16#0	☐	☑	☑	☑	☐		remote ProfiBus partner address
9	LocalPBAddress	Byte	16#0	☐	☑	☑	☑	☐		local ProfiBus partner address
10	RemoteLSAP	Byte	16#0	☐	☑	☑	☑	☐		remote PB link-layer service access point
11	LocalLSAP	Byte	16#0	☐	☑	☑	☑	☐		local PB link-layer service access point

Figure 3-144 Programming an FDL connection

3. Program the parameters of the FDL connection (e.g. the PROFIBUS addresses) in the tag of the data type TCON_FDL.
4. Create a TCON instruction in the program editor.
5. Interconnect the CONNECT parameter of the TCON instruction with the tag of the data type TCON_FDL.
   In the example below, the CONNECT parameter of the TCON instruction is interconnected with the tag "FDL_Connection" (data type TCON_FDL).

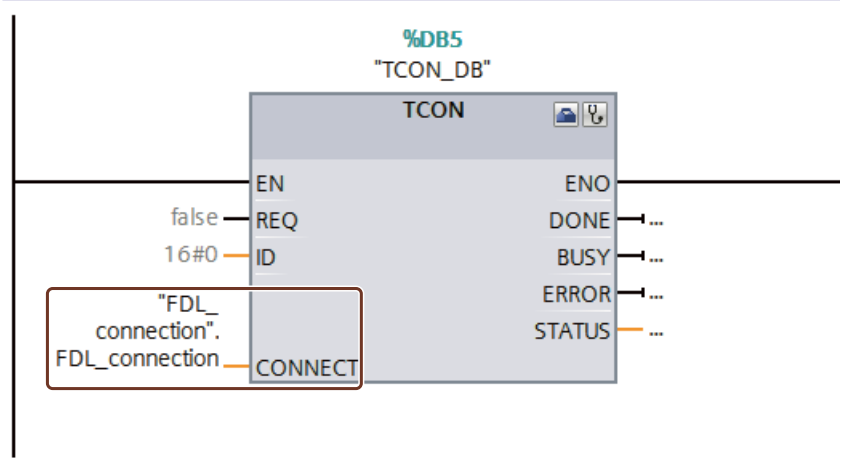


Figure 3-145 Example: TCON Instruction for FDL connection

8.7 Setting up communication with Modbus TCP

Setting up a connection for Modbus TCP via the user program

The parameter assignment takes place in the program editor at the instruction MB_CLIENT or MB_SERVER.

Procedure for setting up communication using Modbus TCP

The MB_CLIENT instruction communicates as a Modbus TCP client via the TCP connection. You establish a connection between the client and the server with the instruction, send Modbus requests to the server and receive the corresponding Modbus responses. You also control the setup of the TCP connection with this instruction.

The MB_SERVER instruction communicates as a Modbus TCP server via the TCP connection. The instruction processes connection requests of a Modbus client, receives and processes Modbus requests and sends responses. You also control the setup of the TCP connection.

Requirement: The client can reach the server via IP communication in the network.

1. Configure an S7-1500 automation system with CPU in the network view of the Devices & networks editor of STEP 7.
2. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.
3. Select the required instruction, for example MB_CLIENT, from the "Instructions" task card, "Communication" area, "Other", "MODBUS TCP" and drag it to a network of OB1.
4. Assign the parameters of the MB_CLIENT or MB_SERVER instruction. Observe the following rules:

   An IPv4 server address must be specified for each MB_CLIENT connection.

   Each MB_CLIENT or MB_SERVER connection must use a unique instance DB with one of the data structures TCON_IP_v4, TCON_QDN or TCON_Configured.

Each connection requires a unique connection ID. The connection ID and instance DB belong together in pairs and must be unique for each connection.

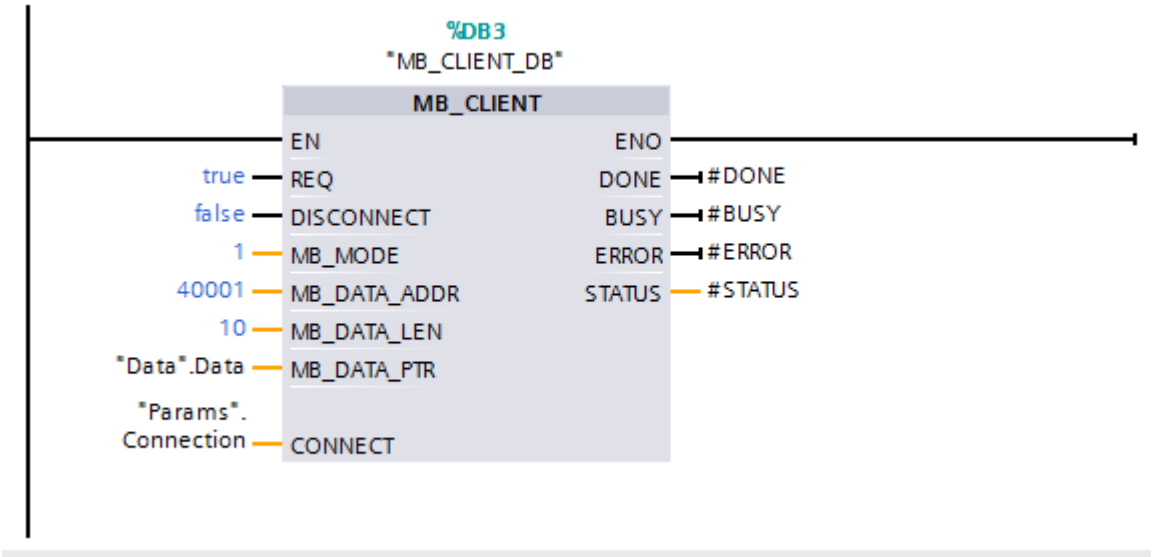


Figure 3-146 MB_CLIENT

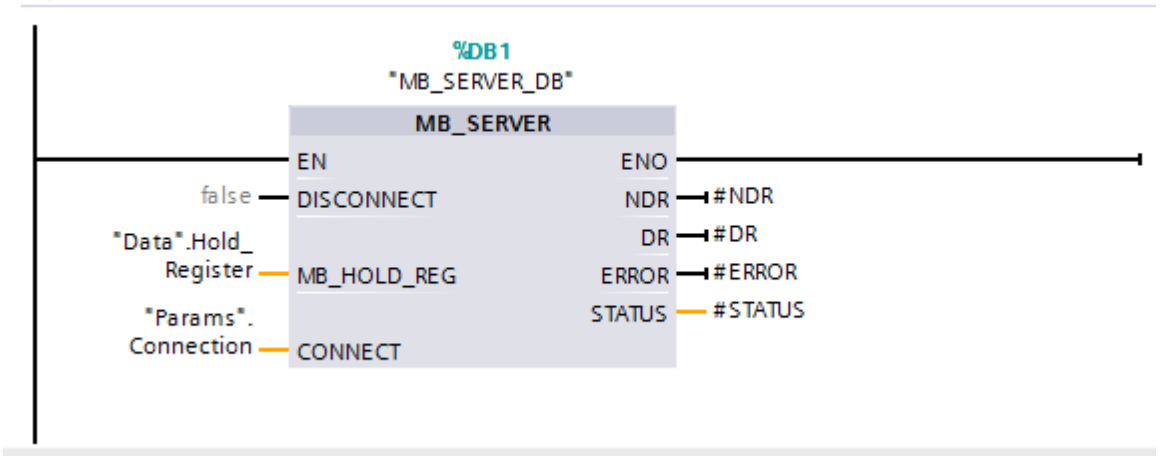


Figure 3-147 MB_SERVER

5. Download the hardware configuration and user program to the CPU.

Redundant communication over Modbus TCP

Assign parameters for redundant communication via Modbus TCP using the MB_RED_CLIENT or MB_RED_SERVER instructions:

MB_RED_CLIENT instruction:
Use the instruction "MB_RED_CLIENT" to establish a redundant connection between the client and the server, send Modbus requests, receive responses and control the connection termination of the Modbus TCP client.

MB_RED_SERVER instruction:
The "MB_RED_SERVER" instruction processes the connection requests of a Modbus TCP client, receives and processes Modbus requests and sends responses. The CPUs can:

- processing multiple server connections and
- accepting multiple connections from different clients simultaneously at one server port.

For more information on the MB_RED_CLIENT or MB_RED_SERVER instructions, refer to the STEP 7 online help.

Modbus TCP server as gateway to Modbus RTU

If you use a Modbus TCP server as a gateway to a Modbus RTU protocol, address the slave device in the serial network using the static parameter, MB_UNIT_ID. The MB_UNIT_ID parameter corresponds to the field of the slave address in the Modbus RTU protocol. The MB_UNIT_ID parameter in this case would forward the request to the correct Modbus RTU slave address.

You do not have to program the gateway function yourself.

You can find the MB_UNIT_ID parameter in the instance data block associated with MB_CLIENT instruction.

You can find more information on the MB_UNIT_ID parameter in the STEP 7 online help.

Reference

- This FAQ (https://support.industry.siemens.com/cs/ww/en/view/94766380) describes how to program and configure the Modbus TCP communication between two S7-1500 CPUs.
- This FAQ (https://support.industry.siemens.com/cs/ww/en/view/102020340) describes how to program and configure Modbus TCP communication between an S7-1500 CPU and an S7-1200 CPU.

8.8 Setting up communication via e-mail

Setting up a connection for e-mail via the user program

For communication using e-mail, you need to create the data block of the relevant system data type yourself, assign parameters and call the instruction directly. This procedure is introduced below.

Procedure for setting up communication using e-mail

A CPU can send e-mails. To send e-mails from the user program of the CPU, use the TMAIL_C instruction.

Requirement: The SMTP server can be reached via the IPv4 network.

1. Configure an S7-1500 automation system with CPU in the network view of the Devices & networks editor of STEP 7.
2. Assign parameters to the instruction TMAIL_C, for example enter the subject of the e-mail in Subject.

3. In a global data block create a variable of the type TMAIL_v4, TMAIL_v6 (only CP 1543-1) or TMAIL_FQDN (only CP 1543-1).
4. Set the connecting parameters of the TCP connection in the variable in the "Start value" column. Enter the IPv4 address of the mail server, for example, for the "MailServerAddress" (for TMAIL_v4)

   NOTE

   Connection parameter Interface ID
   Note that you can enter the value "**0**" for the interface ID with instruction version V5.0 or higher of the instruction TMAIL_C in the data type TMAIL_V4_SEC. In this case, the CPU itself searches for a suitable local CPU interface.

   Interconnect the variable to the MAIL_ADDR_PARAM parameter of the TMAIL_C instruction.
5. Download the hardware configuration and user program to the CPU.

Additional information

The STEP 7 online help describes:

- The system data types
- The instructions for open communication
- The connection parameters

8.9 Setting up communication via FTP

Setting up a connection for FTP via the user program

For communication via FTP, you need to create the data block of the relevant system data type yourself, assign parameters and call the instruction directly. This procedure is introduced below.

FTP client and server functionality

Files can be sent by a CPU to an FTP server and can be received from the FTP server. Communication with FTP is only possible for the S7-1500 using the CP 1543-1. The CP can be an FTP server, FTP client or both. FTP clients can also be third-party systems/PCs.

For the FTP server functionality, configure the CP accordingly in STEP 7.

You can use the FTP client functionality to implement, for example, the establishment and termination of an FTP connection, the transfer and deletion of files on the server. For the FTP client functionality, use the FTP_CMD instruction.

Procedure for setting up FTP server functionality

Requirement: The FTP server can be reached via the IPv4 network.

1. Configure an S7-1500 automation system with CPU and CP 1543-1 in the device view of the Devices & networks editor of STEP 7.

   At the same time, you need to select the option "Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...)" in the HW configuration of the S7-1500 CPU under the "Protection" area navigation in the section "Connection mechanisms".
2. Make the following settings in the properties of the CP under "FTP configuration":
   - Select the "Use FTP server for S7 CPU data" check box.
   - Assign the CPU, a data block and a file name under which the DB for FTP will be stored.

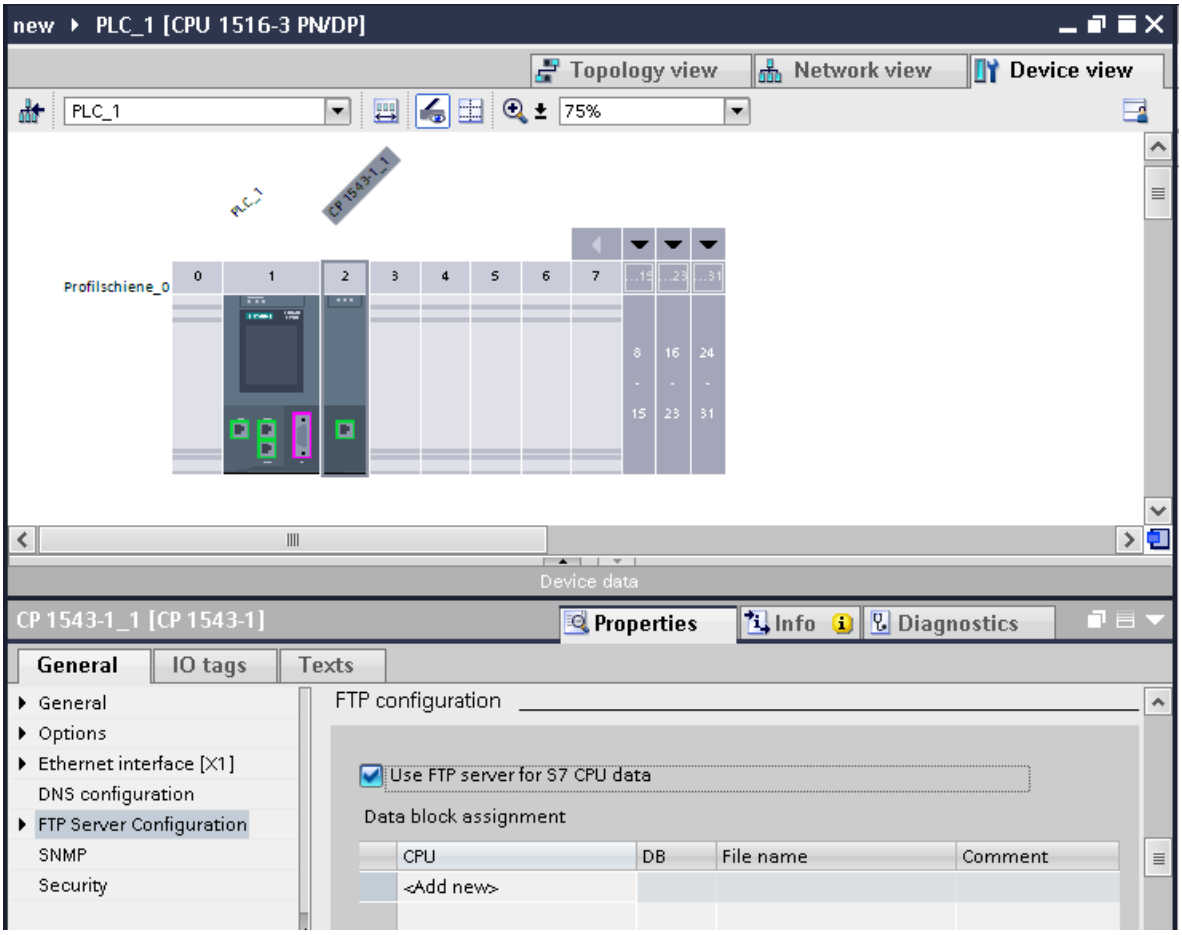


Figure 3-148 Setting up the FTP configuration

3. Download the hardware configuration to the CPU.

Procedure for setting up FTP client functionality

Requirement: The FTP server can be reached via the IPv4 network**.**

1. Configure an S7-1500 automation system with CPU and CP 1543-1 in the device view of the Devices & networks editor of STEP 7.

   At the same time, you need to select the check box "Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...)" in the HW configuration of the S7-1500 CPU under the "Protection" area navigation in the section "Connection mechanisms".
2. Call the FTP_CMD instruction in the user program of the CPU.
3. Set the connection parameters for the FTP server in the FTP_CMD instruction.
4. Create a global DB and within this DB a tag of the type FTP_CONNECT_IPV4, FTP_CONNECT_IPV6 or FTP_CONNECT_NAME.
5. Interconnect the tag within the data block with the FTP_CMD instruction.
6. For the connection to the FTP server, specify the following in the DB:
   – The user name, the password and the IP address for the FTP access in the relevant data type (FTP_CONNECT_IPV4, FTP_CONNECT_IPV6 or FTP_CONNECT_NAME)
7. Download the hardware configuration and user program to the CPU.

Application examples

- Application example: FTP communication with S7-1500 and CP 1543-1
  You can find the application example on the Internet (https://support.industry.siemens.com/cs/ww/en/view/103550797).
- Application example: FTP client communication with S7-1200/1500
  You can find the application example on the Internet (https://support.industry.siemens.com/cs/ww/en/view/81367009).

Additional information

The STEP 7 online help describes:

- The system data types
- The instructions for open communication
- The connection parameters

8.10 Establishment and termination of communications relations

Establishment and termination of communications

The table below shows the establishment and termination of communications as part of open communication.

Table 3-24 Establishment and termination of communications

Setting up the connection	Establishing communication	Terminating communication
With the user program	After downloading the user program to the CPUs: The passive communications partner sets up the local connection access by calling TSEND_C/TRCV_C or TCON. Calling TSEND_C/TRCV_C or TCON on the active partner starts connection establishment. If the connection could be established, there is positive feedback to the instructions in the user program. After you have terminated a connection using the instruction T_RESET, the connection is reestablished. If the connection aborts, the active partner attempts to re-establish the connection. This applies only if the connection was successfully established beforehand with TCON.	• Using the TSEND_C/TRCV_C, TDISCON and T_RESET instructions • When the CPU changes from RUN to STOP mode • With POWER OFF/POWER ON on a CPU
By configuring a connection	After downloading the connection configuration and the user program to the CPUs.	By deleting the connection configuration in STEP 7 and downloading the changed configuration to the CPU.

S7 communication

9

Characteristics of S7 communication

S7 communication as homogeneous SIMATIC communication is characterized by vendor-specific communication between SIMATIC CPUs (not an open standard). S7 communication is used for migration and for connecting to existing systems (S7-300, S7-400).

For data transfer between two S7-1500 automation systems, we recommend that you use open communication (see section Open User Communication (Page 129)).

Properties of S7 communication

Using S7 communication, the CPU exchanges data with another CPU. Once the user has received the data at the receiver end, the reception data is automatically acknowledged to the sending CPU.

The data is exchanged via configured S7 connections. S7 connections can be configured at one end or at both ends.

S7 communication is possible via:

- Integrated PROFINET or PROFIBUS DP interface of a CPU
- Interface of a CP/CM

S7 connections configured at one end

For an S7 connection configured at one end, the configuration for this connection takes place in only one communication partner and is only downloaded to it.

A one-sided S7 connection can be configured to a CPU that is only a server of an S7 connection (e.g. CPU 315-2 DP). The CPU is configured and the address parameters and interfaces are thus known.

In addition, a one-sided S7 connection can be configured to a partner who is not in the project and whose address parameters and interface are therefore not known. You need to enter the address; it is not checked by STEP 7. The partner is initially unspecified (no partner address is registered when you create the S7 connection). Once you enter the address, it is "unknown" (i.e. it is named, but the project is unknown).

This makes it possible to use S7 connections beyond the boundaries of a project. The communication partner is unknown to the local project (unspecified) and is configured in another STEP 7 or third-party project.

S7 connections configured at both ends

When an S7 connection is configured at both ends, the configuration and download of the configured S7 connection parameters takes place in both communication partners.

Instructions for S7 communication

For S7 communication with S7-1500, the following instructions can be used:

- PUT/GET

  You write data to a remote CPU with the PUT instruction. You can use the GET instruction to read data from a remote CPU. The PUT and GET instructions and are one-sided instructions, i.e. you need only an instruction in one communication partner. You can easily set up the PUT and GET instructions via the connection configuration.

  NOTE

  Data blocks for PUT/GET instructions
  When using the PUT/GET instructions, you can only use data blocks with absolute addressing. Symbolic addressing of data blocks is not possible.
  You must also enable this service for protection in the CPU configuration in the "Protection" area.

  This FAQ (https://support.industry.siemens.com/cs/ww/en/view/82212115) provides information about how to configure and program an S7 instruction and the GET and PUT communication instructions for data exchange between two S7-1500 CPUs.

- BSEND/BRCV

  The BSEND instruction sends data to a remote partner instruction of the type BRCV. The BRCV instruction receives data from a remote partner instruction of the type BSEND. You use the S7 communication via the BSEND/BRCV instruction pair for secure transmission of data.

- USEND/URCV

  The USEND instruction sends data to a remote partner instruction of the type URCV. The URCV instruction receives data from a remote partner instruction of the type USEND. You use the S7 communication via the USEND/URCV instruction pair for fast, non-secure transmission of data regardless of the timing of the processing by the communications partner; for example for operating and maintenance messages.

S7 communication via PROFIBUS DP interface in slave mode

You can find the "Test, commissioning, routing" check box in STEP 7 in the properties of the PROFIBUS DP interface of communications modules (e.g. CM 1542-5). Using this check box, you decide whether the PROFIBUS DP interface of the DP slave is an active or passive device on PROFIBUS.

- Check box selected: The slave is an active device on PROFIBUS.
- Check box cleared: The DP slave is a passive device on PROFIBUS. You can only set up S7 connections configured at one end for this DP slave.

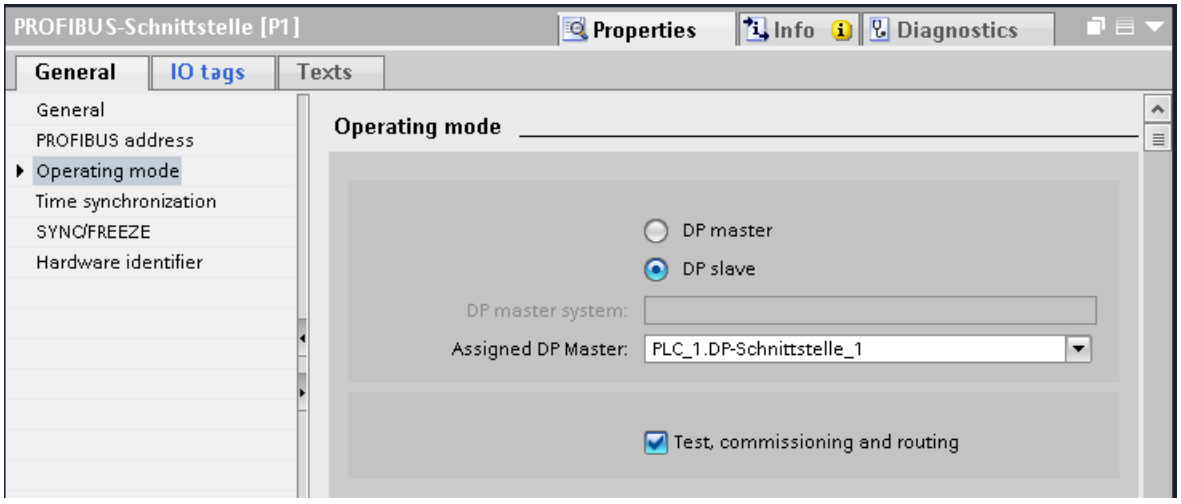


Figure 3-149 "Test, commissioning, routing" check box

Configuring S7 connections for PUT/GET instructions

You can create S7 connections and assign the parameters for these in the connection parameter assignment of the PUT/GET instructions. Changed values are checked immediately by the connection parameter assignment for input errors.

Requirement: A PUT or GET instruction is created in the programming editor.

To configure an S7 connection using PUT/GET instructions, follow these steps:

1. In the program editor, select the call of the PUT or GET instruction.
2. Open the "Properties > Configuration" tab in the inspector window.
3. Select the "Connection parameters" group. Until you select a connection partner, only the empty drop-down list for the partner end point is enabled. All other input options are disabled.

   The connection parameters already known are displayed:

   – Name of the local end point
   – Interface of the local end point

– IPv4 address of the local end point

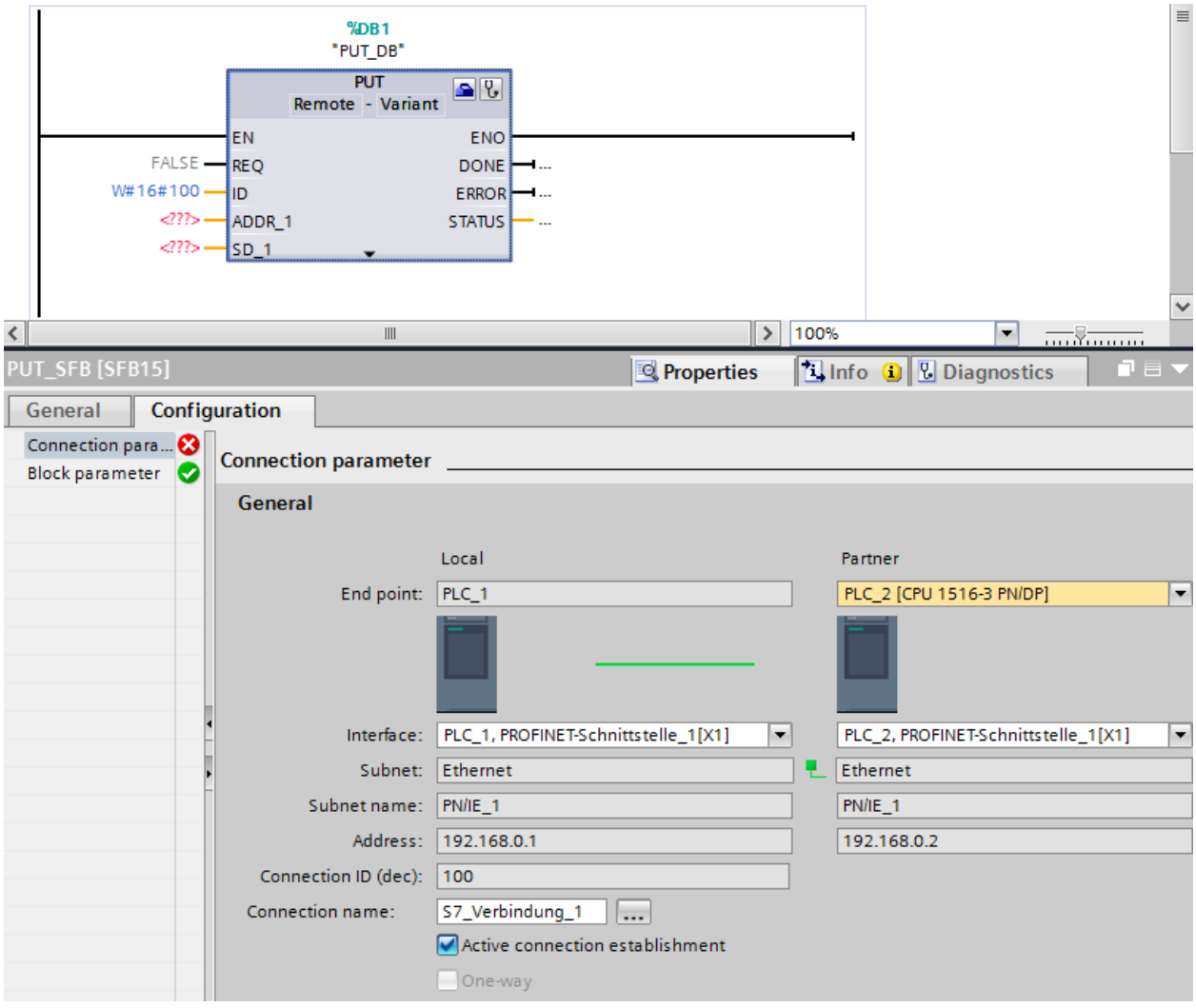


Figure 3-150 Connection configuration for PUT instruction

4. In the drop-down list box of the partner end point, select a connection partner. You can select an unspecified device or a CPU in the project as the communication partner.

   The following parameters are automatically entered as soon as you have selected the connection partner:

   – Name of the partner end point
   – Interface of the partner end point. If several interfaces are available, you can change the interface as required.
   – Interface type of the partner end point
   – Subnet name of both end points
   – IPv4 address of the partner end point
   – Name of the connection which is used for the communication.

5. If required, change the connection name in the "Connection name" input box. If you want to create a new connection or edit an existing connection, click on the "Select connection" button on the right side next to the input box for the connection name.

NOTE

The PUT and GET instructions between two communication partners can only run if both the hardware configuration and the program part for the partner end point have been loaded into the hardware. To achieve fully functional communication, make sure that you load not only the connection description of the local CPU on the device but also that of the partner CPU as well.

Configuring S7 connections for e.g. BSEND/BRCV

If you want to use the instructions for BSEND/BRCV for S7 communication, for example, you first need to configure an S7 connection.

To configure a S7 connection, follow these steps:

1. Configure the communications partners in the network view of the Devices & networks editor of STEP 7.
2. Select the "Connections" button and the "S7 connection" entry from the drop-down list.
3. Using drag-and-drop, connect the communication partner with each other (via an interface or local end point). If the required S7 subnet does not yet exist, it is created automatically.

   You can also set up a connection to unspecified partners.
4. In the "Connections" tab, select the row of the S7 connection.
5. Set the properties of the S7 connection in the "Properties" tab in the "General" area, for example the name of the connection and the interfaces of the communications partner that will be used.

   For S7 connections to an unspecified partner, set the address of the partner.
   You can find the local ID (reference of the S7 connection in the user program) in the "Local ID" area.
6. In the Project tree, select the "Program blocks" folder for one of the CPUs and open OB1 in the folder by double-clicking on it. The program editor opens.
7. In the program editor, call the relevant instructions for S7 communication in the user program of the communication partner (configured at one end) or in the user programs of the communication partners (configured at both ends). Select the BSEND and BRCV instructions from the "Communication" area of the "Instructions" task card, for example, and drag them to a network of OB1.
8. At the ID parameter of the instruction, assign the local ID of the configured connection to be used for the transmission of data.
9. Assign the parameters for the instructions indicating which data will be written to where and which data will be read from where.
10. Download the hardware configuration and user program to the CPU(s).

S7 communication via CP 1543-1

If you set up S7 communication via the Industrial Ethernet interface of the CP 1543-1, you can select the transport protocol for data transfer in the properties of the S7 connection under "General":

- "TCP/IP" check box selected (default): ISO-on-TCP (RFC 1006): for S7 communication between S7-1500 CPUs
- "TCP/IP" check box cleared: ISO protocol (ISO/IEC 8073): Addressing using MAC addresses

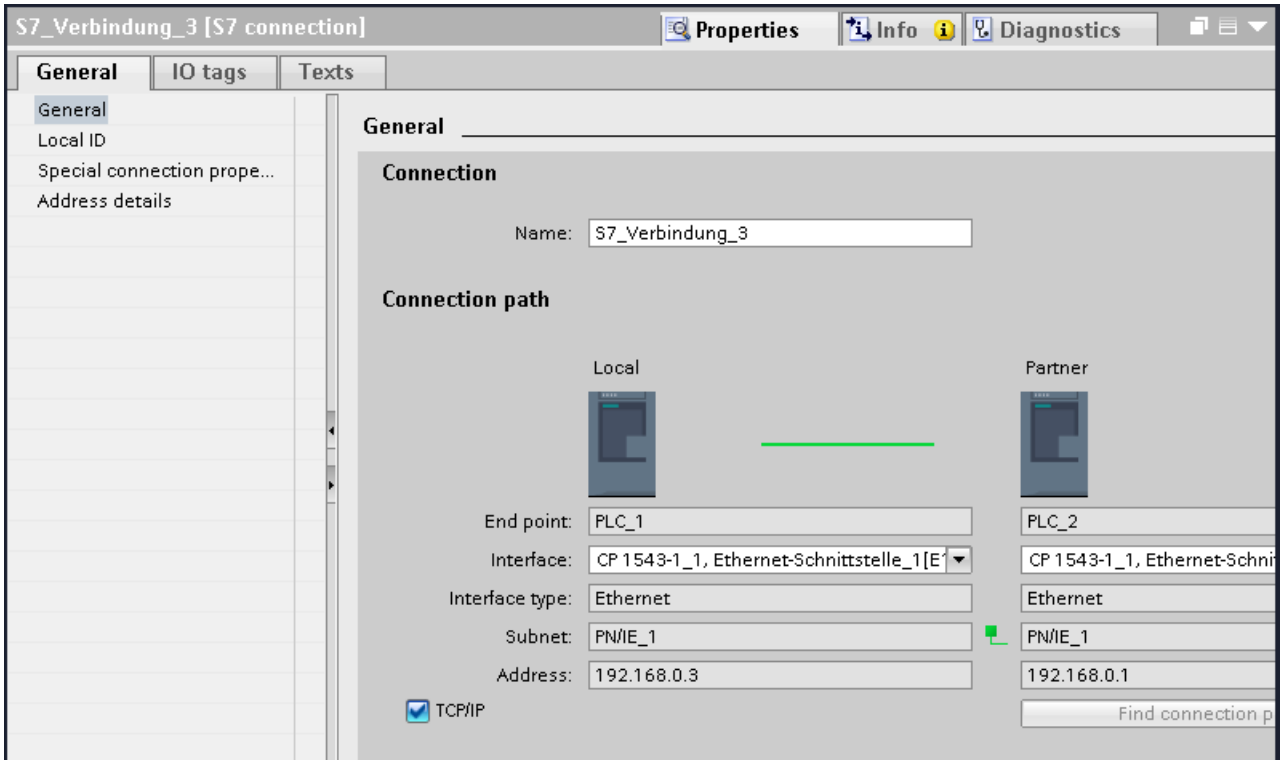


Figure 3-151 Selecting the CP 1543-1 transport protocol

Procedure for setting up an S7 connection via different S7 subnets

You have the option of using an S7 connection over multiple S7 subnets (PROFIBUS, PROFINET/Industrial Ethernet) (S7 routing (Page 397)).

1. Configure the communications partners in the network view of the Devices & networks editor of STEP 7.
2. Select the "Network" button.
3. Connect the relevant interfaces with the S7 subnets (PROFIBUS, PROFINET/Industrial Ethernet) using drag-and-drop.
4. Select the "Connections" button and the "S7 connection" entry from the drop-down list.

5. Using drag-and-drop in our example, connect PLC_1 in the left S7 subnet (PROFIBUS) to PLC_3 in the right S7 subnet (PROFINET).
   The S7 connection between CPU 1 and CPU 3 is configured.

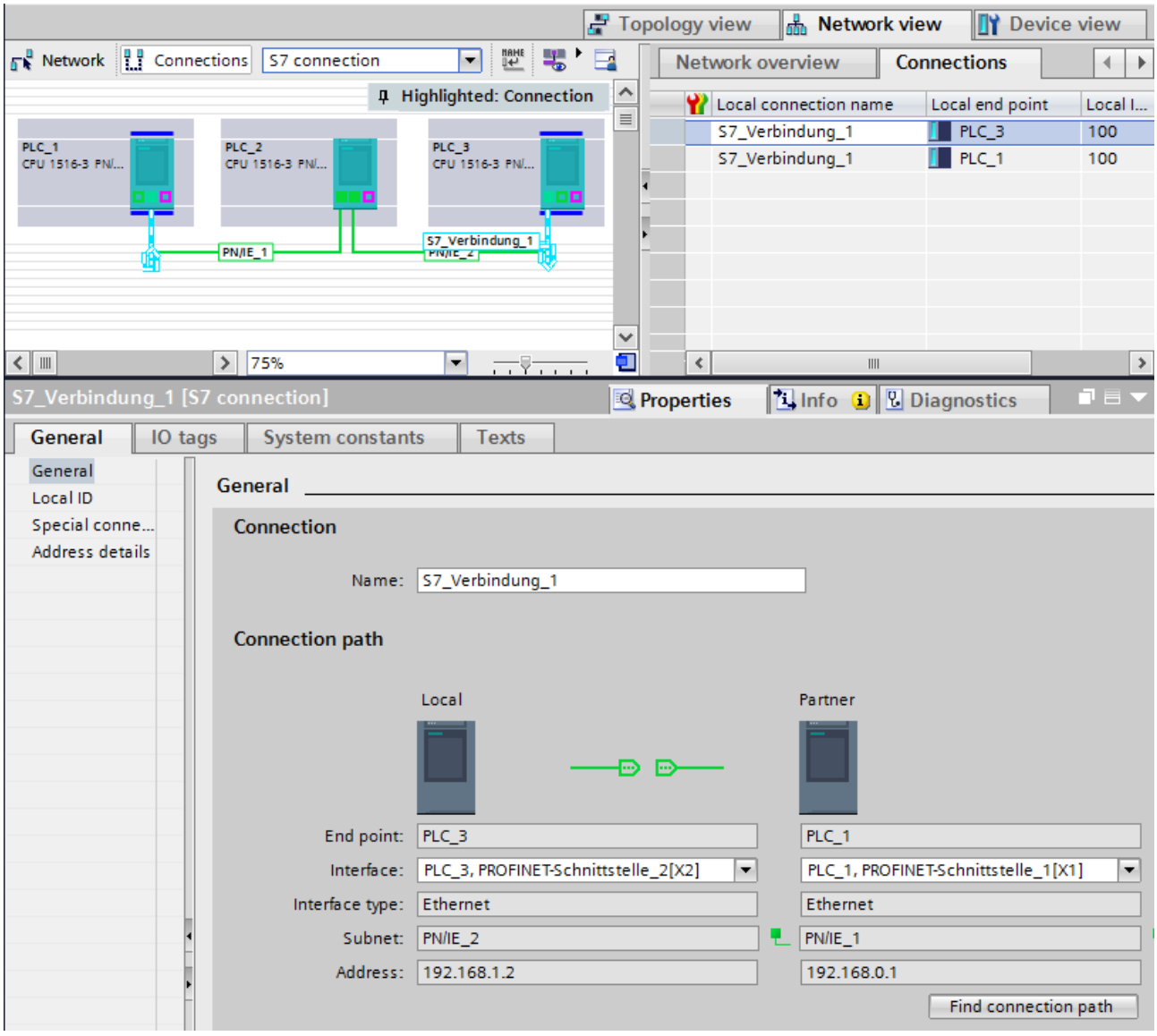


Figure 3-152 S7 connections via different subnets

ET 200SP Open Controller as router for S7 connections

If you assign the "PROFINET onboard [X2]" interface to the CPU 1515SP PC (F) of the SIMATIC PC station, the CPU 1515SP PC (F) can be used as a router for S7 connections. If you use the CP interface for "None, or a different Windows setting", you cannot use the Open Controller as a router for routed S7 connections.

An existing S7 connection routed by the CPU 1515SP PC (F) becomes invalid if the assignment of the interface of the CPU 1515SP PC (F) is changed from "SIMATIC PC station" to "None, or a different Windows setting". Since the PLC now no longer handles routing

functions for this connection, when the CPU 1515SP PC (F) is compiled, no message relating to the invalid connection is displayed. The invalid routed S7 connection is displayed only when the end points of the connection are compiled.

The interfaces required for routed S7 connections must remain explicitly assigned on the CPU 1515SP PC (F) . You can edit the assignment of the interface of the CPU 1515SP PC (F) in the properties under "PROFINET onboard [X2] > Interface assignment".

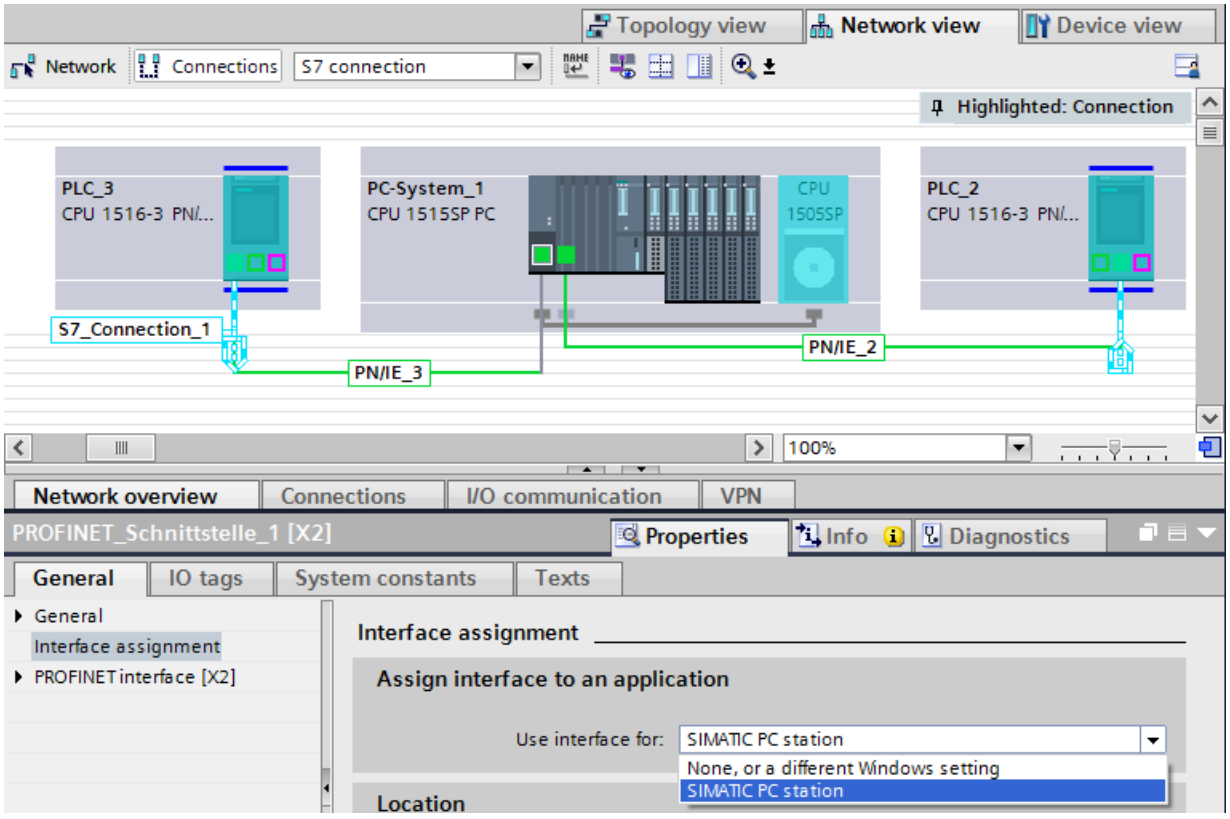


Figure 3-153 S7 routing PC station

More information

You can find detailed information on configuring S7 connections and how to use the instructions for S7 communication in the user program in the STEP 7 online help.

Point-to-point link

10

Functionality

A point-to-point connection for S7-1500, ET 200MP and ET 200SP is established via communications modules (CMs) with serial interfaces (RS232, RS422 or RS485):

- S7-1500/ET 200MP:
  - CM PtP RS232 BA
  - CM PtP RS422/485 BA
  - CM PtP RS232 HF
  - CM PtP RS422/485 HF
- ET 200SP:
  - CM PtP

The bidirectional data exchange via a point-to-point connection works between communications modules or third-party systems or devices capable of communication. At least 2 communication partners are required for communication ("point-to-point"). With RS422 and RS485, more than two communications partners are possible.

Protocols for communication via a point-to-point connection

- Freeport protocol (also called ASCII protocol)
- Procedure 3964(R)
- Modbus protocol in RTU format (RTU: Remote Terminal Unit)
- USS protocol (universal serial interface protocol)

The protocols use different layers according to the ISO/OSI reference model:

- Freeport: Uses layer 1 (physical layer)
- 3964 (R), USS and Modbus: Use layer 1 and 2 (physical layer and data link layer; therefore greater transmission reliability than with Freeport). USS and Modbus use additionally layer 4.

Properties of the Freeport protocol

- The recipient recognizes the end of the data transfer by means of a selectable end criterion (e.g. character delay time elapsed, receipt of end character, receipt of a fixed amount of data).
- The sender cannot recognize whether the sent data arrived free of errors at the recipient.

Properties of procedure 3964 (R)

- When the data is sent, control characters are added (start, end and block check characters). Make sure that these control characters are not included as data in the frame.
- Connection establishment and termination makes use of control characters.
- If transfer errors occur, data transfer is automatically repeated.

Data exchange using Freeport or 3964 (R) communication

The data to be sent is stored in the user program of the corresponding CPU in data blocks (send buffer). A receive buffer is available on the communications module for the received data. Check the properties of the receive buffer and adapt them if necessary. You must create a data block for receiving in the CPU.

In the user program of the CPU, the "Send_P2P" and "Receive_P2P" instructions handle the data transfer between the CPU and CM.

Procedure for setting up Freeport or 3964 (R) communication

1. Configure an S7-1500 configuration with CPU and CM in the device view of the hardware and network editor of STEP 7.
2. Select the interface of the CM in the device view of STEP 7.
3. Assign the parameters of the interface (for example connection communication, configuration of message sending) in the Inspector window of STEP 7 under "Properties" > "General".
4. Select the "Send_P2P" or "Receive_P2P" instruction in the "Instructions" task card under "Communication" > "Communications processor" and drag-and-drop the instruction into the user program (for example into a FB).
5. Assign the parameters for the instructions according to your configuration.
6. Download the hardware configuration and user program to the CPU.

Otherwise: Dynamic parameter assignment of the communications module

In certain types of application it is an advantage to set up communication dynamically; in other words, program-controlled by a specific application.

Typical applications for this, could be, for example manufacturers of serial machines. To make the user interfaces as convenient as possible for their customers, these manufacturers adapt the communications services to the particular operator entries.

Instructions for Freeport communication

There are 3 instructions available for the dynamic configuration in the user program for Freeport communication. The following applies to all 3 instructions: the previously valid configuration data is overwritten but not stored permanently in the target system.

- The "Port_Config" instruction is used for the program-controlled configuration of the relevant port of the communications module.
- The "Send_Config" instruction is used for the dynamic configuration, for example of time intervals and breaks in transmission (serial transmission parameters) for the relevant port.
- The "Receive_Config" instruction is used for dynamic configuration, for example of conditions for the start and end of a message to be transferred (serial receive parameters) for the relevant port.

Instructions for 3964 (R) communication

There are 2 instructions available for dynamic configuration in the user program for 3964 (R) communication. The following applies to the instructions: the previously valid configuration data is overwritten but not stored permanently in the target system.

- The "Port_Config" instruction is used for the program-controlled configuration of the relevant port of the communications module.
- The "P3964_Config" instruction is used for the dynamic configuration of protocol parameters.

Properties of the USS protocol

- Simple, serial data transfer protocol with cyclic message frame traffic in half duplex mode that is tailored to the requirements of drive technology.
- Data transfer works according to the master-slave principle.
  - The master has access to the functions of the drive and can, among other things, control the drive, read status values and read and write the drive parameters.

Data exchange using USS communication

The communications module is the master. The master continuously sends frames (job frames) to the up to 16 drives and expects a response frame from each addressed drive.

A drive sends a response frame under the following conditions:

- When a frame is received without errors
- When the drive is addressed in this frame

A drive must not send if these conditions are not met or the drive was addressed in the broadcast.

The connection to the relevant drives exists for the master once it receives a response frame from the drive after a specified processing time (response delay time).

Procedure for setting up USS communication

1. Configure an S7-1500 configuration with CPU and CM in the device view of the hardware and network editor of STEP 7.
2. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.
3. Select the instructions for USS communication according to your task in the "Communication" area, "Communications processor" folder of the "Instructions" task card and drag them to a network of OB1:
   - The "USS_Port_Scan" instruction allows you to communicate via the USS network.
   - The "USS_Drive_Control" instruction prepares send data for the drive and evaluates the response data of the drive.
   - The "USS_Read_Param" instruction is used to read out parameters from the drive.
   - The "USS_Write_Param" instruction is used to change parameters on the drive.
4. Assign the parameters for the instructions according to your configuration.
5. Download the hardware configuration and user program to the CPU.

Properties of the Modbus protocol (RTU)

- Communication takes the form of serial, asynchronous transfer with a transmission speed of up to 115.2 kbps, half duplex.
- Data transfer works according to the master-slave principle.
- The Modbus master can send jobs for reading and writing operands to the Modbus slave:
  - Reading inputs, timers, counters, outputs, memory bits, data blocks
  - Writing outputs, memory bits, data blocks
- Broadcast to all slaves is possible.

Data exchange using Modbus communication (RTU)

The communications module can be a Modbus master or Modbus slave. A Modbus master can communicate with one or more Modbus slaves (the number depends on the physical interface). Only the Modbus slave explicitly addressed by the Modbus master is permitted to return data to the Modbus master. The slave detects the end of the data transfer and acknowledges it. If an error occurs, it provides an error code to the master.

Procedure for setting up Modbus communication (RTU)

1. Configure an S7-1500 configuration with CPU and CM in the device view of the hardware and network editor of STEP 7.
2. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.

3. Select the instructions for Modbus communication according to your task in the "Communication" area, "Communications processor" folder of the "Instructions" task card and drag them to a network of OB1:
   - The "Modbus_Comm_Load" instruction configures the port of the CM for Modbus communication.
   - The "Modbus_Master" instruction is used for Modbus master functionality.
   - The "Modbus_Slave" instruction is used for Modbus slave functionality.
4. Assign the parameters for the instructions according to your configuration.
5. Download the hardware configuration and user program to the CPU.

Additional information

- You can find more detailed information on communication via point-to-point connections and basics of serial data transmission in the function manual CM PtP communication module - Configurations for point-to-point connections (https://support.industry.siemens.com/cs/us/en/view/59057093).
- You can find a description of how to use the instructions for point-to-point connections in the user program in the STEP 7 online help.
- You can find information about the communications modules with a serial interface in the manual of the particular communications module.

OPC UA communication 11

11.1 What you need to know about OPC UA

11.1.1 OPC UA and Industry 4.0

Uniform standard for information and data exchange

Industry 4.0 stands for the intensive utilization, evaluation and analysis of the large volumes of data from production in IT systems at the enterprise level. With Industry 4.0, data exchange between the production and enterprise levels is rapidly increasing. However, a prerequisite for success is a uniform standard for the information and data exchange.

Classic OPC only runs on Windows operating systems. To get around this restriction, the OPC Foundation developed the OPC UA (OPC Unified Architecture) standard.

The OPC UA standard is particularly suitable for data exchange across different levels thanks to its independence from specific operating systems, its secure transfer procedures and the semantic description of data. Machine data (controlled variables, measured values or parameters) can also be transferred in this way.

An important component of this concept is that OPC UA communication can take place in parallel with real-time communication for time-critical, machine-level data transfer.

OPC UA is highly scalable so that a consistent information exchange between sensors, controllers and MES or ERP systems is possible.

OPC UA makes available not only data but also information about the data (data types), at the same time making possible machine-interpretable access to the data.

OPC UA topic page

For an overview of the most important articles and links on the subject of OPC UA, refer to the SIEMENS Industry Online Support.

OPC UA topic page (https://support.industry.siemens.com/cs/ww/en/view/109770435)

11.1.2 General features of OPC UA

OPC UA and PROFINET

OPC UA and PROFINET can be used together. The two protocols use the same network infrastructure.

Independence from the operating system

The OPC UA standard is platform-independent and uses an optimized TCP-based binary protocol for high-performance applications.

OPC UA can be used, for example, under Windows, Linux, Mac OS X, a real-time operating system or a mobile operating system (Android or iOS).

Independence of a specific transport layer

OPC UA currently supports the following transport mechanisms and protocols:

- The transfer of messages as a binary stream directly via TCP/IP
- The transfer of messages with XML via TCP/IP and HTTP. This transport mechanism allows only a slow transfer and is therefore almost never used. S7-1500 CPUs do not support this transport mechanism.

Binary data exchange is supported by all OPC UA applications (required in OPC UA specification).

Simple client-server principle

An OPC UA server provides a great deal of information within a network, e.g. relating to the CPU, the OPC UA server itself, the data and the data types. An OPC UA client accesses this information.

Implementation in different programming languages

The OPC Foundation has implemented the OPC UA standard in several programming languages: Stacks for .NET, ANSI C and Java are available, although maintenance has been discontinued for the stacks for ANSI C and Java.

The OPC Foundation offers the .NET stack as well as example programs as open source software. See Github (https://github.com/opcfoundation).

A number of companies offer Software Development Kits (SDK). These development packages contain the stacks of the OPC Foundation and other functions that facilitate the development of solutions.

Advantages of using SDKs:

- Support from the supplier
- Tested software
- Detailed documentation
- Clear license conditions (important for selling of solutions)

Scalability

OPC UA can be used for devices of different performance classes:

- Sensors
- Embedded systems
- Controllers
- PC systems
- Smartphones
- Servers running MES or ERP applications.

The performance class of the devices is differentiated by profiles. Different OPC UA profiles offer the possibility to scale OPC UA for very small and simple devices as well as for very high-performance devices.

An OPC UA profile describes functions and services that must be supported by the server and client. In addition, other functionalities/services that are not required by the profile can be optionally provided.

OPC UA profiles differ from PROFINET profiles; the latter define additional cross-vendor properties and behavior for installations and systems in the sense of a vendor-neutral software interface.

Nano Embedded Device 2017 Server Profile
For the smallest devices with severely limited functionality, there is the "Nano Embedded Device.2017 Server Profile" of the OPC Foundation. This profile is functionally equivalent to the core server facet and defines the OPC UA TCP binary protocol as the required transport profile. The profile allows for connections without UA Security and does not allow subscriptions or method calls. Support for diagnostic objects and variables is optional for this profile.

Additional profiles build on the "Nano Embedded Device 2017 Server Profile", requiring more resources and offering more functionality.

Micro Embedded Device 2017 Server Profile
This profile provides limited functionality; it requires at least two parallel connections. Additionally, it allows subscriptions/data monitoring, but no UA Security and no method calls.

- The S7-1200 Basic Controllers support the "Micro Embedded Device 2017 Server Profile", the S7-1200 also supports UA Security.

Embedded 2017 UA Server Profile
This profile has been developed for devices with more than 50 MB RAM and a more high-performance processor. It is based on the Micro Embedded Device Server profile. In addition, it requires UA security and method calls.

In addition, the servers must make their used type model (data types, reference types, variable types, etc.) available.

- S7-1500 Advanced Controllers support the "Embedded 2017 UA Server Profile".

Standard and global discovery profiles
The "OPC UA Specification Part 7" defines additional profiles:

- The "Standard 2017 UA Server Profile", which is suitable for PC-based OPC UA servers
- 2 global profiles, "Global Discovery Server 2017 Profile" and "Global Discovery and Certificate Management 2017 Server Profile", that cover the required service and information models of a Global Discovery Server

Type-instance concept

OPC UA offers a fully networked (full-meshed network), object-oriented information model for namespaces, including metadata for the object description. Any object structures can be generated via referencing of the instances among each other and their types. Because servers disclose their instance and type systems, clients can navigate through this network and obtain all the information they need. Both instances and their type definitions are available in runtime.

Procedures or concepts on how to handle references to types are optimized over time. These optimizations lead to new versions of the OPC UA Specification (e.g. V1.03 => V1.04).

PLC tag mapping

The information of the OPC UA server (for example the PLC tags) is modeled as nodes connected to one another via references. The semantics are displayed by the server in the address space and can be acquired by clients (while navigating). This makes it possible to browse from node to node with an OPC UA client and find out what content can be read, monitored or written.

Integrated security mechanisms

OPC UA uses security mechanisms at various levels:

- A secure connection can only be established between an OPC UA server and an OPC UA client if the client and server can register with X.509v3 certificates and accept each other's certificates (security at the application level). Various security policies are possible, including an unsecured connection between server and client (Security Policy: "No security").
- A server can always request the following information from the user for authorized access (authentication):
  - A user certificate (not configurable in STEP 7)
  - User name and password
  - No user authorization

The security mechanisms are optional and configurable.

More information

You can find more information on the website of the OPC Foundation (https://opcfoundation.org).

11.1.3 OPC UA for S7-1200/S7-1500 CPUs

In OPC UA, one system operates as a server and provides data the existing information to other systems (clients).

OPC UA clients, for example, have read and write access to data on an OPC UA server. OPC UA clients call methods on the OPC UA server.

You can access this data online with a client, including e.g. information on performance and diagnostics. In OPC UA terminology, this function is called "Browse". The "Subscription" function eliminates regular reading of a tag; with this function, the server informs a client about value changes.

If a system supports the OPC UA client and the OPC UA server, the system can be both a client and a server at the same time.

OPC UA server of the S7-1500 CPU

As of firmware version 2.0, an S7-1500 CPU is equipped with an OPC UA server.

The following sections describe how you configure the OPC UA server of the S7-1500 CPU to make data and methods available for OPC UA clients so that clients have read or write access to PLC tags on the CPU and can call server methods.

The following sections also set out how to integrate companion specifications into the address space of the OPC UA server.

OPC UA server of the S7-1200 CPU

As of firmware V4.4, an S7-1200 CPU is equipped with an OPC UA server.

The OPC UA server is generally configured as it is for an S7-1500 CPU; the scope of functions and the quantity limits are limited according to the supported "Micro Embedded Device 2017 Server Profile". Unlike for an S7-1500 CPU, the functions "Registered Read" and "Registered Write" are **not** available.

As of firmware V4.5, S7-1200 CPUs support server methods as well as structured data types (structures and arrays).

You can find additional information in the STEP 7 online help.

OPC UA client of the S7-1500 CPU

As of firmware version V2.6, an S7-1500 CPU is additionally equipped with an OPC UA client.

The following sections show how to use standardized instructions (PLCopen function blocks) to create a user program that, as an OPC UA client, provides the following functions:

- Reading data from an OPC UA server
- Writing data to an OPC UA server
- Calling methods of an OPC UA server

STEP 7 (TIA Portal) assists you in creating user programs by providing an editor for client interfaces and a parameter assignment for OPC UA connections.

The OPC UA instructions for an S7-1500 CPU as client are described in detail in the help to the instructions (Instructions > Communication > OPC UA).

OPC UA client for test purposes

The following description uses various different OPC UA clients to illustrate the use of OPC UA clients:

- "UaExpert" of Unified Automation. An extensive client that can be used free of charge:
  Link for downloading UaExpert (https://www.unified-automation.com/downloads/opc-ua-clients.html)
- "UA Sample Client" of the OPC Foundation. This client is available free of charge for users who are registered with the OPC Foundation :
  Link for downloading the example client of the OPC Foundation
  (https://opcfoundation.org)

Application example in Industry online support

Siemens Industry Online Support provides a free application example with a client API for various applications. You use the functions of this interface to create your own OPC UA clients that match your application. To simplify handling the API, we offer a higher-level .NET helper class.

The client API is based on the .NET OPC UA stack of the OPC Foundation.

The application example shows how to establish connections between servers and clients, for example. It also demonstrates the reading and writing of PLC tags.

Link to download: OPC UA .NET client for the SIMATIC S7-1500 OPC UA Server
(https://support.industry.siemens.com/cs/us/en/view/109737901)

11.1.4 Access to OPC UA applications

The access possibilities that an S7-1500 CPU with an OPC UA application (client or server) has via a CP in the same station are described below. In addition, an approach for combining these access possibilities with the "IP Forwarding" function to allow access to devices of another IP subnet via an S7-1500 station is presented.

All the settings for this can be found in the CPU properties, "Advanced configuration" area in the Inspector window.

The possibility of accessing the OPC UA application in the CPU via CP interface is subject to the following requirements:

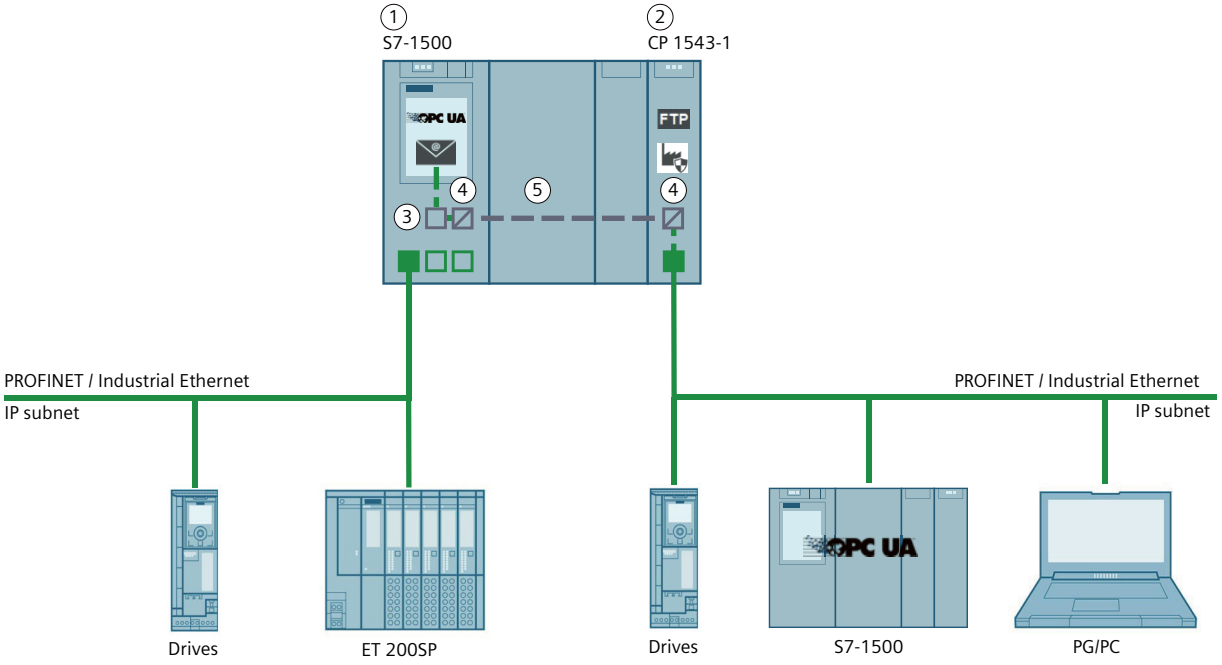
- S7-1500 CPU (Advanced Controller) firmware version V2.8 or higher, S7-1500R/H CPUs firmware version V3.1 or higher
- CP 1543-1 firmware version V2.2 or higher

Recommendation: Use a CP 1543-1 with firmware V3.0 or higher. As of this version, the security functions (firewall) are also available for the virtual interface (W1) and no additional firewall needs to be installed between the station and an insecure network.

Principle: Interface for access via communications module

For a CPU application, such as OPC UA, to be accessed via CP interface, you must configure a virtual interface (W1). IP-based applications can then be accessed via the IP address parameters of this virtual interface.

The schematic is shown in the following figure.



① CPU S7-1500 FW V2.8 or higher (e.g. CPU 1515-2 PN)
② CP 1543-1 (FW V2.2 or higher)
③ Virtual interface (W1)
④ Protocol conversion PROFINET / Industrial Ethernet on backplane bus or backplane bus on PROFINET / Industrial Ethernet
⑤ Backplane bus

Figure 3-154 Principle: Interface for access via communications module

Example: Access of OPC UA clients to the OPC UA server of the CPU

For access of an OPC UA client to the OPC UA server of the CPU, the following interfaces of the S7-1500 station are available:

- The local PROFINET interfaces of the S7-1500 CPU
- The Ethernet interface of a CP 1543-1 (firmware version V2.2 and higher)

The following figure shows an example of a possible configuration: The CPU could also have the role OPC UA client and the device on the subnet of the CP could have the role OPC UA server.

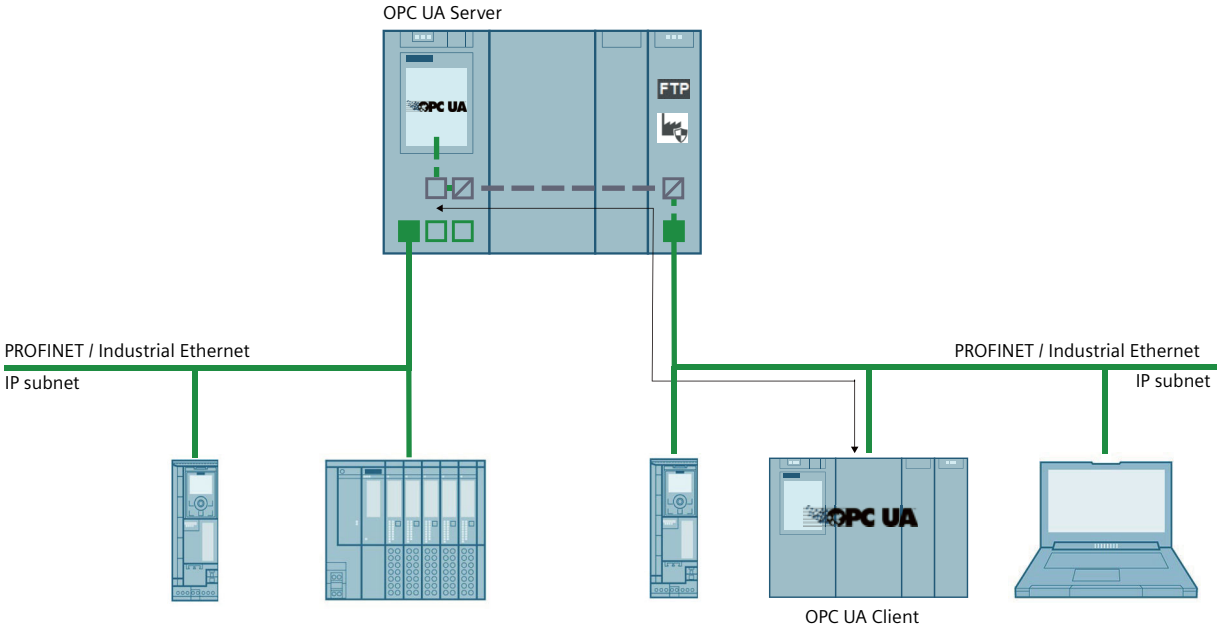


Figure 3-155 Example: Access of OPC UA clients to the OPC UA server of the CPU

Example: Access of OPC UA clients to OPC UA servers via S7-1500 CPU with activated IP Forwarding

OPC UA client and OPC UA server can also be connected to one another via an S7-1500 CPU, in which case the S7-1500 CPU operates as an IP Forwarder. This configuration option allows for flexible expansion of existing systems.

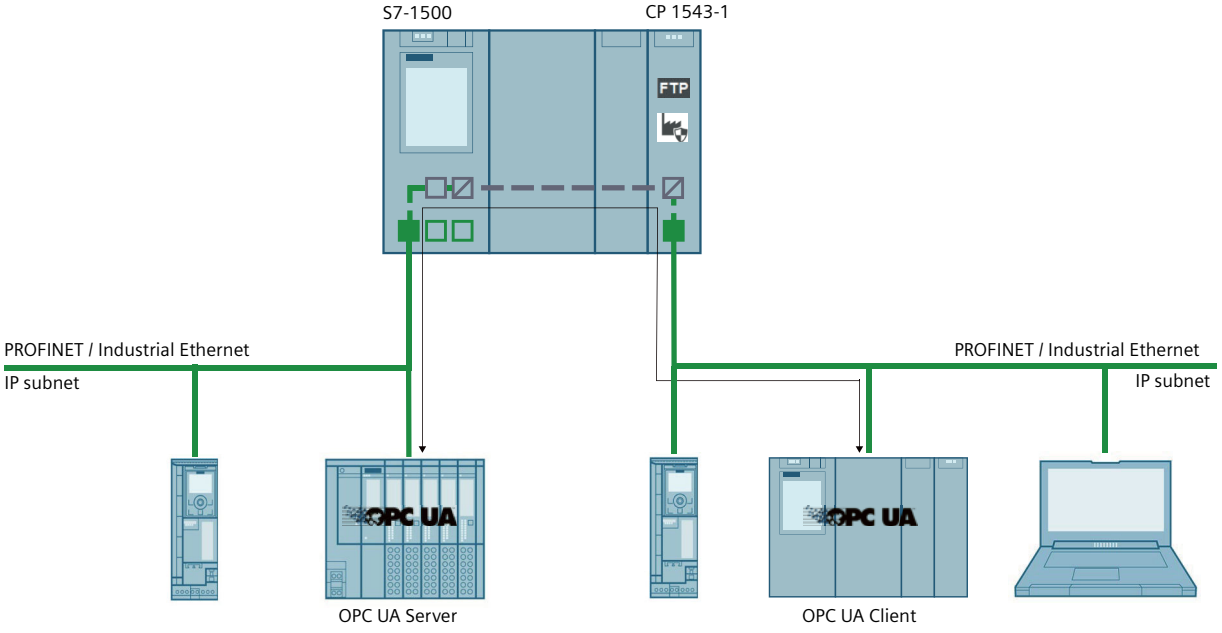


Figure 3-156 Example: Access of OPC UA clients to OPC UA servers via S7-1500 CPU with activated IP Forwarding

More information

More information on access options via the virtual interface and via IP forwarding can be found in the following sections:

- IP forwarding (Page 402)
- Virtual interface for IP-based applications (Page 417)

11.1.5 Addressing nodes

Nodes are the basic elements of OPC UA, they are comparable with objects from object-oriented programming. Nodes are used, for example, for user data (tags) or other metadata. Nodes are used to model an OPC UA address space that also contains a type model with type definitions.

Node ID (NodeId)

Nodes in the OPC UA address space are uniquely identified by a NodeId (Node Identifier).

The NodeId consists of an identifier, identifier type and a namespace index. Namespaces are used to avoid naming conflicts.

The OPC Foundation has defined a wide range of nodes that provide information about the given OPC UA server. These nodes can be found in the namespace of the OPC Foundation and have the index 0.

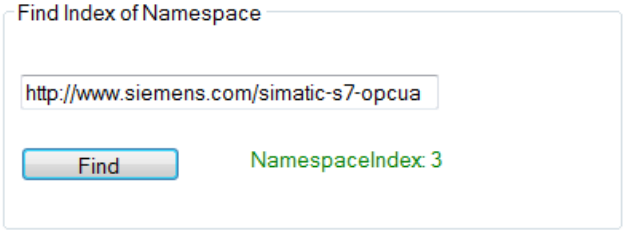
The OPC Foundation also defines data types and tag types.

Namespace (Namespace)

In addition to the above-described namespace of the OPC Foundation, the namespace for accessing CPU data is of interest: All the tags or methods of an S7-1500 OPC UA server are contained in the namespace (Namespace) of the standard server interface "http://www.siemens.com/simatic-s7-opcua".

By default this namespace has the Index 3. The index may change later if additional namespaces are inserted into the server or if existing ones are deleted. It is therefore necessary for an OPC UA client to request the current index of the namespace (e.g. "http://www.siemens.com/simatic-s7-opcua") from the server before reading or writing its values.

The following figure shows an example of the result of such a request.



Identifier

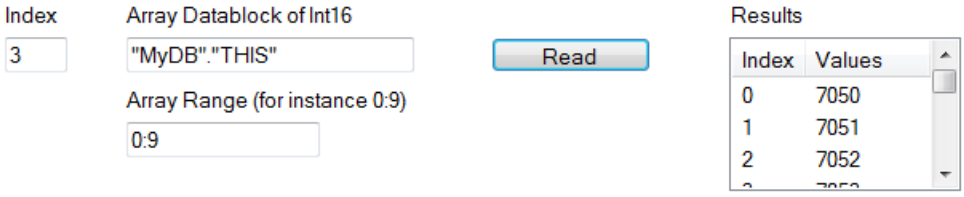
The Identifier corresponds to the name of the PLC tag in quotation marks. The quotation mark is the only sign that is not permitted as part of a name in STEP 7. Quotation marks avoid naming conflicts.

The following example reads the value of the "StartTimer" tag:



The Identifier can consist of several components. The individual components are then separated by a dot.

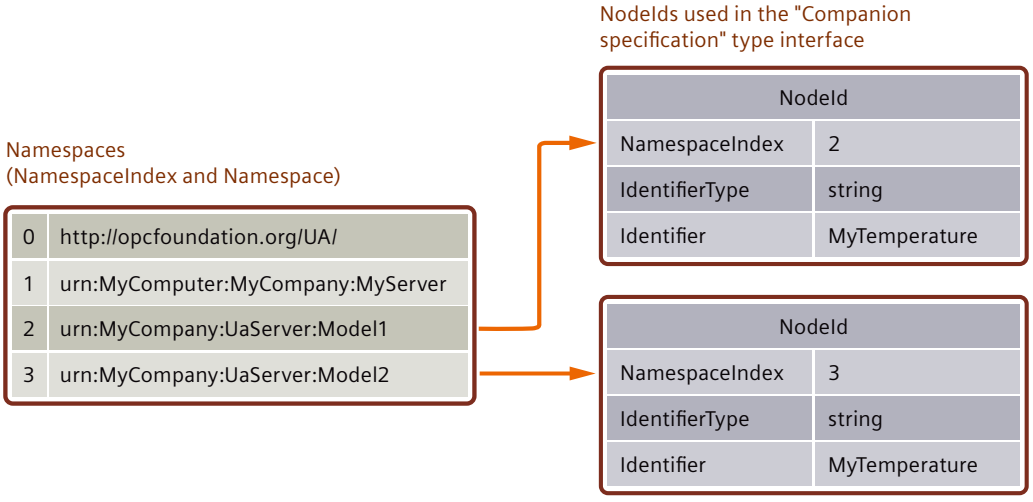
The following example reads the "MyDB" array data block completely. This data block contains an array with ten integer values. All ten values should be read in one pass. Therefore, "0:9" is entered at the array range.



Example of NodeIds, identifiers and namespaces

The following figure illustrates the relation between NodeIds, identifiers and namespaces: It is no problem if two nodes have the same identifiers but belong to different namespaces.

STEP 7 (TIA Portal) allows you to easily import namespaces via a server interface.



PLC tags in the address space of the OPC UA server

The figure below shows where the PLC tags in the example are located in the address space of the OPC UA server (excerpt from UA client):

The "MyDB" data block is a global data block. The data block is therefore located below the node "DataBlocksGlobal". "StartTimer" is a memory tag and is therefore stored below the "Memory" node.

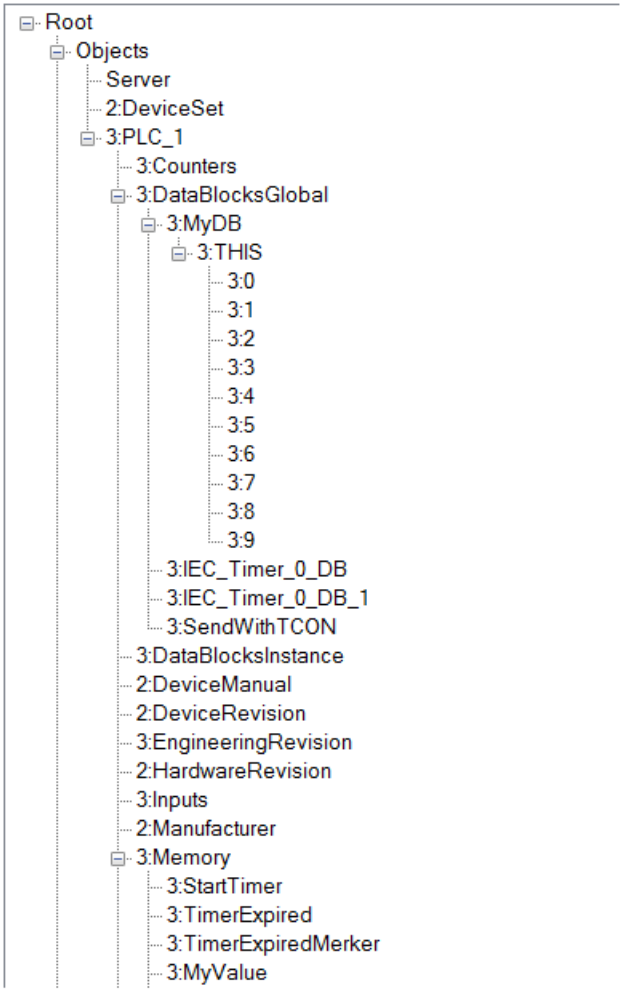


Figure 3-157 PLC tags in the address space of the OPC UA server

Methods in the address space of the OPC UA server

If you implement a method via your user program, it takes the following form in the address space of the OPC UA Server

(see Providing methods on the OPC UA server (Page 306)):

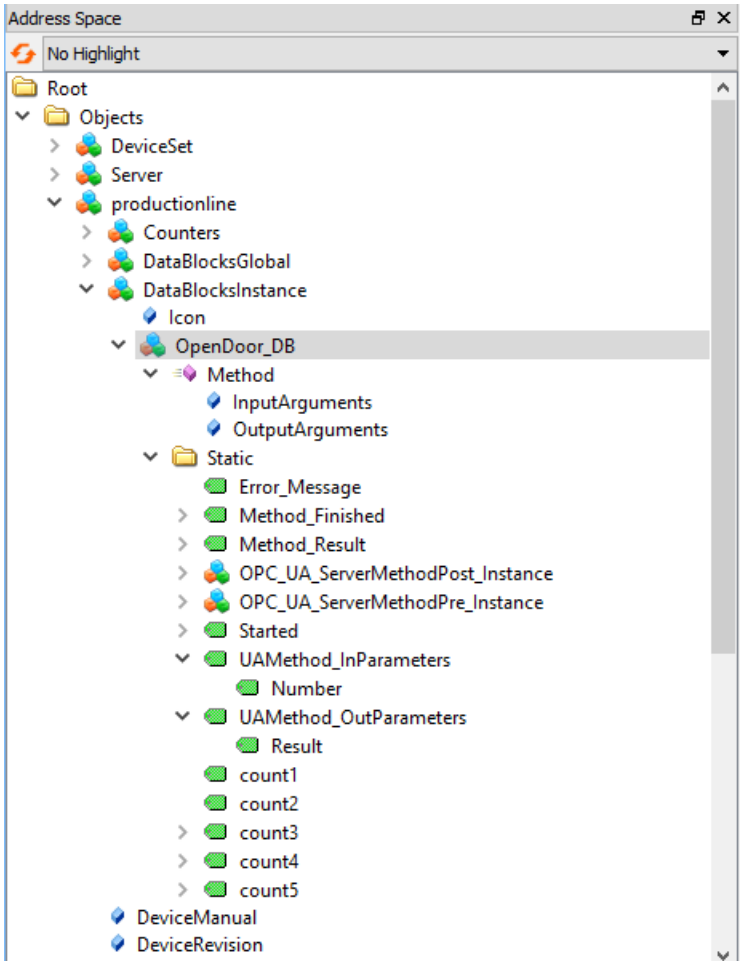


Figure 3-158 Methods in the address space of the OPC UA server

11.1.6 Namespace overview for the OPC UA server of the S7-1200/1500 CPUs

As already written for the topic "Addressing of nodes", the namespace index is part of the node ID. To ensure that a node ID is always unique in the address space, namespaces are used in OPC UA; the BrowseName as the sole means of identifying a node can be ambiguous.

Namespaces are specified at OPC UA through different "Naming Authorities" which develop the OPC UA information models, for example by a working group, the OPC Foundation or organizations that develop standard information models.

Namespaces are identified through a namespace URI; the namespace URI identifies the Naming Authority.

A namespace index is used to optimize accesses to the nodes of the server instead of the namespace URI. The namespace index is a pointer to a namespace array that the server manages. A client reads the namespace index once from the server to be able to access the nodes of the server afterwards with a simple integer instead of a URI string.

The following table contains the assignment between namespace URIs and namespace indexes of S7-1500 and S7-1200 CPUs.

Assignment between namespace URI and namespace index

The namespace indexes are fixed at S7-1200 and S7-1500 CPUs for the namespace indexes 0 to 3. Further namespace indexes are currently not specified.

Namespace URI	Namespace index	Description
http://opcfoundation.org/UA/	0	Namespace for the node IDs and BrowseNames of the OPC UA specification (OPC 10000-3). **Example** 0:EngineeringUnits
Local Server URI ("urn:SIMATIC:" + application name as configured in TIA Portal (area "OPC UA > General" in the CPU properties))	1	Namespace for nodes that are defined in the local server (OPC 10000-5). **Example** urn:SIMATIC:PLC_1
http://opcfoundation.org/UA/DI/	2	Namespace for node IDs and BrowseNames of the OPC UA specification for devices (OPC 10000-100). **Example** 2:DeviceRevision
http://www.siemens.com/simatic-s7-opcua	3	Namespace for node IDs and BrowseNames that are defined product-specifically for an S7-1200/S7-1500 CPU. In this namespace instances (CPU, tags, DBs, etc.) as well as their types (UDTs, LDTs, FBs, etc.) are defined. **Example** 3:DataBlocksGlobal
URIs of additional namespaces for further instances and types **Examples** http://machinesupplier.org/implementedPackML http://opcfoundation.org/UA/PackML	> 3	Not specified. Can, for example, be defined with SiOME. **Examples** 4:MyPackMLMachineInstance 5:PackMLBaseObjectType

11.1.7 What you need to know about OPC UA clients

Basics of OPC UA clients

OPC UA clients are programs that do the following:

- Access the information from an OPC UA server (for example an S7-1500 CPU): read/browse access, write access, subscriptions
- Execute methods through the OPC UA server

However, OPC UA clients can only access data that is enabled for this purpose (see "Managing write and read rights (Page 235)").

You need the endpoint of the server to establish a connection to an OPC UA server (see "Endpoints of the OPC UA servers (Page 224)").

Reading out information from the OPC UA server

When a connection to an end point of the server exists, you can use the navigation function of the client: You navigate starting from a defined starting point (from the "root" node) through the address space of the server.

The following information is provided in the process:

- Enabled PLC tags, data blocks and data block components
- Namespace index and identifiers of these PLC tags, data blocks and DB components
- Data types of the PLC tags and DB components
- Number of components in arrays (required for reading and writing arrays)

In addition, you receive information about the OPC UA server itself as well as information about the S7-1500 based on the "OPC UA for Devices" standard of the OPC Foundation (for example, serial number, firmware version).

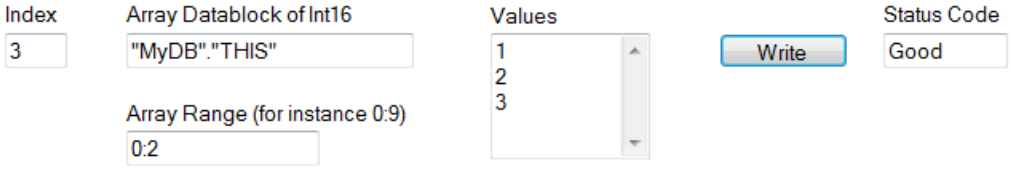
Reading data from the server and writing to the server

You now know the namespace, identifier and data type of PLC tags. This means that you can now specifically read individual PLC tags and DB components as well as complete arrays and structures.

You can find examples of the reading of Boolean tags and array data blocks in Addressing nodes (Page 174).

Rules for access to structures are available here (Page 363).

With the information that you obtain while navigating through the address space of the server (index, identifier and data type), you can also transfer values to the S7-1500 with the OPC UA client. The following example overwrites the first three values in the array data block "MyDB".



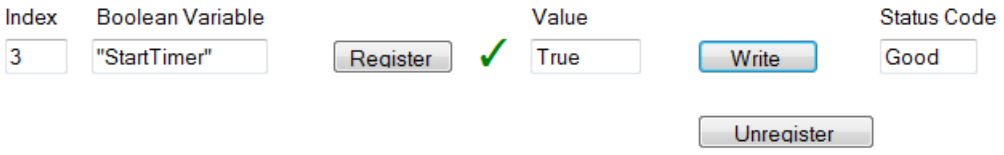
For "Array Range" you specify which components of the array you want to overwrite. The "Good" status code indicates that the values were transferred successfully. However, you can only write the values to the S7-1500 but not the time stamps of these values. The time stamps can only be read.

Faster access through registration

Registered Read/Write lends itself to repeated, optimized access to data – with maximum performance. When tag nodes are registered, the OPC UA server creates a numerical Identifier (numerical NodeId) that directly references the registered node. For read or write jobs of the client to this numerical Identifier, the server does not have to resolve any strings as Identifier and can access the requested tag in an optimized manner.

This Identifier applies solely to the current session and has to be queried again when the session connection is terminated/lost.

In the following example, the "StartTimer" tag is first registered on the server. Afterwards, the rapid function "RegisteredWrite" is used for setting the value.



In accordance with the same scheme, the "RegisteredRead" function can also be used, which is particularly useful for recurring data readouts. Take into account, however, that depending on the application it may be advisable to use a Subscription instead.

Recommendation: It is best to place registrations in the startup program of the OPC UA client, since the registration takes up time.

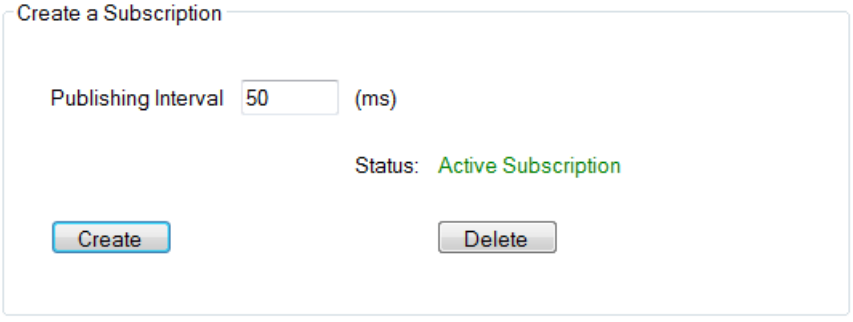
Please note that you can set the maximum number of registered nodes in the properties of the S7-1500 CPU and that the Clients have to respect this number, see General settings of the OPC UA server (Page 250).

Subscription

The term "Subscription" is used for a function in which only those tags for which an OPC UA client has registered at the OPC UA server are transferred. The OPC UA server only sends a message to the OPC UA client for these registered tags (monitored Items) when a value has changed. The monitoring of these tags makes constant sampling (Polling) by the OPC UA client superfluous; the network load is thus reduced.

You have to create a Subscription to use this function. For this purpose, you specify the "Publishing Interval" at the UA client and click the "Create" button. The publishing interval is the time interval in which the server sends new values to the client in a notification (data change notification).

In the following example a subscription has been created: The client receives a message with the new values (publishing interval 50 ms) every 50 milliseconds here.



Preventing server overload

You can set the OPC UA server of the S7-1500 CPU by means of the "Minimum publishing interval" so that it does not serve extremely short send intervals requested by the client, see Settings of the server for subscriptions (Page 252).

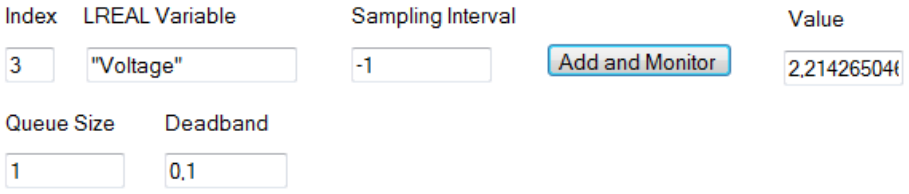
Example: A client wants to be operated at a publishing interval of 50 ms as detailed above. Such a short publishing interval would, however, result in a high network and server load. You should therefore set 1000 ms as the "Minimum publishing interval" for the server. Clients whose subscription requires shorter publishing intervals are "slowed" to 1000 ms and the server is protected from overload.

Sampling and transmission (Sampling & Publishing) within the scope of a subscription are communication processes which, like other communication processes (TCP/UDP/Web server communication...), are processed by the CPU with priority 15. OBs with higher priority interrupt the communication. If you set the sampling and transmission intervals too short, this setting causes a high communication load. Therefore, select intervals as large as possible, which are still sufficient for the application.

For information about the consistency of tags, refer to Consistency of CPU tags (Page 241).

Monitoring of PLC tags

When the Subscription has been created, you inform the server which tags are to be monitored with it. In the following example, the "Voltage" tag was added to the subscription.



The "Voltage" tag contains the value of a voltage that is detected by an S7-1500 CPU.

The sampling interval ("Sampling Interval") contains a negative value (-1). This determines that the default setting of the OPC UA server is used for the sampling interval. The default setting is defined by the transmission interval ("Publishing Interval") of the subscription. If you want to set the smallest possible sampling interval, select the value "0".

In this example, the length of the queue is set to "1": Only one value is read from the CPU at an interval of 50 milliseconds and subsequently sent to the OPC UA client when the value has changed.

The "Deadband" parameter in this example is "0.1": Changes in value have to amount to 0.1 Volt; only then does the sender send the new value to the client. The server does not send smaller changes in value. You can use this parameter, for example, to disable signal noise: Slight changes in a process variable which do not have a real meaning.

11.2 Security at OPC UA

11.2.1 Security settings

Addressing risks

OPC UA allows the exchange of data between different systems, both within the process and production levels and to systems at the control and enterprise level.

This possibility also entails security risks. That is why OPC UA provides a range of security mechanisms:

- Verification of the identity of OPC UA server and clients.
- Checking of the identity of the users.
- Signed/encrypted data exchange between OPC UA server and clients.

These security policies should only be bypassed in cases where it is absolutely necessary:

- During commissioning
- In stand-alone projects without external Ethernet connection

If you have selected the endpoint "None" for "UA Sample Client" of the OPC Foundation, for example, the program issues a clear warning:



When STEP 7 compiles your project it also checks whether you have considered the setting options for the protection and warns you of possible risks. This also includes an OPC UA security policy with the setting "no security", which corresponds to the end point "None".

NOTE

Disabling security policies you do not want

If you have enabled all security policies in the secure channel settings of the S7-1500 OPC UA server – thus, also the end point "None" (no security) – unsecured data traffic (neither signed nor encrypted) between the server and client is also possible. The OPC UA server of the S7-1500 CPU also sends its public certificate to the client at "None" (No security). And some clients check this certificate. However, the client is not forced to send a certificate to the server. The identity of the client may possibly remain unknown. Each OPC UA client can then connect to the server irrespective of any subsequent security settings.

When configuring the OPC UA server, make sure that only security policies that are compatible with the security concept of your machine or plant are selected. All other security policies should be disabled.

Recommendation: Use the setting "Basic256Sha256 - Sign and Encrypt", which means that the server only accepts Sha256 certificates. The security policies "Basic128Rsa15" and "Basic256" are deactivated by default and should not be used as an end point. Select end points with a higher security policy.

Additional security rules

- Only use the end point "None" in exceptional cases.
- Only use the "guest authentication" of the user in exceptional cases.
- Only allow access to PLC tags and DB components via OPC UA if it is genuinely necessary.
- Use the list of trusted clients in the settings of the S7-1500 OPC UA server to allow access to certain clients only.

11.2.2 Certificates pursuant to ITU X.509

Security mechanisms are integrated in several layers in OPC UA. Digital certificates have an important role here. An OPC UA client can only establish a secure connection to an OPC UA server when the server accepts the digital certificate of the client and classifies it as trusted.

See section Handling client and server certificates (Page 255).

The client must also check and trust the certificate of the server. The server and client must show their identities and prove that they are what they claim to be: They must prove their identity. Mutual authentication of client and server, for example, prevents man-in-the-middle attacks.

Man-in-the-middle attacks

A "man-in-the-middle" could have positioned itself between server and client. A man-in-the-middle is a program that intercepts communication between server and client and claims to be a client or server, and is thus able to obtain information about the S7 program or to set values in the CPU and attack a machine or plant.

OPC UA uses digital certificates that meet standard X.509 of the International Telecommunication Union (ITU).

This allows the identity of a program, a computer or an organization to be proven (authenticated).

X.509 certificates

An X.509 certificate includes the following information:

- Version number of the certificate
- Serial number of the certificate
- Information on the algorithm used by the certificate authority to sign the certificate.
- Name of the certificate authority
- Start and end of the validity period of the certificate
- Name of the program, person or organization for which/whom the certificate has been signed by the certificate authority.
- The public key of the program, person or organization.

An X509 certificate thus links an identity (name of a program, person or an organization) to the public key of the program, person or organization.

Check during connection establishment
When a connection is being established between the client and server, the devices check all information from the certificate that is required to determine its integrity, such as signature,

period of validity, application name (URN) and, in case of firmware version V2.5 only, also the IP address of the client in the client certificate.

NOTE
The validity period stored in the certificate is also checked. The CPU clock must therefore be set and date/time must be within the validity period, otherwise no communication takes place.

Signing and encryption

To allow you to check whether a certificate has been manipulated, certificates are signed.

There are various possible procedures here**:**

- Within the TIA Portal you have the possibility to generate and sign certificates. If you have protected your project and are logged in as a user with the function right to make security settings, you can use the global security settings. The global security settings allow access to the certificate manager and therefore to the certificate authority (CA) of the TIA Portal.
- Additional options are available for creating and signing certificates. In the TIA Portal, you can import certificates into the global certificate manager.
  - You contact a certificate authority (CA) and have your certificate signed.
    In this case, the certificate authority checks your identity and signs your certificate with the private key of the certificate authority. For this purpose you send a CSR (Certificate Signing Request) to the certificate authority.
  - You yourself create a certificate and sign it.
    To this purpose you use, for example, the "Opc.Ua.CertificateGenerator" program of the OPC Foundation. Alternatively, you use OpenSSL.
    You can find more information in Generating PKI key pairs and certificates yourself (Page 187).

Useful information: Certificate types

- Self-signed certificate:
  Each device generates and signs its own certificate. Application examples: Static configuration with limited number of communication nodes.
  No new certificates can be derived from a self-signed certificate. However, you need to load all self-signed certificates from partner devices to the CPU (STOP required).
- CA certificate:
  All certificates are generated and signed by a certificate authority. Application examples: Dynamically growing plants.
  You only need to download the certificate from the certificate authority to the CPU. The certificate authority can generate new certificates (partner devices can be added without CPU STOP).

Signing

The signature makes it possible to prove the integrity and source of a message as detailed below.

Signing starts with the sender creating a hash value from the plain text (plain text message). The sender then encrypts the hash value with its private key and subsequently transfers the plain text together with the encrypted hash value to the recipient. To verify the signature, the recipient needs the public key of the sender (this is contained in the X509 certificate of the sender). The recipient uses the sender's public key to decrypt the hash value received. The recipient then forms the hash value themselves from the plain text received (the hash process is contained in the sender's certificate). The recipient compares the two hash values:

- If the two hash values are identical, the plain text message has reached the receiver unchanged and has not been manipulated.
- If the two hash values do not match, the plain text message has not reached the receiver unchanged. The plain text message has been manipulated or has been distorted during transfer.

Encryption

Encrypting data prevents unauthorized parties from reading the content. X509 certificates are not encrypted; they are public and can be viewed by anyone.

Encryption involves the sender encrypting the plain text message with the public key of the recipient. To do so, the sender requires the recipient's X509 certificate, as it contains the public key of the recipient. The recipient decrypts the message with their private key. Only the recipient can decrypt the message: They alone hold the private key. The private key must therefore never be disclosed.

Secure channel

OPC UA uses the private and public key of client and server to establish a secure connection, the secure channel. Once the secure connection has been established, the client and server generate an internal key only known to them which they both use for signing and encrypting messages. This symmetric process (a shared key) is much faster than asymmetric processes (private and public key).

More information

An application example for the use of certificates with the TIA Portal can be found here: Using certificates with TIA Portal (https://support.industry.siemens.com/cs/ww/en/view/109769068).

11.2.3 Certificates with OPC UA

Usage of X509 certificates with OPC UA

OPC UA uses various types of X.509 certificates for establishing a connection from client to server:

- OPC UA application certificates
  Such X.509 certificates identify the software instance, the installation of client or server software. For the "Organization name" attribute, you enter the name of the company that uses the software.

  NOTE
  The OPC UA server of the S7-1500 uses application certificates even for the security setting "None" (no security). This ensures compatibility to OPC UA V1.1 and earlier versions.

- OPC UA software certificates
  This X-509 certificate identifies a specific version of the client or server software. These certificates contain attributes that describe which tests this version of the software has passed during certification by the OPC Foundation (or recognized test laboratories). For the "Organization name" attribute, you enter the name of the company that has developed or markets the software.

  NOTE
  Software certificates are not supported in STEP 7.

- OPC UA user certificates
  This X.509 certificate identifies the specific user who, for example, retrieves process data from the OPC UA server. This certificate is not required if the user can authenticate itself with a password, or if anonymous access is configured.

  NOTE
  User certificates are not supported in STEP 7.

The described certificates are end-entity certificates: They identify, for example, a person, an organization, a company or an instance (installation) of a software.

11.2.4 Creating self-signed certificates

Using the client's certificate generator

Many OPC UA client applications or SDKs are integrated in a sample application that allows you to generate certificates for the client from this application.

The description for certificate generation can generally be found in the context for describing the OPC UA client application.

Example client from the online support
The OPC UA .NET client for the SIMATIC S7-1500 OPC UA server (https://support.industry.siemens.com/cs/ww/en/view/109737901) creates a self-signed

software certificate of the client application in the Windows Certificate Store during the first program start. The documentation for this example describes the procedure for handling these certificates.

Using the certificate generator of the TIA Portal

If you use an OPC UA client that does not generate a client certificate, you can create self-signed certificates with STEP 7.

To do this, follow these steps:

1. In the properties of the CPU, double-click "<Add new>" under "Protection & Security > Certificate manager > Device certificates".
2. Click "Add".
3. In the "Create a new certificate" dialog, select the "OPC UA client" option for "Usage".
4. Click "OK".

In the field "Subject Alternative Name" STEP 7 automatically enters the URI for the generated certificate. In the program-specific certificate generation by means of the .NET stack of the OPC Foundation, the field is called, for example, "ApplicationUri" - it can have a different name in other tools for certificate generation.

More information

For more information on handling client certificates, refer to the section Handling of the client certificates of the S7-1500 CPU (Page 368).

11.2.5 Generating PKI key pairs and certificates yourself

This section is only relevant if you want to use an OPC UA client that cannot itself create a PKI key pair and a client certificate. In this case, you generate a private and a public key using OpenSSL, generate an X.509 certificate, and sign the certificate yourself.

Using OpenSSL

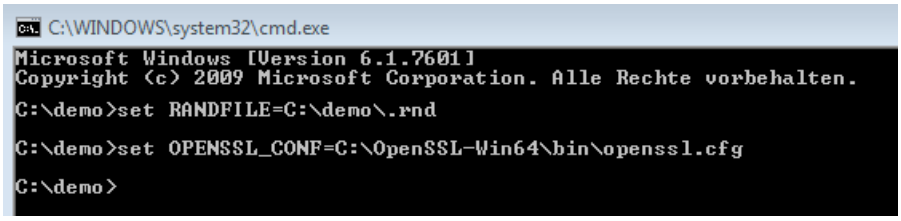
OpenSSL is a tool for Transport Layer Security that you can use to create certificates. You can also use other tools, for example XCA, a type of key management software with a graphical user interface for an improved overview of certificates issued.

To work with OpenSSL under Windows, follow these steps:

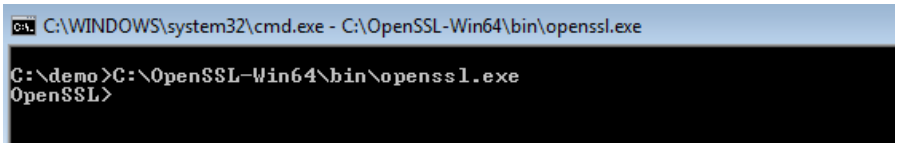
1. Install OpenSSL under Windows. If you are using a 64-bit version of the operating system, install OpenSSL in the "C:\OpenSSL-Win64" directory, for example. You can obtain OpenSSL-Win64 as a download from various providers for open source software.
2. Create a directory, for example "C:\demo".
3. Open the command prompt. To do so, click "Start" and enter "cmd" or "command prompt" in the search field. Right-click "cmd.exe" in the results list and run the program as an administrator. Windows opens the command prompt.
4. Change to the "C:\demo" directory. To do this, enter the following command: "cd C:\demo".

5. Set the following network variables:
   - set RANDFILE=c:\demo\.rnd
   - set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg

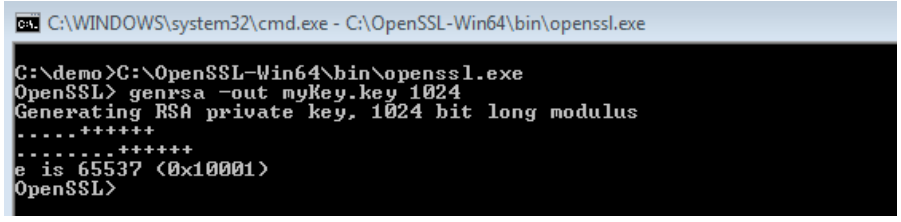
   The figure below shows the command line with the following commands:



6. Now start OpenSSL. If OpenSSL has been installed in the C:\OpenSSL-Win64 directory, enter the following: C:\OpenSSL-Win64\bin\openssl.exe The figure below shows the command line with the following command:



7. Generate a private key. Save the key to the "myKey.key" file. The key in this example is 1024 bits long; for greater RSA security, use 3072 bits in practice. Enter the following command: "genrsa -out myKey.key 3072" ("genrsa -out myKey.key 1024" in the example). The figure below shows the command line with the command and the output of OpenSSL:



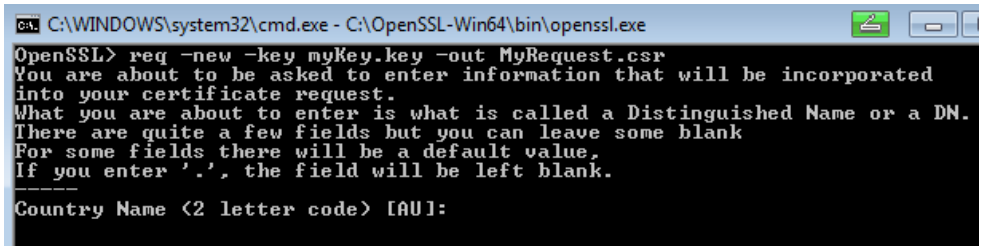
8. Generate a CSR (Certificate Signing Request). To do this, enter the following command: "req -new -key myKey.key -out myRequest.csr". During execution of this command, OpenSSL queries information about your certificate:
   - Country name: for example "DE" for Germany, "FR" for France
   - State or province name: for example "Bavaria".
   - Location Name: for example "Augsburg".
   - Organization Name: Enter the name of your company.
   - Organizational Unit Name: for example "IT"
   - Common Name: for example "OPC UA client of machine A"
   - Email Address:

NOTE

Note for S7-1500 CPU as server with firmware version V2.5

The IP address of the client program has to be stored in the "Subject Alternative Name" field of the created certificate for S7-1500 CPUs version V2.5 (only for this version); otherwise, the CPU will not accept the certificate.

The information you enter is added to the certificate. The figure below shows the command line with the command and the output of OpenSSL:



The command creates a file in the C:\demo directory containing the Certificate Signing Request (CSR); in the example, this is "myRequest.csr".

Using the CSR

There are two ways to use a CSR:

- You send the CSR to a certificate authority (CA): Read the information of the respective certification authority. The certificate authority (CA) checks your information and identity (authentication) and signs the certificate with the private key of the certificate authority. You receive the signed X.509 certificate and use this certificate for OPC UA, HTTPS or Secure OUC (secure open user communication), for example. Your communication partners use the public key of the certificate authority to check whether your certificate was really issued and signed by that CA (i.e. that the certificate authority has confirmed your information).
- You sign the CSR yourself: Using your private key. This option is shown in the next step.

Signing the certificate yourself

Enter the following command so that you can generate and sign your certificate (self-signed certificate) yourself: "x509 -req -days 365 -in myRequest.csr -signkey myKey.key -out myCertificate.crt".

The figure below shows the command line with the command and OpenSSL:



The command generates an X.509 certificate with the attributes that you transfer with the CSR (in the example "myRequest.csr"), for example with a validity of one year (-days 365). The command also signs the certificate with your private key ("myKey.key" in the example). Your communication partners can use your public key (contained in your certificate) to check that you are in possession of the private key that belongs to this public key. This also prevents your public key from being misused by an attacker.

With self-signed certificates, you yourself confirm that the information in your certificate is correct. There is no independent body that checks your information.

More information

You will find information about the handling of client certificates of the S7-1500 CPU in the section Handling of the client certificates of the S7-1500 CPU (Page 368).

11.2.6 Secure transfer of messages

Establishing secure connections with OPC UA

OPC UA uses secure connections between client and server. OPC UA checks the identity of the communication partners. For the authentication of client and server, OPC UA uses certificates in accordance with X.509 V3 the ITU (International Telecommunication Union). Exception: A secure connection is not established with the "No security" security policy.

Message security mode

OPC UA uses the following security policies to protect messages:

- No security

  All messages are unsecured. In order to use this security policy, establish a connection to a None end point of a server.
- Signing

  All message are signed. This allows the integrity of the messages received to be checked. Manipulations are detected. In order to use this security policy, establish a connection to a Sign end point of a server.
- Sign & Encrypt

  All messages are signed and encrypted. This allows the integrity of the messages received to be checked. Manipulations are detected. What is more, no attacker can read the content of the message (protection of confidentiality). In order to use this security policy, establish a connection to a "Sign & Encrypt" end point of a server.

The security policies are also named according to the algorithms used. Example: "Basic256Sha256 - Sign & Encrypt" means: Secure endpoint, supports a series of algorithms for 256-bit hashing and 256-bit encryption.

Layers required

The figure below shows the three layers that are always required for establishing a connection: the transport layer, the secure channel and the session.

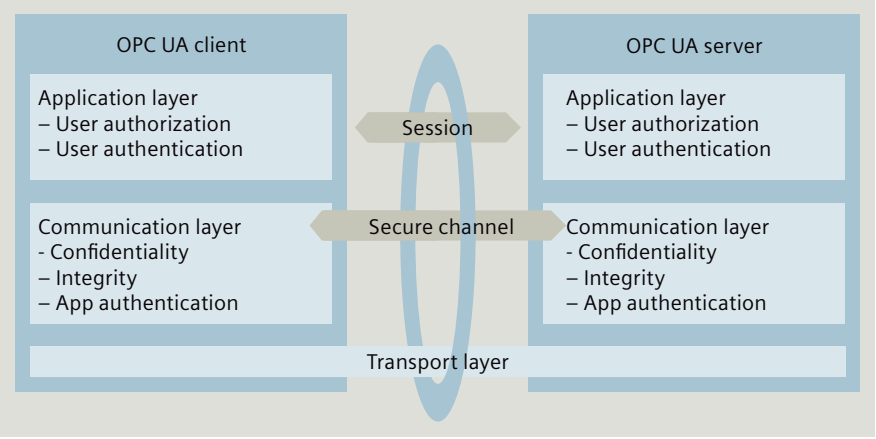


Figure 3-159 Necessary layers: transport layer, secure channel and session

- Transport layer:

  This layer sends and receives messages. OPC UA uses an optimized TCP-based binary protocol here. The transport layer is the basis for the subsequent secure channel.

- Secure channel

  The secure channel receives the data received from the transport layer, and forwards that data to the session. The secure channel forwards data of the session that is to be sent to the transport layer.

  In "Sign" security mode, the secure channel signs the data (messages) that is sent. When a message is received, the secure channel checks the signature to detect any manipulations.

  With a "Sign & Encrypt" security policy, the secure channel signs and encrypts the send data. Data received is decrypted by the secure channel, and the secure channel then checks the signature.

  With the "No security" security policy, the message packages pass the secure channel unchanged (the messages are received and sent in plain text).

- Session

  The session forwards the messages from the secure channel to the application, or receives from the application the messages that are to be sent. The application uses the process values or provides the values.

Establishing the secure channel

The secure channel is established as follows:

1. The server starts establishing the secure channel when it receives a request to this effect from the client. This request is signed or signed and encrypted, or the message is sent in plain text (security mode of the selected server end point). With "Sign" and "Sign & Encrypt", the client sends a "secret" (random number) with the request.
2. The server validates the client certificate (contained in the request, unencrypted) and checks the identity of the client. If the server trusts the client certificate,
   - it decrypts the message and checks the signature ("Sign & Encrypt"),
   - checks the signature only ("Sign"),
   - or leaves the message unchanged ("No security")
3. The server then sends a response to the client (same level of security as the request). The server secret is contained in the response. The client and server calculate a symmetric key from the client and server secret. The secure channel is now established.

The symmetric key (instead of the private and public key of client and server) is now used for signing and encrypting messages.

Establishment of the session

The session is executed as follows:

1. The client starts establishing the session by sending a CreateSessionRequest to the server. This message contains a Nonce, a random number that is only used once. The server must sign this random number (Nonce) to prove that it is the owner of the private key. The private key belongs to the certificate that the server uses to establish the secure channel. This message (and all subsequent messages) is secured in line with the security policies of the selected server endpoint (selected security policies).
2. The server responds with the CreateSession Response. This message contains the public key of the server and the signed Nonce. The client checks the signed Nonce.
3. If the server passes the test, the client sends a SessionActivateRequest to the server. This message contains the information that is required for user authentication:
   - User name and password, or
   - X.509 certificate of the user (not supported in STEP 7), or
   - No data (if anonymous access is configured).
4. If the user has the necessary rights, the server returns a message to the client (ActivateSessionResponse). This activates the session.

The secure connection between the OPC UA client and server has been established.

Establishing a connection to PLCopen function block

The PLCopen specification defines a range of IEC 61131 function blocks for OPC UA clients. The instruction UA_Connect initiates both a secure channel and a session following the pattern described above.

11.2.7 Certificate management via Global Discovery Server (GDS)

11.2.7.1 Automated certificate management with GDS

As of TIA Portal version V21 and S7-1500 CPU firmware version V4.1, you can also use the GDS push management functions for OPC UA client certificates. If there are several instances of the OPC UA client, a separate certificate can be created and customized for each instance. You can find information or restrictions in the section Handling client certificates during runtime (Page 371).

NOTICE
High resource consumption poses risks when using GDS If you use GDS, high resource consumption can have an impact on general security services. For example, the management of users or certificates can be affected with OPC UA. As soon as general security services are affected, the CPU reports this as an alarm in the diagnostics buffer and generates a syslog message. Adapt the use of resources to your actual requirements.

As of TIA Portal version V18 and S7-1500 CPU firmware version V3.0, you can also use the GDS Push Management function for web server certificates. The sequence of, for example, certificate updates via GDS Push management functions is identical here in principle to the certificate update of OPC UA server certificates. Instead of OPC UA server certificates, you transfer web server certificates to the CPU at runtime or during operation. The differences or restrictions are explained in the following description at the corresponding places.

As of TIA Portal V17 and S7-1500 CPU firmware version V2.9, you can use the certificate management services of the OPC UA server to transfer OPC UA server certificates during runtime.

OPC UA certificates, trust lists and certificate revocation lists (CRLs) for the OPC UA server of the S7-1500 CPU can be updated automatically using GDS Push Management functions. The automation of the certificate management eliminates any manual work required for reconfiguring the CPU, for example, after the period of validity of a certificate has expired, and a fresh download of the CPU. You can also use the GDS Push Management functions to transfer updated certificates and lists in the STOP and RUN operating states of the CPU.

The certificate management information model is specified in OPC UA Part 12 (OPC 10000-12: OPC Unified Architecture, Part 12: Discovery and Global Services).

The following sections provide a general overview of Global Discovery Services and the function of an automated certificate update supported as of TIA Portal V17 / CPU firmware version V2.9.

Discovery server

To connect to an OPC UA server, an OPC UA client requires information about its endpoint such as the endpoint URL and the security policy. When a large number of possible servers are available in the network, a discovery server can take over the search and management of this server information.

- OPC UA servers register with the discovery server.
- OPC UA clients request a list of accessible servers from the discovery server and then connect to the desired OPC UA server.

Global Discovery Server (GDS)

The OPC UA GDS concept allows the configuration of cross-subnet discovery services on the one hand and provides interfaces for central certificate management on the other hand.

A Global Discovery Server (GDS) makes mechanisms available for the central management of the following components:

- CA-signed certificates and self-signed certificates
- Trusted Lists and Certificate Revocation Lists (CRL)

A GDS thus provides an access point to central certificate management and takes over the task of a security server within an OPC UA network.

The main application of GDS is the management of CA-signed certificates with the corresponding CRLs:

- Initial creation of an OPC UA application certificate, for example, for the OPC UA server or for the web server
- Regular update of the trust list and the CRLs
- Renovation of an application certificate

Certificate management

Certificate management has the task of automating the administration and distribution of certificates and trust lists for different services or UA applications.

In this context, a distinction is made between the following roles:

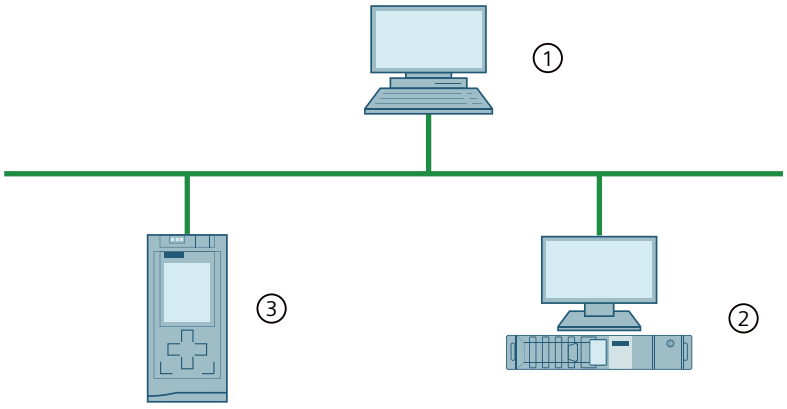
- Certificate manager - an OPC UA application that provides certificate management functions
- Certificate recipient – an OPC UA application that receives certificates, trust lists and CRLs from the certificate manager.

There are two models for certificate management: Pull and push management.

- With pull management, the OPC UA application acts as a client of the GDS server and uses certificate management methods to request certificate updates and trust list updates.
- With push management, the OPC UA application acts as a server and provides methods for an OPC UA GDS as OPC UA client. The GDS in the role of certificate manager uses these methods to transfer ("push") certificates and trusted list updates, see explanation of the concept for automated certificate update below.

System configuration with GDS

The figure below shows an example of the tasks of the devices involved in combination with a GDS that provides certificate management functions.



① Root CA - device that issues certificates for the system (these certificates can also be transmitted in other ways, for example, by email)

② OPC UA GDS with certificate manager creates or signs device certificates, manages trust lists and certificate revocation lists (CRLs), and writes certificates and lists to the devices (push function). This device requires OPC UA client functionality for the push function.

③ Device with OPC UA application receives "pushed" certificates and lists

Concept for automated certificate update for STEP 7 version V17 and higher

GDS and certificate manager are usually combined into one application; however, in the figure below, they are two separate components.

Devices such as "normal" OPC UA clients are also suitable as certificate managers, but they need to support the Bytestring data type that is required to transfer certificates, for example, an S7-1500 CPU firmware V2.9 and higher as OPC UA client or the UA Expert tool (Unified Automation) with GDS plugin.

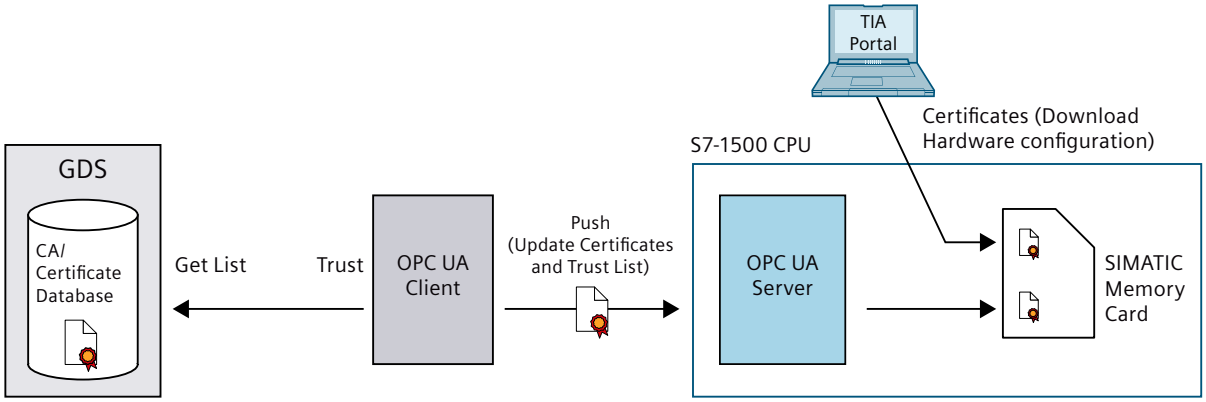
The OPC UA server of the S7-1500 CPU as certificate receiver provides the standardized methods and attributes that the OPC UA client certificates need to read and write trust lists and CRLs.

The focus in the context of the OPC UA server of the S7-1500 CPU is the description of the push function in contrast to the usual manner in which certificates are provided to the CPU: By loading the hardware configuration.

The figure below shows how to transfer certificates and lists for OPC UA in an S7-1500 CPU FW V2.9 or higher:

- Either by loading the hardware configuration (if appropriate, in STOP mode of the CPU; the certificates are part of the hardware configuration and can only be loaded in RUN mode under specific conditions; see Tip: Updating loaded certificates in RUN (Page 75))
- Or via GDS push methods in RUN or in STOP mode of the CPU.

It is not possible to use both transmission paths in parallel. If, for example, you have opted for transfer of OPC UA server certificates with GDS push functions at runtime, you must also transmit all the other certificate types to the CPU via this route.



More information

You can find more information on the certificates for OPC UA in the section What you should know about the certificate management (Page 62) and Certificates with OPC UA (Page 186).

11.2.7.2 Configuration limits for Push function

Number of certificates for Push function

For the OPC UA Push function, an S7-1500 CPU, regardless of the type, has a configuration limit of 62 trust list entries as of firmware version V2.9.

- Each activated certificate-based service (CPU application) "consumes" one entry each for a certificate and an entry for the private key.
- A Certificate Revocation List entry (CRL) counts just as an entry in the list of trusted certificates.
- A certificate that is used by different services (CPU applications) counts as a single trust list entry.

Size of elements for Push function (e.g. certificates)

Max. 4096 bytes

Example

You want to grant access to the OPC UA server for up to 62 OPC UA clients and fill the trusted list accordingly.

When you add a Certificate Revocation List entry in the trusted list, you can only trust up to 61 client certificates.

Additional OPC UA certificates can **not** be transferred by loading the hardware configuration to the CPU.

Tip

To keep the number of required certificates low, we recommend having the OPC UA client certificates signed by the same CA.

In this case, the CPU as OPC UA server only needs the corresponding CA certificate and CRLs. With these elements, the OPC UA server can then verify all client certificates signed by the CA. This means you do not have to add the individual client certificates to the trusted list.

11.2.7.3 Setting and loading GDS parameters

The following describes the settings required for the certificate update.

Requirement

- Depending on the application certificate, the corresponding STEP 7/TIA Portal version and S7-1500 CPU firmware version is required.

  See also here: What you should know about the certificate management (Page 62)
  - For OPC UA server certificates, for example, TIA Portal as of V17, CPU as of FW version V2.9
  - For web server certificates, for example, TIA Portal as of V18, as of CPU FW version V3.0
  - For OPC UA client certificates, e.g. TIA Portal V21, CPU as of FW version V4.1
- Timet/date of the CPU is set (generally applies to certificate-based communication)
- The OPC UA server is enabled.
- The service that the GDS push management uses must be enabled. For example, the web server must be enabled for the transfer of web server certificates.
- At least one endpoint with the "Sign & Encrypt" security policy must be configured for the OPC UA server. The partner must use this endpoint
- An authenticated user with sufficient function rights is configured
  The user must have a role that has the **"Manage certificates" function right**.

  This function right, in turn, has the following requirements:
  - **Project protection** must be enabled in the project tree: Project tree: "Security settings > Settings > Project protection".
  - The user with a role that has the "Manage certificates" function right is configured in the project navigation "Security Settings > Users and Roles".
    TIA Portal < V19: In the "OPC UA > General" area of the CPU settings, the following general user management setting must be enabled: "Enable additional user management via project security settings"

The Users and roles with OPC UA function rights (Page 266) section describes how to set the function rights.

Activating GDS

When the requirements listed above are met, you must still enable the GDS:

1. In the Inspector window (CPU parameters), go to the "OPC UA > Server > General" area.
2. Enable the "Enable Global Discovery Services (Push)" option.

Determining the certificate store used

Certificates that are managed using GDS, are in a different memory area than the certificates that are downloaded via the TIA Portal (STEP 7).

When GDS push certificate management is enabled, the services (applications) of the CPU also use certificates from the certificate store whose certificates are managed at runtime.

1. In the CPU settings, navigate to the area "Protection & Security > Certificate management".
2. Select the option "Use certificates provided by certificate management during runtime".

   The other option (use certificates configured and downloaded using TIA Portal) uses the certificates that are downloaded from the TIA Portal to the CPU with the configuration or configuration changes. In this certificate store, no certificates or trust lists can be updated at runtime and certificates can only be updated within specific constraints (see Tip: Updating loaded certificates in RUN (Page 75)).

Enabling the diagnostics for the lapsing of certificates

If you wish to be informed in advance about the lapsing of a certificate, select the "Enable system diagnostics event for the certificate lapsing" option in the area "Protection & Security > Certificate management".

Enter a percentage value in the text box "Show event at remaining certificate validity period of:".

Effect of these settings:

- At the instant when this value is reached by a certificate, a corresponding system diagnostics message appears till the certificate lapses or is refreshed.
- If the end of the validity period of a certificate has been reached, the CPU generates a corresponding system diagnostics message as well as an entry in the diagnostics buffer and the maintenance LED lights up.

Example:
The certificate transferred via GDS on June 01, 2022 has a validity from June 01, 2022 to June 30, 2022 (30 days). You have input a percent value of 10 for the diagnostics event. On June 27, 2022, when 90% of the period of validity lapses, a corresponding message will appear stating that the certificate that had been transferred will lapse on June 30, 2022. Regardless of the configured percentage value, upon lapsing of the period of validity of a certificate, a corresponding message is displayed in any case, an entry is made in the diagnostics buffer, and the maintenance LED lights up.

Download to CPU

When downloading the configuration to the CPU, you can delete the certificates that are managed via GDS before the download. When you confirm the deletion, the download is followed by a provisioning phase (see section on commissioning).

When you download the memory card outside of the CPU (card reader), this certificate store is always deleted.

When Global Discovery Services (Push) is activated and no pushed certificates are available, then no separate certificate, trust list or CRL is available for the OPC UA server.

11.2.7.4 GDS commissioning

Part 12 of the OPC UA specification distinguishes between a provisioning phase and a run time phase during certificate management.

In the provisioning phase, a GDS or OPC UA client provides initial trust lists and CRLs for clients of the OPC UA server. In this phase, the OPC UA server of the CPU accepts all client certificates and lists it is offered – similar to the "Trusted clients" setting for the OPC UA server that all client certificates are accepted during runtime. This is the only way in which a connection to clients not known to the server is possible. For example, clients that the server cannot authenticate using existing certificates or trust lists until it has received the corresponding client certificate or the corresponding trust list.

The provisioning phase is characterized by lower security; therefore, the provisioning phase is indicated by a lit Maintenance LED and a corresponding diagnostics buffer entry (Maintenance demanded).

During the runtime phase, the existing CRLs are updated, for example, and the certificates and trust lists are renewed. Communication is secure in this phase.

Requirement

Only authorized users with sufficient function rights can set up a connection in the provisioning phase. The users must have a role with the function right "Manage certificates".

See also Setting and loading GDS parameters (Page 197).

Rules for the provisioning phase

In the provisioning phase, the OPC UA server of the CPU cannot authenticate the OPC UA clients that initiate connection establishment. Therefore, the following rules must be observed:

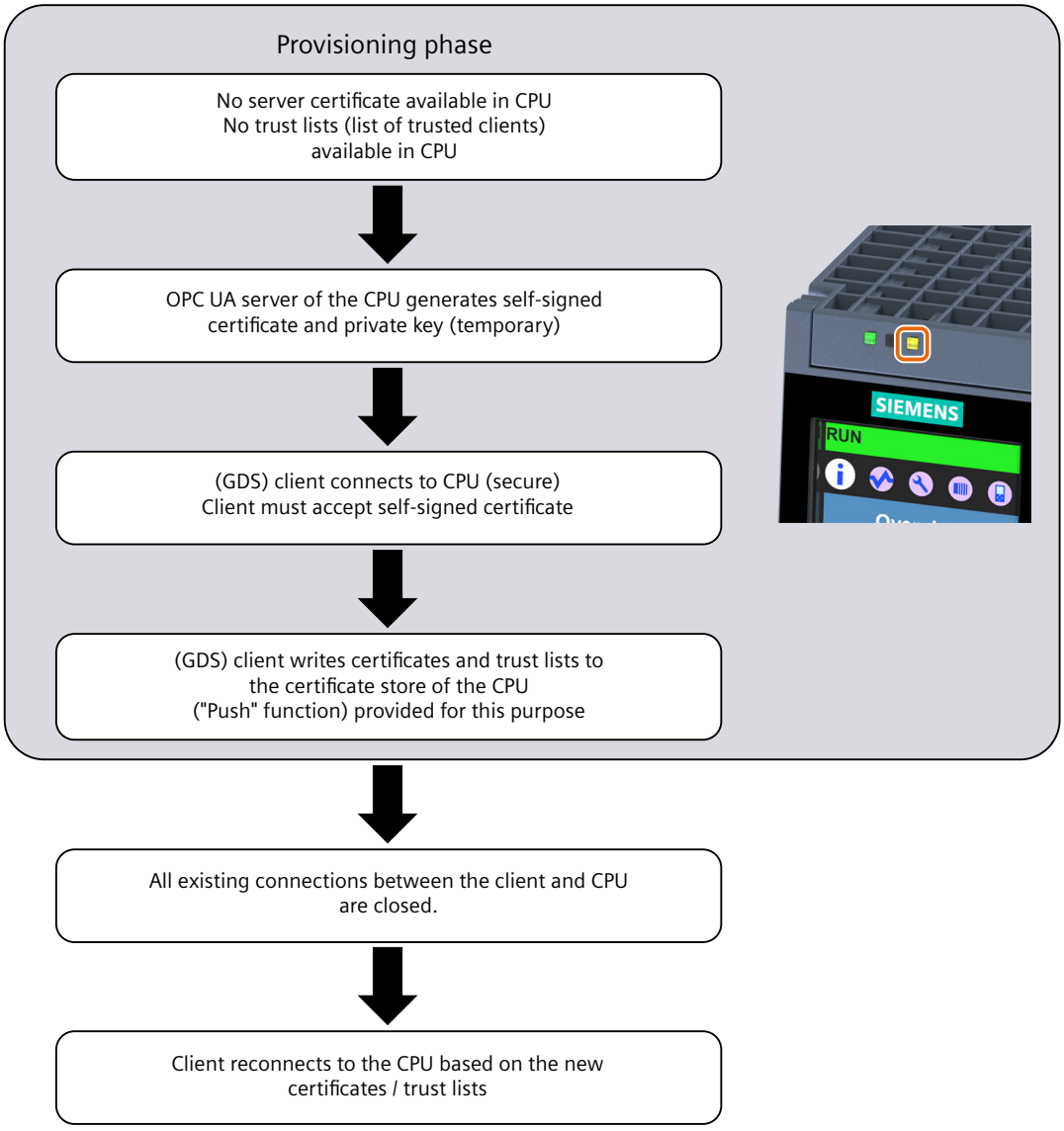
- Ensure a secure environment, e.g:
  - Only the commissioning personnel have access to the CPU.
  - The CPU and programming device are directly connected to each other.
  - Check that the correct devices are communicating with each other.
- Limit the time for this phase.

The CPU signals that it is in the provisioning phase by the lit Maintenance LED as well as a corresponding diagnostics buffer entry (Maintenance demanded).

Sequence of the provisioning phase

The following provides an outline of the process of the provisioning phase for OPC UA server certificates and trust lists.

The process of the provisioning phase for web server certificates is comparable. In contrast to OPC UA, the GDS client only pushes web server certificates but not trust lists into the corresponding certificate store.



Entering the provisioning phase

After startup of the OPC UA server, the CPU automatically enters the provisioning phase when one of the following conditions is met:

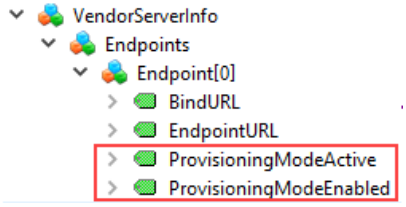
- The OPC UA server certificate is the initial self-signed certificate generated by the CPU and has not yet been replaced by a valid server certificate.
- The trust list (list of trustworthy clients) is empty.

The OPC UA server certificate generated by the CPU contains the most important parameters of the OPC UA server and is re-generated, including the private key, after each startup of the OPC UA server following POWER ON - until the valid server certificate is present. For this reason, the OPC UA server may take longer to start up after a POWER ON.

After the hardware configuration is downloaded, the certificate store for certificates that can be updated during runtime is deleted on download or the certificates are retained, depending on the setting. This means that if GDS is activated and the certificate store has been deleted, the CPU is in the provisioning stage after the hardware configuration has be loaded.

Provisioning phase diagnostics

In addition to the lit Maintenance LED, the GDS address model has two nodes that provide information on whether the OPC UA server of the CPU is in the provisioning phase:



You can only use the two nodes as marked in the figure for diagnostics if the requirements for GDS are met (endpoint security signed & encrypted plus administrator function rights available).

ProvisioningModeEnabled: Indicates that a provisioning phase is supported

ProvisioningModeActive: Indicates that the OPC UA server of the CPU is in the provisioning phase.

End of the provisioning phase

The CPU ends the provisioning phase automatically when the following conditions are met:

- The certificate generated and self-signed by the CPU for the provisioning phase has been overwritten by a valid server certificate. This valid server certificate can be a self-signed certificate or a CA-signed certificate.
- The trust list in the CPU is not empty, i.e. client certificates of the OPC UA clients to be trusted or CA certificates for checking the client certificates are available.

If the OPC UA client transfers a CA-signed certificate and also adds the CA certificate to the trust list, the OPC UA server of the CPU can automatically accept all other certificates from OPC UA clients that were signed by the same CA.

Request of a valid server certificate

As of TIA Portal version V18 / S7-1500 CPU version V3.0, in addition to OPC UA server certificates, certificates for other services can also be transferred to the CPU, for example, for the web server.

The corresponding service, for example, the OPC UA server of the CPU, receives a valid certificate in the following steps:

1. A GDS client (OPC UA client) calls the method "CreateSigningRequest" to request a server certificate: with a Certificate Signing Request (CSR).
2. This CSR must be signed by a Certificate Authority (CA).
3. The signed CSR must then be transferred back to the OPC UA server of the CPU as a certificate.

The OPC UA server of the CPU makes this method available if the client has the required function right "Manage certificates".

The "CreateSigningRequest" method allows for the following variants:

- Certificate update without creating a new key pair (internal CPU keys that are already available are used)
- Certificate update with creation of a new key pair (CPU-internal)

There is also the possibility to generate certificates with externally created key pairs.

NOTICE
Recommended procedure to generate certificates Transport of private keys should be avoided; a private key should not leave a device. We, therefore, recommend the generation of a certificate without creating a new key pair or with the creation of a key pair inside the CPU.

Create certificate without key pair

- The "CreateSigningRequest" method returns a Certificate Signing Request (CSR), that is, a file (*.csr) with specific information on the server or on the service, for example, application name and URL.
- Outside of the CPU, this CSR must be validated and signed by a Certificate Authority (CA) and the certificate must be returned.
- The certificate must then be transferred to the CPU ("pushed") using the "UpdateCertificate" method.

The key does not leave the CPU in this scenario.

Create certificate with internally created key pair

The procedure is similar to the method explained in the previous section; the only difference is that a key pair is generated in addition to the CSR. You specify in the parameter of the "CreateSigningRequest" method that it is to generate a key pair.

The private key does not leave the CPU in this procedure either.

The generation of a new key pair creates a very heavy load on the CPU. The CPU processes this request over a longer period of time with lower priority in the reserved area for the communication load. The duration of this time period depends on the performance of the CPU.

Because the share of the set communication load is fully utilized during key generation over a longer period of time, set the "Cycle load due to communication" share so that the maximum cycle time is not exceeded and sufficient reserves are available. For this, use the web server

page "Diagnostics > Runtime information" of the CPU. This page shows information about the current program/communication load and cycle time of your user program. Via a controller, you can get help on the effects of a changed communication load on the cycle time.

Create certificate with externally created key pair
The certificate is generated with the help of tools, for example, that can generate additional keys.

Certificate and keys are transferred to the CPU using the "UpdateCertificate" method.

Due to low security, this procedure is not recommended.

NOTICE
Different keys for different target systems Always use newly generated keys for a production system. If you simulate and test your project, e.g. with PLCSIM Advanced on your PC, do not under any circumstances use the keys used for the simulation also for a productive system. Restrict the access to PC-based controllers by setting up appropriate permissions.

11.2.7.5 Address model for the push certificate management

The OPC UA specification Part 12 (OPC 10000-12: Discovery, Global Services) defines methods and attributes for OPC UA servers, for example, that enable GDS or OPC UA clients to update certificates and trust lists on the server ("Push certificate management"). These methods and attributes are also included in the address model of the OPC UA server.

The relevant section in the address model of the OPC UA server of the S7-1500 CPU is explained below.

Requirement

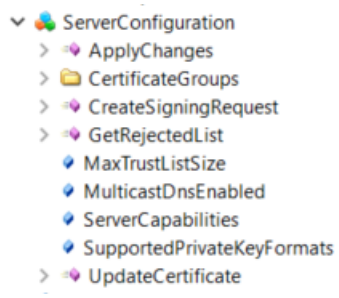
The following requirements must be met for the relevant methods and attributes to become visible for the GDS push functionality:

- GDS is activated.
- The set security policy supports the integrity and confidentiality of the data through signature and encryption (Sign & Encrypt).
- Access with runtime function right "Manage certificates"

Address model for the GDS push functionality

The address model for the GDS push functionality corresponds to the "Information Model for Push Certificate Management" of the OPC UA specification OPC 10000-12: Discovery, Global Services.

You will find the following structure below the "ServerConfiguration" node:



Methods and attributes for access to the address model

The methods and attributes are briefly described below with special features and restrictions of the specific address model of the S7-1500 CPU. The OPC UA specification listed above contains the general description.

You can find a detailed description of the individual methods below this overview table.

Method / Attribute (Variable)	Description
CreateSigningRequest	Method for generating a PKCS#10-encoded certificate request signed with the private key of the service (for example, OPC UA server).
UpdateCertificate	Method for updating the server certificate, for example, for the OPC UA server.
ApplyChanges	Method for applying a security-relevant change if the "ApplyChangesRequired" attribute was set when executing a previously executed method. **Note** If, as a result of "ApplyChanges", a certificate is changed, the CPU interrupts the connections/sessions that are secured via this certificate. Background: The basis for the secured connections - the certificate - is no longer valid.
GetRejectedList	Method that returns a list of certificates that were rejected by the OPC UA server. Rejected certificates are currently not stored by the OPC UA server of the S7-1500 CPUs. The method returns an empty array (RejectedList).
ServerCapabilities	Variable is not supported by the OPC UA server of the S7-1500 CPU.
SupportedPrivateKeyFormats	Variable that specifies permitted formats of the private key. For S7-1500 CPUs only "PEM" (String Array)
MaxTrustListSize	Variable that specifies the maximum size of the trust list.
MulticastDnsEnabled	Variable that specifies whether multicast DNS is supported. For S7-1500 CPUs, the value is "False".
CertificateGroups	Object (folder) that organizes all certificate groups supported by the OPC UA server. The certificate groups contain the objects that can be updated dynamically during runtime: For

Method / Attribute (Variable)	Description
	example, one trust list each and one or multiple certificates that are assigned to a service (for example, OPC UA application). Details on the structure of the CertificateGroups object and the methods and attributes that are available in the object are described in the next section.

CreateSigningRequest

The method has the following parameters:

Parameter	Data type	Description
[in] certificateGroupId	NodeId	NodeId of the CertificateGroup object.
[in] certificateTypeId	NodeId	Requested certificate type. List of permitted certificate types is specified by the "CertificateTypes" variable of the certificate group. For the OPC UA server for example, certificate type "RsaSha256ApplicationCertificateType", for the web server the certificate type "HttpsCertificateType"
[in] subjectName	String	Subject Name that is requested in the Certificate Request. If not specified, the current Subject Name of the certificate is used.
[in] regeneratePrivateKey	Boolean	True: Server generates a new private key. This key is saves until the UpdateCertificate methods with the matching signed certificate is called. False: Server uses the available private key.
[in] nonce	ByteString	Additional nonce for generating the new private key (see regeneratePrivateKey). Must be at least 32 bytes long.
[out] certificateRequest	ByteString	PKCS #10 - DER coded Certificate Request.

Method Result Codes

Result Code	Description
Bad_InvalidArgument	certificateTypeId, certificateGroupId or subjectName is invalid.
Bad_UserAccessDenied	The current user does not have the required function rights.

UpdateCertificate

Applications:

- Generation of certificate with CreateSigningRequest. No private key is available.
- New private key and new certificate were generated outside of the server. Both are updated with UpdateCertificate.
- Certificate generated and signed with the private key of the existing certificate. No private key is available.

Parameter	Data type	Description
[in] certificateGroupId	NodeId	NodeId of the CertificateGroup object.
[in] certificateTypeId	NodeId	Requested certificate type. List of permitted certificate types is specified by the "CertificateTypes" variable of the certificate group.
[in] certificate	ByteString	DER-coded certificate that replaces the existing certificate.
[in] issuerCertificates	ByteString	Issuer certificates
[in] privateKeyFormat	String	Format of the private key. Currently only PEM is supported. If the privateKey is not specified: zero or empty string.
[in] privateKey	ByteString	Privater key coded as specified in privateKeyFormat.
[out] applyChangesRequired	Boolean	Indicates that the "ApplyChanges" method must be called before you use the new certificate.

Method Result Codes

Result Code	Description
Bad_InvalidArgument	certificateTypeId or certificateGroupId is invalid.
Bad_CertificateInvalid	The certificate is invalid or the format is not supported.
Bad_NotSupported	The private key is invalid or the format is not supported.
Bad_UserAccessDenied	The current user does not have the required function rights.
Bad_SecurityChecksFailed	Error occurred when verifying the integrity of the certificate.

Apply Changes

The method has no parameters.

Method Result Codes

Result Code	Description
Bad_UserAccessDenied	The current user does not have the required function rights.

GetRejectedList

The method has the following parameters:

Parameter	Data type	Description
[out] certificates	ByteStrings	DER-coded list of rejected certificates. The method currently returns an empty list (empty array), because rejected certificates are not stored.

Method Result Codes

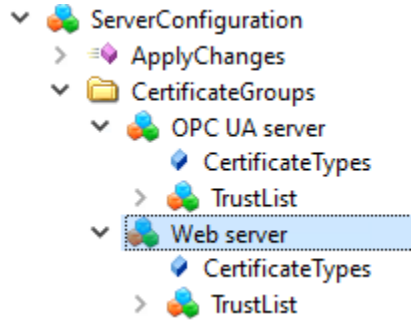
Result Code	Description
Bad_UserAccessDenied	The current user does not have the required function rights.

11.2.7.6 CertificateGroups in the address model

Certificates and trust lists for services or applications of the CPU (for example, OPC UA servers) that can be updated during runtime are located in the address model in the "CertificateGroups" object - there is one certificate group each for the various services of the S7-1500 CPU. For the OPC UA server certificate, the certificate group has the name "OPC UA server".

CertificateGroup in the address model

The following figure shows an example structure of the "CertificateGroups" object below the "ServerConfiguration" node. In this example, the OPC UA server and the web server of the CPU use certificates that can be updated during runtime.



You can change the name of the certificate store at runtime (e.g. "OPC UA server ") in STEP 7 (TIA Portal):

1. In the Inspector window (CPU properties), navigate to the area "Protection & Security > Certificate management".
2. Enable the option "Use certificates provided by certificate management during runtime" option.
3. Change the name of the certificate store at runtime in the table below. 1-64 characters in 7-bit ASCII format are permitted.
   The first column shows the activated service for which certificates can be transferred in runtime. The "ID" column contains a fixed numerical identifier that is used internally by the CPU to reference the certificates. The respective application URI is generated automatically

based on the entry in the "Certificate store at runtime" column. If you change the name of the certificate store at runtime, the respective application URI also changes.

Here is an example for the display in the area "Certificate management":

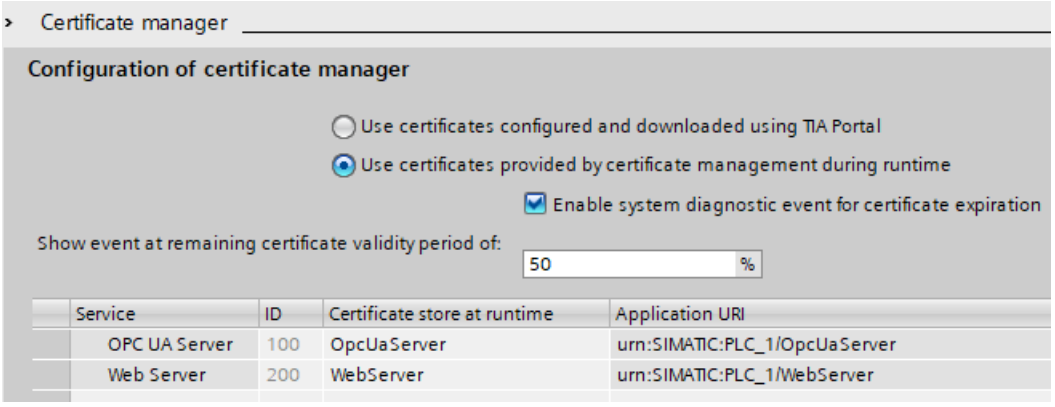


Figure 3-160 Certificate management settings

If you have activated the OPC UA client of the CPU and also enabled certificate management during runtime, you can change the IDs of the individual certificates. Each ID can only be assigned once in the project. STEP 7 shows duplicate IDs as incorrect.

"CertificateTypes" node

The "CertificateTypes" variable specifies the NodeIds of the certificate types that are assigned to the server application.

For the OPC UA server service, for example, the "RsaSha256ApplicationCertificateType" CertificateType is supported, for the web server, it is the "HttpsCertificateType CertificateType".

"TrustList" node

The node for the trust list object (TrustList file) defines an OPC UA file type (Binary encoded stream) that contains information on the certificates and CRLs that can be read and updated in the "pki store\trusted\issuer" directory of the Memory Card. This node provides methods and attributes that make reading and updating possible.

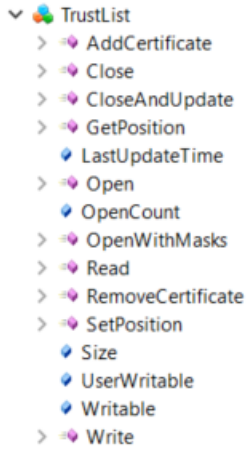
The node is an instance of the OPC UA data type "TrustListDataType" with the following structure:

Parameter	Data type	Description
specifiedLists	TrustListsMasks	Bit mask that shows which lists contain information.
trustedCertificates	ByteStrings	List of the application certificates and CA certificates that can be trusted.

Parameter	Data type	Description
trustedCrls	ByteStrings	CRLs for the certificates in the "trustedCertificates" list.
issuerCertificates	ByteStrings	List of the CA certificates that are required for validating the CA signed certificates.
issuerCrls	ByteStrings	CRLs of the CA certificates in the "issuerCertificates" list.

Structure of the "TrustList" node

The "TrustList" node has the following structure:



Methods and attributes for the "TrustList" node

Below is a description of the nodes under "TrustList" that supplement the methods of the Object Type "FileType". The TrustList Type is derived from FileType (see OPC 10000-5: OPC Unified Architecture, Part 5: Information Model).

Method / Attribute (Variable)	Description
LastUpdateTime	Variable that shows the time of the last update.
OpenWithMasks	Method that permits a client to only read a part of the TrustList.
CloseAndUpdate	Method for closing the TrustList file and applying the changes.
AddCertificate	Method for adding a single certificate to the TrustList.
RemoveCertificate	Method for removing a single certificate from the TrustList.

Description of the methods

The description of the methods with their result codes, attributes and types of the TrustList object is available in the OPC UA specification Part 12, Discovery and Global Services.

11.2.8 Role-based security in OPC UA

11.2.8.1 Interesting facts about role-based security

In OPC UA, the concept for role-based security is defined in Part 18 of the OPC UA specification (OPC 10000-18: UA Part 18: Role-Based Security). Parts 3 and 5 of the OPC UA specification, which contain individual aspects of the role definition, are also relevant, e.g. which roles a server should support with which permissions and which objects are defined with which attributes or properties in the address space.

With the implementation of the role-based concept for the S7-1500 CPUs as of FW version V4.0, the OPC UA server can manage in detail the access of specific clients to the address space.

Individual OPC UA access rights to nodes in the address space

Using role-based security in OPC UA, you can configure roles with permissions and access restrictions to nodes in existing namespaces.

The configuration options for roles and permissions in the server interface together with the user management in the TIA Portal (users and roles) enable effective access management.

Requirements for using role-based security

- S7-1500 CPU as of FW version V4.0
- TIA Portal:
  - To add user-defined roles to OPC UA, you need TIA Portal as of version V20 Update 3.

Relationship between roles/permissions for OPC UA and roles/function rights for users and roles

The following permissions are required to perform actions in a namespace, e.g. reading or writing to a node:

- Access to the OPC UA server of a CPU
- Permissions for the namespace

To access the OPC UA server of a CPU, a user from the local or central user management requires a role with the "OPC UA server access" function right. You can add/edit users and roles in the security settings of the project under "Users and roles".

You configure the permissions for the namespace in the "Access control at OPC UA server" editor of a CPU. Open the editor by double-clicking the entry of the same name in the project navigation (PLC > OPC UA communication). There you have the following configuration options for OPC UA communication:

- Assignment of existing roles (from the Security settings of the project > Users and roles) to the OPC UA user roles.
  Only roles that contain the "OPC UA server access" function right can be assigned to an OPC UA user role.
- Assignment of default permissions for the namespace of the server interface.
- Configure access restrictions, e.g. that the messages must be signed and encrypted.

The connection between users and OPC UA user roles is formed by the roles in the project with the "OPC UA server access" function right. Mapping the roles in the "Access control at OPC UA server" editor creates a hierarchy of responsibilities that regulate user access:

- Local or central user management of the CPU:
  Responsible for authenticating the users (OPC UA clients) who access the OPC UA server.
- OPC UA server of the CPU:
  Responsible for authorizing users (OPC UA clients). The OPC UA server of the CPU checks whether a user is allowed to perform the requested action (e.g. read or write to a node).

During operation, a user (OPC UA client) who is assigned a role with the "OPC UA server access" function right can be authenticated by the OPC UA server and can access the OPC UA server.
The user can perform actions in the namespace in accordance with the OPC UA user role assigned to this role.

User roles on the OPC UA server

When importing companion specifications with user management data, you can choose whether or not you want to import the configuration of the user management data. It is also possible to import individual OPC UA roles.

You can assign (map) roles from the project to the OPC UA roles contained in the Companion specification. You can only assign roles that contain the "OPC UA server access" function right.

You can also see next to each OPC UA role in which namespace this OPC UA role is defined and the configured standard authorizations for this namespace. An OPC UA role can also be valid for several namespaces.

For some pre-defined OPC UA roles in namespace 0, there are no direct equivalents in "Users and roles", e.g. the "AuthenticatedUser" role. Users who successfully authenticate themselves with username/password receive the access rights that were assigned to the "AuthenticatedUser" role.

In addition to the role permissions, you can also define the access restrictions for the companion specification to be imported. A companion specification to be imported can also contain namespaces that already exist with the same name in a server interface. In this case, you can choose whether the configured settings in the project or the import file should apply to this namespace.

NOTE

Naming the standard OPC UA user roles
The pre-defined standard OPC UA roles are sometimes named like users, which can lead to misunderstandings. The OPC UA roles and their rights are initially independent of the user management. Only by assigning the role authorizations (OPC UA user role - Assigned role in the project) do you connect the OPC UA roles with the user administration in the TIA Portal.
Example: There is the "Anonymous" **user** in the user management. OPC UA has the **standard OPC UA user role** "Anonymous".

Well-Known Roles

The OPC Foundation has pre-defined roles in namespace 0 (http://opcfoundation.org/UA/). These roles are available without a separate role definition for every OPC UA server that supports role-based security.

Examples of "Well-Known Roles":

- Anonymous
- AuthenticatedUser
- Observer
- Operator
- Engineer
- Supervisor
- ConfigureAdmin
- SecurityAdmin

You can easily add these roles as standard OPC UA roles in the TIA Portal.

Roles and permissions for OPC UA

You can assign OPC UA user roles and OPC UA authorizations for complete namespaces (i.e. for all nodes in the namespace).

You use either pre-defined standard OPC UA roles or the OPC UA roles imported with a nodeset. You can also create custom OPC UA user roles for custom namespaces of OPC UA server interfaces and assign them to these namespaces.

You can assign the following OPC UA permissions to an OPC UA user role:

- Browse - A client with this permission can see references to/from this node, i.e. also for all attributes with the exception of the Value and RolePermissions attributes.
- Read - A client with this permission can read the Value attribute.
- Write - A client with this permission can write to the Value attribute.
- Call - A client with this permission can call the corresponding method; valid for objects, object types or methods.
- Receive events - A client with this permission can receive events (alarms and conditions).
- Read Role Permissions - A client with this permission may read the RolePermissions attribute.

You can also activate access restrictions for namespaces:

- Signing Required - A client only has access to the nodes if a SecureChannel is used that digitally signs the messages. See also the explanation of the "Apply Restrictions to Browse" access restriction.
- Encryption Required - A client only has access to the nodes if a SecureChannel is used that encrypts the messages. See also the explanation of the "Apply Restrictions to Browse" access restriction.
- Apply Restrictions to Browse - If this access restriction is enabled, the requirements described for "Signing required" and "Encryption required" also apply to the browse permission.

To assign an OPC UA user role to a user, create a role with the "OPC UA server access" function right in the editor for users and roles. Only roles that contain this function right can be assigned to OPC UA user roles.

Rules

- To assign roles to users or user groups, use the editor for users and roles (Security settings > Users and roles in the project tree).

  These users and user groups are also used by the OPC UA server. The CPU or a connected UMC server carries out the authentication service when logging on.
- The logged-in user must have a role with the "OPC UA server access" function right.
- Adding additional roles during runtime is not possible. All roles and associated OPC UA permissions for the address space have to be configured before commissioning and loaded in the CPU.

  You can achieve greater flexibility with regard to users if you use a UMC server for central user management and combine users into groups.
- OPC UA offers various criteria for authorizing server access; in OPC UA jargon these are "mapping rules", for example:
  - User identity: Access depends on the identity of the user
  - Application identity: Access depends on the ApplicationUri specified in the client certificate
  - Endpoint: Access depends on the URL used to access the server.

  The OPC UA server of the S7-1500 CPU only validates the permission via the user identity.
- The OPC UA server of the S7-1500 CPU supports "Well-Known Roles", which are defined in OPC 10000-3: UA Part 3: Address Space Model.

More information

You can find the latest information on configuring the role-based security for S7-1500 CPUs in the product information (https://support.industry.siemens.com/cs/ww/en/view/68052815).

11.2.8.2 Configuring role-based access control for OPC UA

The following sections describe how to configure permissions for OPC UA roles in the editor for OPC UA communication.

Requirement

- TIA Portal as of Version V20 Update 3
- S7-1500 CPU as of FW version V4.0 with the following parameterization:
  - Access control for local user management is enabled (Protection & Security > Access control)
  - The OPC UA server of the CPU **and** the access control for the OPC UA server are enabled (OPC UA > Server > General)

- You have configured the required users and their roles:
  - Users who are to have access to the OPC UA server have been assigned a role that contains the "OPC UA server access" function right.
  - Users who are to manage certificates have been assigned a role that contains the "Manage certificates" function right.

    In the "Access control on the OPC UA server" editor, you must assign a role for this user in the project to the standard OPC UA role "SecurityAdmin".

Overview: Editor for OPC UA role permissions and access restrictions

You can find the editor for managing roles and permissions in the project navigation under the desired CPU ("OPC UA communication > Access control at OPC UA server"). Double-click the "Access control at OPC UA server" entry to open the editor. After opening, the editor shows the "Role permissions" tab.

If the access control for the CPU is not configured as described in the requirements, the editor displays a message in the upper area. The message contains a link to the corresponding area in the CPU properties. The message only disappears when the CPU is configured as described in the requirements.

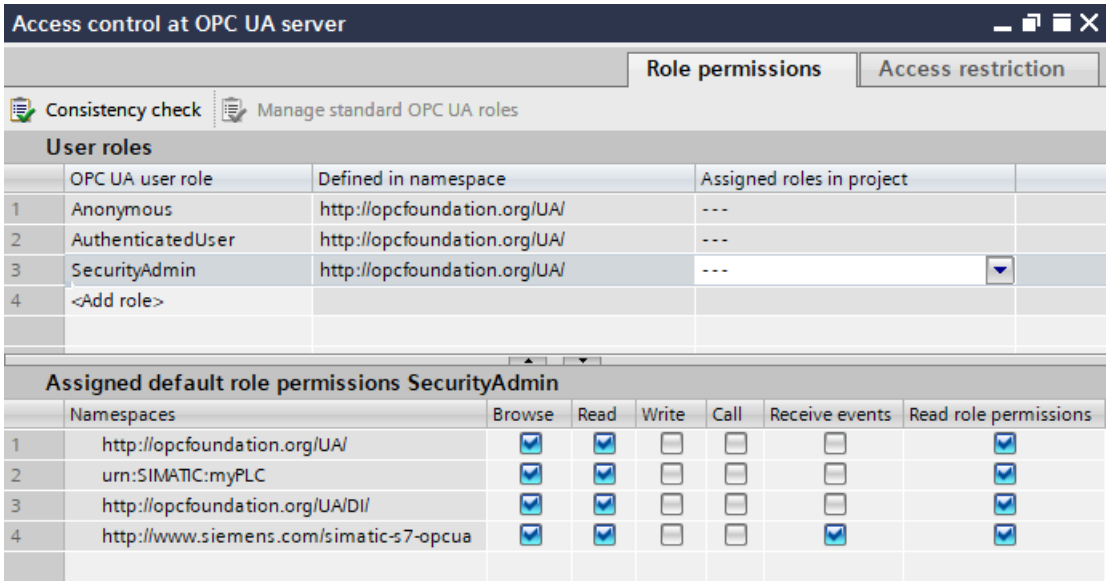


Figure 3-161 Access control with OPC UA server

The "User roles" area shows the OPC UA user roles with their namespace details and the assigned role in the project.

If you have previously imported a node set file with role definitions, the OPC UA user roles defined there are also listed.

You can easily add additional standard OPC UA roles by clicking the "Manage standard OPC UA roles" button and activating the desired roles. The activated standard OPC UA roles are defined in the OPC UA namespace (http://opcfoundation.org/UA/) and are added in the "User roles" area.

The editor also offers the option of creating custom OPC UA user roles. You can only create self-defined OPC UA user roles for self-defined namespaces of OPC UA server interfaces.

You can check the configuration of the OPC UA user roles by clicking the "Consistency check" button. You can see the result of the consistency check in the Inspector window (Info tab >

General). A configuration is faulty in the following cases, for example, and cannot be loaded onto the CPU:

- You use more than 52 role assignments.
- No role from the local user management is assigned to an OPC UA user role.
- An incorrect role from the local user management is assigned to an OPC UA user role:
  - The role is no longer available in the local user management.
  - The "OPC UA server access" function right has been removed from the role.

You configure the access restrictions for namespaces of the OPC UA server in the "Access restrictions" tab. For example, you can specify that client access is restricted to encrypted connections.

Mapping OPC UA user roles

In the "Access control for the OPC UA server" editor, assign a role from the project to the OPC UA user roles. The role from the project must contain the "OPC UA server access" function right.

The editor shows the existing OPC UA user roles in the "User roles" area. The following OPC UA user roles are available by default, with their namespace details for the OPC UA namespace (http://opcfoundation.org/UA/):

- Anonymous: Role for a user without credentials
- AuthenticatedUser: Role that every user with valid credentials automatically has
- SecurityAdmin: Role for the administration of security settings and user permissions

You cannot assign a role from the project to the OPC UA user roles "Anonymous" and "AuthenticatedUser". You must assign a role to the "SecurityAdmin" OPC UA user role that also includes the "Manage certificates" function right.

To assign a role from the project to an OPC UA user role, select the corresponding role in the "Assigned roles in project" column.

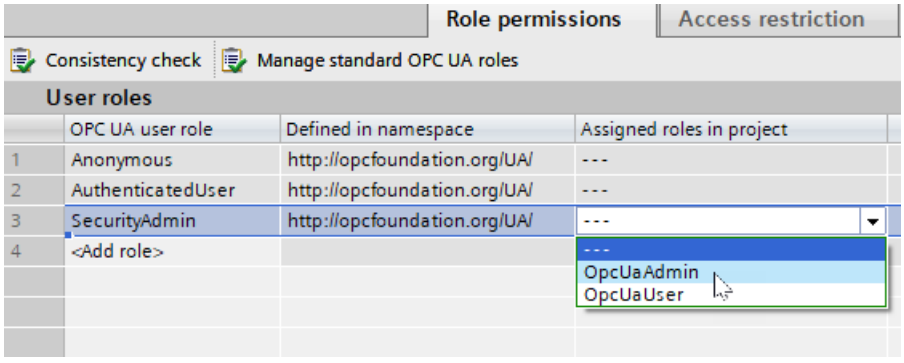


Figure 3-162 Assigning role from the project

Assigning permissions for namespaces

To be able to perform actions in the respective namespaces, you must assign the corresponding permissions for the namespaces to the OPC UA user roles. To do this, select the desired OPC UA user role in the "Access control on the OPC UA server" editor. Then activate the required permissions for the namespaces in the "Assigned default role permissions" area.



Assigned default role permissions SecurityAdmin

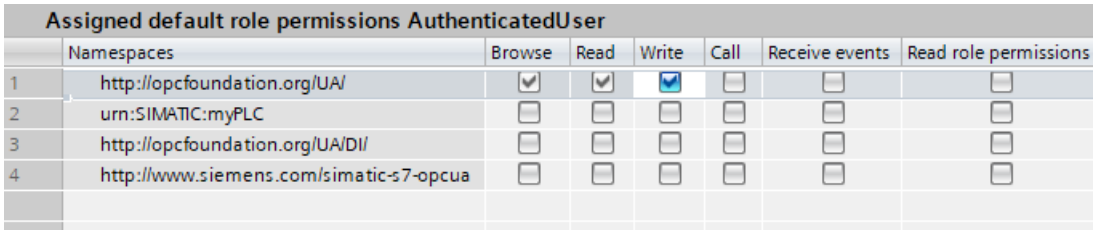
	Namespaces	Browse	Read	Write	Call	Receive events	Read role permissions
1	http://opcfoundation.org/UA/	☑	☑	☐	☐	☐	☑
2	urn:SIMATIC:myPLC	☑	☑	☐	☐	☐	☑
3	http://opcfoundation.org/UA/DI/	☑	☑	☐	☐	☐	☑
4	http://www.siemens.com/simatic-s7-opcua	☑	☑	☐	☐	☑	☑

Figure 3-163 Editing permissions for namespaces

By default, no permissions are enabled for the OPC UA user roles "Anonymous" and "AuthenticatedUser" for the namespaces. If you assign permissions for these two OPC UA user roles, this has the following effect on other OPC UA user roles:

- Add permissions:
  - Permissions that you add to the "Anonymous" OPC UA user role are automatically added to all other OPC UA user roles.
    These permissions can only be changed for the "Anonymous" OPC UA user role. All other OPC UA user roles display these permissions in gray and enabled, since each OPC UA user role must have at least the permissions of the "Anonymous" OPC UA user role.
  - Permissions that you add to the "AuthenticatedUser" OPC UA user role are automatically added to all other OPC UA user roles except "Anonymous".
    These permissions can only be changed for the "AuthenticatedUser" OPC UA user role. All other OPC UA user roles, except "Anonymous", show these permissions in gray and enabled.
  - Permissions that you add to the other OPC UA user roles are not added to the "Anonymous" and "AuthenticatedUser" OPC UA user roles.
- Remove permissions:
  - If you remove permissions for the "Anonymous" OPC UA user role, these permissions become subject to editing for the "AuthenticatedUser" OPC UA user role. All other OPC UA user roles show these permissions in gray and enabled.
  - If you remove permissions for the "AuthenticatedUser" OPC UA user role, these permissions become subject to editing for all other OPC UA user roles except "Anonymous".

The following figure shows an example of the permissions assigned to the OPC UA user role "AuthenticatedUser" in namespace 0 (http://opcfoundation.org/UA/). Because the permissions for browse and read access have been added to the "Anonymous" OPC UA user role, the permissions for "AuthenticatedUser" are displayed in gray and enabled. The permission for write access has also been added to the OPC UA user role "AuthenticatedUser".



Assigned default role permissions AuthenticatedUser

	Namespaces	Browse	Read	Write	Call	Receive events	Read role permissions
1	http://opcfoundation.org/UA/	☑	☑	☑	☐	☐	☐
2	urn:SIMATIC:myPLC	☐	☐	☐	☐	☐	☐
3	http://opcfoundation.org/UA/DI/	☐	☐	☐	☐	☐	☐
4	http://www.siemens.com/simatic-s7-opcua	☐	☐	☐	☐	☐	☐

11.2.8.3 How the OPC UA server evaluates permissions on nodes

The following describes how the OPC UA server evaluates a client request (session setup) and manages access depending on the assigned roles and permissions. The node attributes or properties of OPC UA objects mentioned here are set automatically by your configuration of the OPC UA access control in the TIA Portal.

Requirements

For different users you have, for example, assigned names and passwords in the local user management of the CPU.

You have defined several user roles for the OPC UA server of an S7-1500 CPU. These user roles have the "OPC UA server access" function right under "Security settings > Users and roles". The roles are assigned to different users.

The names of the roles in the project and the OPC UA user roles are mapped in the "Access control at OPC UA server" editor.

The user "Joe" is assigned the role "MaintenanceEngineer" in the project.

The "MaintenanceEngineer" role has display and read rights (Browse and Read) for the namespace of a server interface (e.g. "http://server-interface-machine1").

A client requests read access to the "HealthState" node as user "Joe" in the namespace "http://server-interface-machine1".

Example of the review process

In the following example, user "Joe" is assigned the "MaintenanceEngineer" role in the project. The "MaintenanceEngineer" role has browse and read rights for the namespace of a server interface (e.g. "http://server-interface-machine1").

A client requests read access to the "HealthState" node as user "Joe" in the namespace "http://server-interface-machine1".

The check is performed as follows:

1. Authentication: The client with the user name "Joe" logs onto the server of the S7-1500 CPU.
   The CPU authenticates Joe using his credentials (user name and password in the UserNameIdentityToken).
2. Role assignment: After successful authentication, the OPC UA server of the CPU assigns the configured "MaintenanceEngineer" role to the user "Joe".
3. Access request: As a MaintenanceEngineer, "Joe" wants to query maintenance information for a machine. This information is represented by the "HealthState" node in the "http://server-interface-machine1" namespace.
4. Verification of permission and decision: The server first checks whether the "RolePermissions" attribute is set on the "HealthState" node.
   This attribute defines the permissions that apply to a node for all roles that have access to this node.
   - If the attribute exists and the "MaintenanceEngineer" role with the "Read" permission exists in this attribute and there are no access restrictions, access is granted.
     The attribute is only set if permissions have been adapted at node level. This adapting of authorizations on the node level is currently not supported.
   - If the "RolePermissions" attribute does not exist on the node, the server uses the value of the DefaultRolePermissions property from the NamespaceMetadata object that is linked to the node.

     This property is set when permissions are assigned at the namespace level in TIA Portal.

     If the "MaintenanceEngineer" role with the "Read" permission exists in the "http://server-interface-machine1" namespace and there are no access restrictions, access is granted.
   - If none of the above conditions are met, the user "Joe" does not have access to the "HealthState" node.

Users with more than one role

In the example above, only one role is assigned to the user "Joe". If a user has more than one role, the OPC UA server checks the permissions for each role on the node. The resulting permissions result from the OR link of the role permissions.

Example: If at least one of the assigned user roles has the "Write" permission for the node, the user has write permission for this node.

11.2.8.4 Importing nodeset files with role definitions

As of STEP 7 V20, you can also import an included access control configuration when importing nodeset files.

These nodeset files are created with tools outside the TIA Portal, e.g. Siemens OPC UA Modeling Editor SiOME (https://support.industry.siemens.com/cs/ww/en/view/109755133).

Procedure: Import nodeset file with configuration for access control

To import a nodeset file with access control information (role permissions and access restrictions), proceed as follows:

1. Select the entry "OPC UA communication > Server interfaces > Add new server interface" for the desired CPU in the project navigation.
   The "Add new server interface" dialog opens.
2. Select the "Companion specification" type.
3. Select the path to the corresponding XML file.
4. Click the "OK" button.
   STEP 7 displays a warning if there are any abnormalities. Click "OK" to confirm the warning.
   You can find messages about the anomalies in the Inspector window in the "Info > General" area.

Result: You have selected the desired XML file. STEP 7 opens the "Import configuration of the access control " dialog.

Editing and importing the access control configuration

In the "Import configuration of the access control " dialog, select whether or not you want to load the access control configuration from the XML file. If you select the "Keep access control configuration" option, the configuration contained in the XML file will be imported. The dialog offers the following configuration options for the import:

- "Role permissions" tab:
  Shows the OPC UA roles contained in the XML file with the configured permissions for the respective namespaces.
  - Disable OPC UA roles that you do not want to import.
    If an OPC UA role is valid for multiple namespaces, i.e. the role also has permissions in other namespaces, this is displayed in the "OPC UA role" and "Role valid for namespace" columns.
  - You can assign roles from the project to the OPC UA roles contained directly in this dialog.
    In the "Role in project" column, you can select a role from the project in addition to the OPC UA role. Only roles that contain the "OPC UA server access" function right are available for selection.

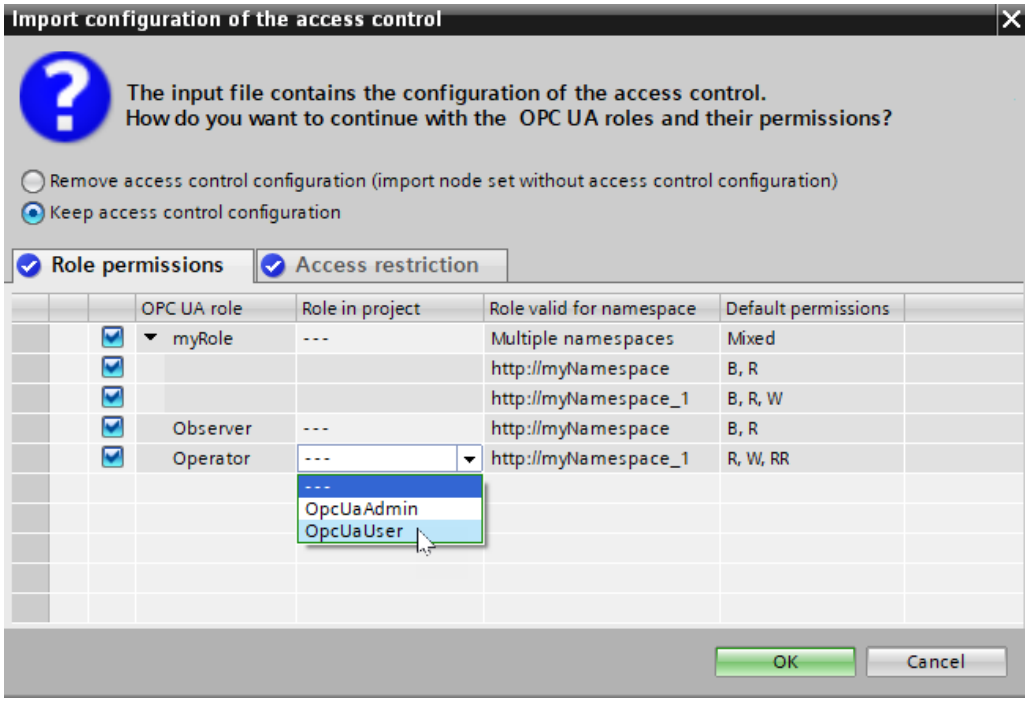


Figure 3-164 Import role permissions

- "Access restrictions" tab:
  If the project already contains namespaces of the same name with differently configured access restrictions, the "Access restrictions" tab displays a warning symbol. Click the tab to compare the access restrictions in the import file and the configured access restrictions in the project for these namespaces.
  Select the desired option for each namespace. Only the selected access restrictions then apply to this namespace after the import.

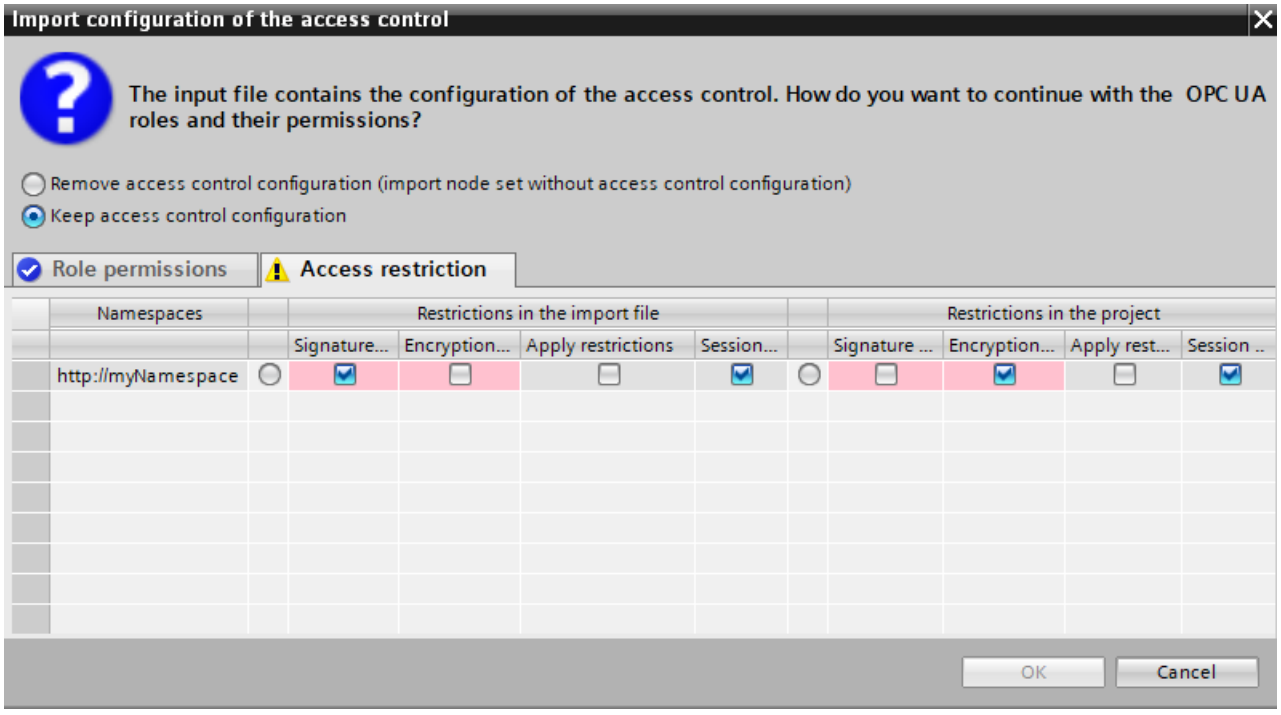


Figure 3-165 Select access restrictions

11.3 Using the S7-1500 as an OPC UA server

11.3.1 Interesting information about the OPC UA server of the S7-1500 CPUs

11.3.1.1 The OPC UA server of the S7-1500 CPUs

The S7-1500 CPUs as of firmware V2.0 are equipped with an OPC UA server. Apart from the Standard-S7-1500 CPUs this applies to the variants S7-1500F, S7-1500T, S7-1500C, S7-1500pro CPUs, ET 200SP CPUs, SIMATIC S7-1500 SW controllers and PLCSIM Advanced.

Convention: "S7-1500 CPUs" also includes the above-mentioned CPU variants.

S7-1500 CPU OPC UA server basics

Access to the OPC UA server of the CPU is possible via all integrated Ethernet interfaces of the S7-1500 CPU.

Direct access to the OPC UA server of the CPU over the backplane bus of the automation system is not possible via CPs under the following conditions:

- Configuration with TIA Portal Version V16 or higher
- S7-1500 CPU firmware version 2.8 or higher and CP 1543-1 firmware version V2.2 or higher

For configuration, see Access to OPC UA applications (Page 170).

Direct access to the OPC UA server of the CPU over the backplane bus of the automation system is not possible via CMs.

For access by clients, the server saves the enabled PLC tags and other information in the form of nodes (see Accessing OPC UA server data (Page 231)). These nodes are interconnected and form a network. OPC UA defines access points to this network (well-known nodes) that enable navigation to subordinate nodes.

With an OPC UA client you can read, observe or write values of tags of the PLC program as well as call methods that are available to the server. As of firmware version 2.5 you can implement methods, see Useful information about server methods (Page 306).

Node classes

OPC UA servers provide information in the form of nodes. A node can be, for example, an object, a tag, a method or a property.

The example below shows the address space of the OPC UA server of an S7-1500 CPU (extract from the OPC UA client "UaExpert" from Unified Automation).

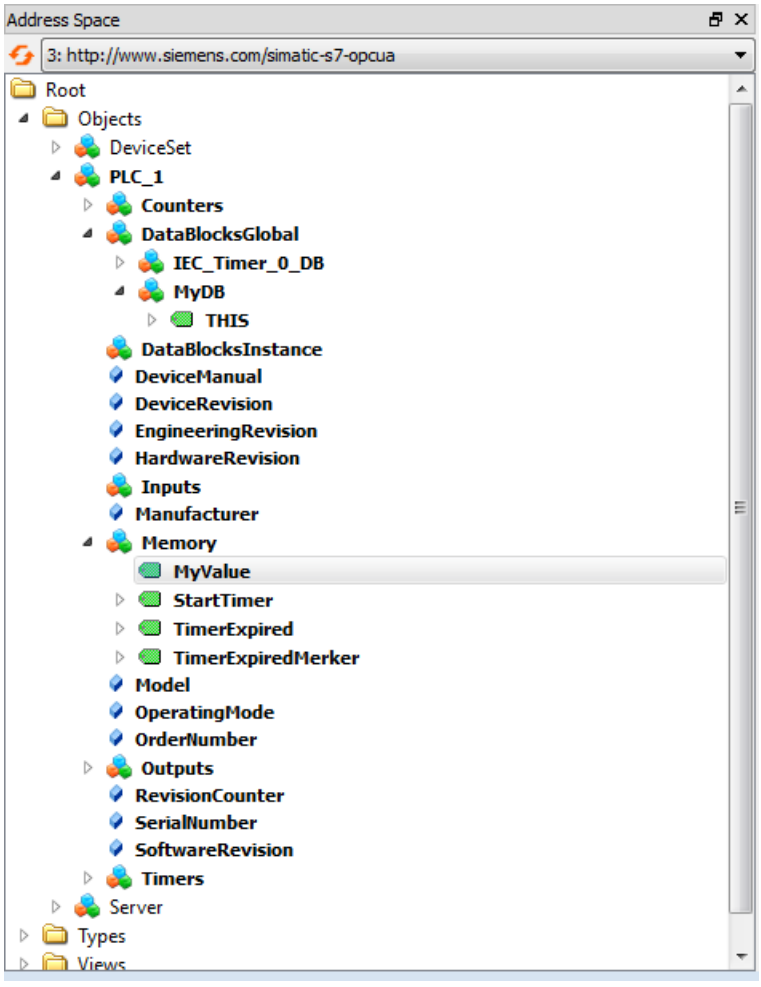


Figure 3-166 Example of the address space of the OPC UA server of an S7-1500 CPU

In the figure above, the "MyValue" tag is selected (highlighted in gray).

This tag is located below the "Memory" node, which has the node class "Object".

"Memory" is below the "PLC_1" node (also an Object).

Address space

The nodes are interconnected via references, e.g. via the "HasComponent" reference, which represents a hierarchical relationship between a node and its subordinate nodes. With their references, the nodes form a network that can, for example, take the form of a tree.

A network of nodes is also called an address space. Starting from the root, all nodes can be reached in the address space.

11.3.1.2 End points of the OPC UA server

The end points of the OPC UA server define the security level for a connection. Depending on the purpose of use or desired security level, you have to carry out the corresponding settings for the connection at the end point.

Different security settings

Before establishing a secure connection, OPC UA clients ask the server with which security settings connections are possible. The server returns a list with all the security settings (endpoints) that the server offers.

Structure of end points

End points consist of the following components:

- Identifier for OPC: "opc.tcp"
- IP address: 192.168.178.151 (in the example)
- Port number for OPC UA: 4840 (standard port)
  The port number can be configured.
- Security setting for messages (Message Security Mode): None, Sign, SignAndEncrypt.
- Encryption and hash procedures (Security Policy): None, Basic128Rsa15, Basic256, Basic256Sha256 (in the example).

The following figure shows the "UA Sample Client" of the OPC Foundation.

The client has established a secure connection to the OPC UA server of an S7-1500 CPU to the end point "opc.tcp://192.168.178.151:4840 - [SignAndEncrypt: Basic256Sha256:Binary]". The security settings "SignAndEncrypt:Basic256Sha256" are contained in the end point.

NOTE

Select an endpoint with a security policy that is as strict as possible for the server

- Only activate the most secure endpoints on the OPC UA server that a client still supports.
- Deactivate the security policy with a lower security policy on the OPC UA server.

Establishing a connection to the server (client-side)

- To establish a connection to the server, select the appropriate security policy for the application.
- Corresponding certificates are required for the activated endpoints of the OPC UA server of the CPU (e.g. a Sha256 certificate for Basic256Sha256).

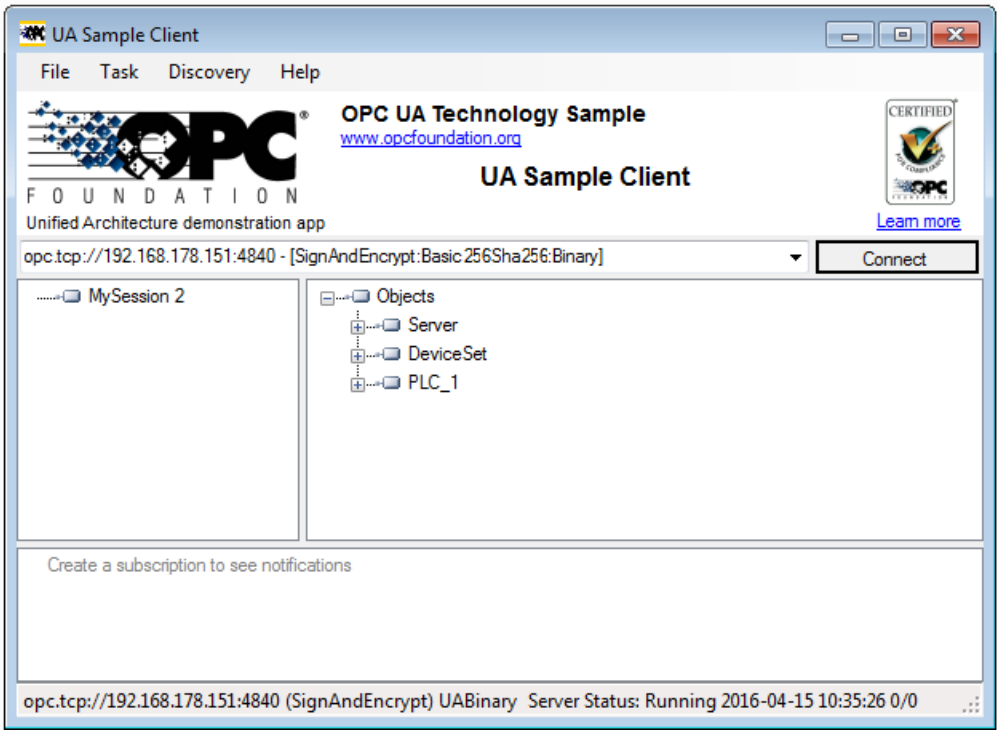


Figure 3-167 "UA Sample Client" program of the OPC Foundation

A connection to a server end point is only established if the OPC UA client complies with the security policies of that end point.

Through the information provided by the OPC UA server

OPC UA servers provide a wide range of information:

- The values of PLC tabs and DB components which clients may access.
- The data types of these PLC tags and DB components.
- Information on the OPC UA server itself and on the CPU.

This gives clients an overview and allows them to read out specific information. Previous knowledge of the PLC program and the CPU data is not required. You do not need to ask the developer of the PLC program when PLC tags are to be read. All necessary information is stored on the server itself (for example, the data types of the PLC tags).

Display of the information of the OPC UA server

You have the following options:

- Online: You have all the available information displayed during the runtime of the OPC UA server. To do so, navigate (browse) the address space of the server.
- Offline: You export an XML file that is based on the XML schemes of the OPC Foundation.
  Server methods created by the user (FB instance that can be called by an OPC UA client) are not exported as of STEP 7 V15.1, see Providing methods on the OPC UA server (Page 306).
- Offline with the Openness API: In your program, you use the API (Application Programming Interface) of the TIA Portal to access the function for exporting all PLC tags that can be read by OPC UA. This requires .NET Framework 4.0; see TIA Portal Openness, Automating SIMATIC projects with scripts (https://support.industry.siemens.com/cs/ww/en/view/109477163).
- If you already know the syntax and the PLC program, you can access the OPC UA server without first researching the information.

11.3.1.3 Mapping of data types

SIMATIC and OPC UA data types

SIMATIC data types do not always correspond with OPC UA data types.

S7-1500 CPUs provide SIMATIC tags (with SIMATIC data types) to their own OPC UA server as OPC UA data types. OPC UA clients can then access these tags with OPC UA data types via the server interface.

A client can read the attribute "DataType" from such a tag and reconstruct the original data type in SIMATIC.

Example
A tag has the SIMATIC data type "COUNTER". You read COUNTER → UInt16 in the table. You now know that you do not need to convert; the COUNTER value is sent over the line as a UInt16 data type.

The client detects from the attribute "DataType" that the tag is actually the SIMATIC data type "COUNTER". With this knowledge, the client reconstructs the data type.

Table 3-25 SIMATIC and OPC UA data types

SIMATIC data type	OPC UA data type
BOOL	Boolean
BYTE	BYTE → Byte
WORD	WORD → UInt16
DWORD	DWORD → UInt32
LWORD	LWORD → UInt64
SINT	SByte
INT	Int16
DINT	Int32
LINT	Int64

SIMATIC data type	OPC UA data type
USINT	Byte
UINT	UInt16
UDINT	UInt32
ULINT	UInt64
REAL	Float
LREAL	Double
S5TIME	S5TIME → UInt16
TIME	TIME → Int32
LTIME	LTIME → Int64
DATE	DATE → UInt16
TIME_OF_DAY (TOD)	TOD → UInt32
LTIME_OF_DAY (LTOD)	LTOD → UInt64
DATE_AND_TIME (DT)	DT → Byte[8]
LDT	DateTime
DTL Special note: You can only describe the structure completely with an OPC UA client. You have read-only access individual elements of this structure (e.g. "YEAR")	mapped as structure
CHAR	CHAR → Byte
WCHAR	WCHAR → UInt16
STRING (Code page 1252 or Windows-1252)	STRING → String
WSTRING (UCS-2; Universal Coded Character Set)	String
TIMER	TIMER → UInt16
COUNTER	COUNTER → UInt16

Arrays

A read or write job with OPC UA is always an array access, which means that it always has an index and length. A single tag is a special case of an array (index 0 and length 1). The data type is simply sent repeatedly on the line. For the tags, the "DataType" attribute indicates the basic data type. The attributes "ValueRank" and "ArrayDimensions" show whether or not you are dealing with an array and how large the array is.

Data types based on arrays

There are SIMATIC data types for which an OPC UA value is mapped to an array of bytes. An array of these data types is then mapped to a two-dimensional array.

Example: The SIMATIC data type DATE_AND_TIME (DT) is mapped on the OPC UA side to an 8-byte array (Byte[8]), see table above. When you define an array of the SIMATIC data type DATE_AND_TIME (DT), then it is considered as two-dimensional array.

This fact affects the use of system data types such as OPC_UA_NodeAdditionalInfo and OPC_UA_NodeAdditionalInfoExt, for example:

For the data types described above, you must use the system data type OPC_UA_NodeAdditionalInfoExt for multidimensional arrays instead of OPC_UA_NodeAdditionalInfo.

Structures

Structures are transferred as ExtensionObject. The S7-1500 server uses binary representation for transmission of the ExtensionObjects over the line; the individual structure elements come one after the other. At the front is the NodeId of the data type; this is used by the client to establish the structure.

For OPC UA Specification <= V1.03, a client has to read, decode and interpret the complete DataTypeDictionary for this (unless it has already learned this library offline through an XML import).

AS of OPC UA V1.04, the DataTypeDefinition attribute is available, which can be read and interpreted more quickly and easily. A client only determines the setup of the structure once, before or during the first access, and then uses this information for the duration of the session.

Special SIMATIC data types

SIMATIC data types that are not in the table above and cannot be defined as elements of a structure or PLC data type are not supported by the OPC UA client.

These are, for example, "ANY" or "POINTER" pointers, function block "Block_FB", function "Block_FC" or hardware data type "REMOTE".

The selection of an unsupported data type leads to an error message.

Additional information

More details on mapping of basic data types, arrays and structures can be found in the OPC UA Specification Part 6, "Mappings" (see OPC UA BINARY there).

What must be considered with arrays and data types DTL and LDT in the OPC UA server of a SIMATIC S7-1500? FAQ (https://support.industry.siemens.com/cs/ww/en/view/109766726)

11.3.1.4 Runtime behavior of the OPC UA server

OPC UA server in operation

The OPC UA server of the S7-1500 CPU starts when you activate the server and download the project to the CPU.

How to activate the OPC UA server is described here.

Behavior in the operating state STOP of the CPU

An activated OPC UA server remains in operation even if the CPU switches to "STOP". The OPC UA server continues to respond to requests from OPC UA clients.

Server response in detail:

- If you request the values of PLC tags, you will get what were the latest values before the CPU switched to or was set to "STOP".
- If you write values to the OPC UA server, the OPC UA server will accept those values.

  However, the CPU will not process the values because the user program is not executed in "STOP" mode.

  An OPC UA client can nonetheless read the values written at STOP from the OPC UA server of the CPU.

  During restart, the CPU overwrites the values written at STOP with the start of the PLC tags.
- If you call a server method, the error message 16#00AF_0000 (BadInvalidState) is output because the server method (user program) is not running.
- Connections to the OPC UA server remain active during an operating mode transition (STOP > RUN or RUN > STOP). Exception: OPC UA-relevant data is loaded, see next section.

Download to the CPU may affect OPC UA server

If you load a CPU with running OPC UA server, you may need to stop and restart the server depending on the loaded objects. In this case, active connections are interrupted and must be re-established once the server restarts.

The duration of the restart depends mainly on the following parameters:

- The scope of the data structure
- The number of variables visible in the OPC UA address space
- The setting for downward compatible data type definition according to OPC UA specification to V1.03 (TypeDictionary enabled)
- Settings for the communication load and minimum cycle time, you can find additional information here (Page 380)

With CPU FW versions older than V2.8, the OPC UA server was stopped at each download to the CPU and then restarted.

As of FW version V2.8, the behavior of the OPC UA server has been optimized as follows:

- When objects are downloaded in STOP operating state of the CPU, the OPC UA server still always stops and then restarts. STEP 7 does not show a warning in this case.

- When objects are downloaded in RUN operating state of the CPU, the OPC UA server only stops if the downloaded objects are, or could be, OPC UA-relevant. The OPC UA server restarts after re-initialization due to the modified OPC UA data.

  Before OPC-UA-relevant objects are loaded into the CPU and stop the OPC UA server, STEP 7 displays a warning in the preview dialog for loading. You can then decide whether a server restart is compatible for the running process or whether you want to cancel the download. These warnings are only displayed when the OPC UA server is running. If the OPC UA server is not enabled, modified OPC UA data have no influence on the download process.

Examples

- You only want to add another code module to the program.
  Neither data blocks nor inputs, outputs, flags, times or counters are affected.
  Reaction during loading: A running OPC UA server is not interrupted.
- You want to load a new data module and you have flagged the data module as non-OPC-UA-relevant:
  Reaction during loading: A running OPC UA server is not interrupted.
- You want to overwrite a data module.
  Reaction during loading: A warning appears that the server will be restarted.
  Background: STEP 7 cannot determine whether the changes refer to OPC-UA-relevant data or not.

Reading CPU operating mode over OPC UA server

The OPC UA server allows you to read out the CPU mode, see figure below:

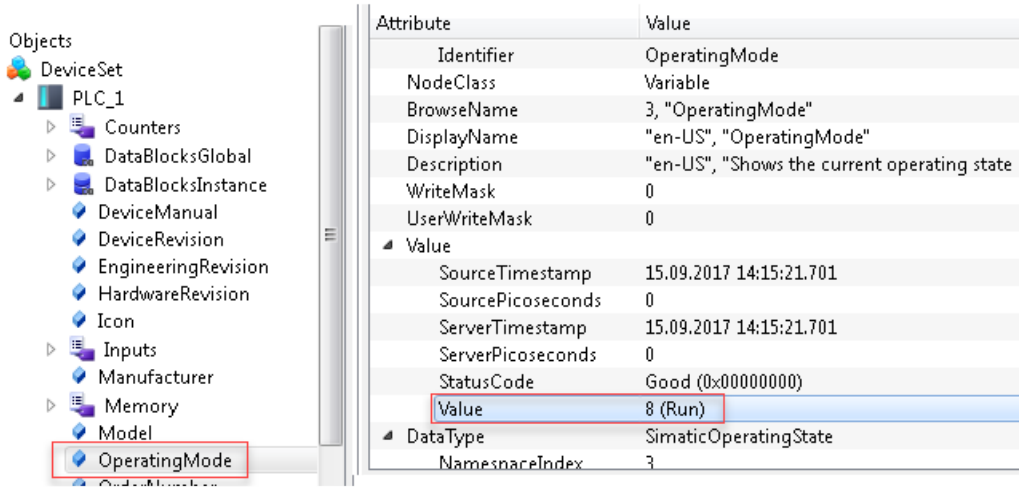


Figure 3-168 Reading CPU operating mode over OPC UA server

In addition to the operating mode of the CPU, you can also read out information about the manual (DeviceManual) or the hardware version (HardwareRevision), for example.

11.3.2 Accessing OPC UA server data

11.3.2.1 Client accesses and local accesses to the OPC UA server

An OPC UA server provides a lot of information for OPC UA clients within a network. The following section describes options for making CPU tags (PLC tags and DB elements) available in the address space of your own OPC UA server.

Provide CPU tags via server interfaces in the OPC UA address space

The easiest way to transfer CPU tags automatically into the address space of the OPC UA server:

- Activate the standard SIMATIC server interface in the OPC UA properties of the CPU.
  All CPU tags released for OPC UA are then automatically also available in the OPC UA address space under the name of the CPU.

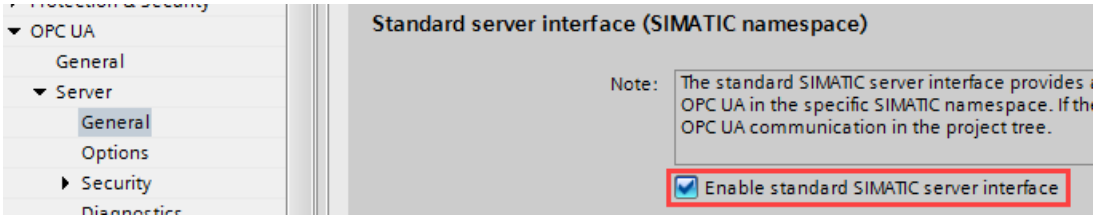


Figure 3-169 Standard SIMATIC server interface of the OPC UA server

The use of OPC UA server interfaces is more flexible and clearer because you configure the server interfaces in the project tree (below the CPU, "OPC UA Communication" folder). User-defined OPC UA server interfaces allow you to easily map OPC UA tags and CPU tags (local data).

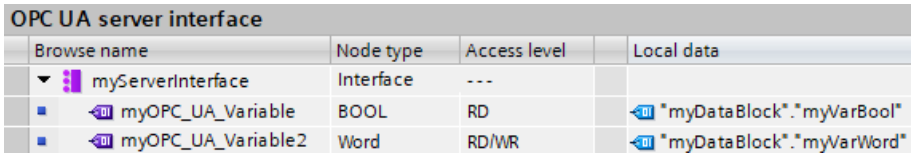


Figure 3-170 Creating a user-defined server interface with mapped CPU tags

The data exchange between OPC UA client and OPC UA server is clearly illustrated in the following example of two S7-1500 CPUs.

Here, an S7-1500 CPU as client writes values to an OPC UA tag of the OPC UA server. The mapping between CPU variable and OPC UA tag makes it look as though the OPC UA client writes a value directly into the CPU variable. For an S7-1500 client CPU, use the "OPC_UA_WriteList" instruction in conjunction with additionally required instructions for the data exchange.

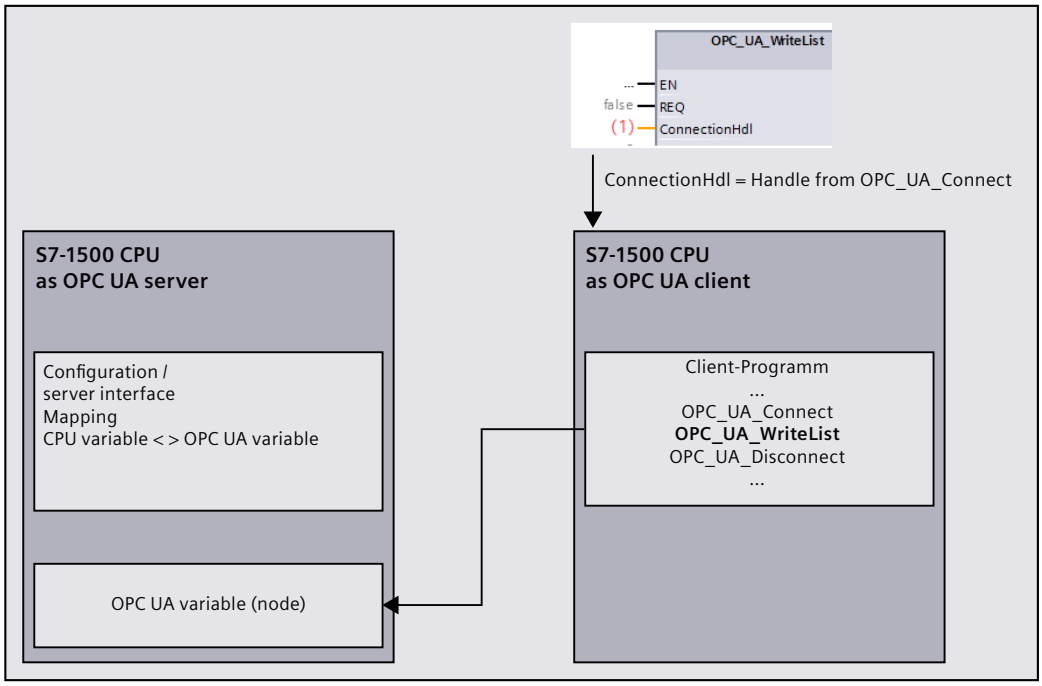


Figure 3-171 Client access to the server's OPC UA tag

Writing CPU tag values directly to OPC UA tags (set OPC UA DataValue)

From firmware version V3.0, S7-1500 CPUs also offer the option of writing values directly to local OPC UA variable nodes on the server using the "OPC_UA_WriteList" instruction in addition to mapping tags. Normally, the "OPC_UA_WriteList" instruction in the client program of the CPU is used to write values to OPC UA tags of a remote OPC UA server.

Advantage of using "OPC_UA_WriteList" in the server: In addition to the value, you can provide the OPC UA tag node with the following additional information:

- SourceTimestamp
- StatusCode

OPC UA provides a built-in "DataValue" data type. DataValue is a structure that records both the Value as well as the SourceTimestamp and StatusCode as additional information for the value. The DataValue structure is only used by OPC UA services and you cannot write directly in the program of the CPU to the elements of this structure. Write access is only possible via a special use of the "OPC_UA_WriteList" instruction.

Application options

CPU variables cannot record a time stamp indicating when a value was last written to the CPU variable. If you map CPU tags and OPC UA tags via server interfaces, the OPC UA server does not therefore set the SourceTimestamp to the time when the CPU tag changed, but to the time when the value was "collected" in the server, such as by a read service or by sampling in the context of a subscription.

If you write DataValue directly with "OPC_UA_WriteList" to an OPC UA tag node, for example, you can provide a time stamp determined in the program as the SourceTimestamp for the value.

Principle functionality of the "OPC_UA_WriteList" instruction for setting DataValues

The DataValue structure is, for example, modeled as a UDT and a tag of this data type is transferred to the "OPC_UA_WriteList" instruction. The instruction then consistently transfers the elements of the tag to the OPC UA tag node.

The value of the "ConnectionHdl" instruction parameter determines the function of the "OPC_UA_WriteList" instruction: Either "Normal" client instruction or instruction to write to local OPC UA tag nodes. OPC UA clients can read the value with additional information in the latter case and evaluate it accordingly.

This principle is illustrated in the following figures, once with any client and once with an S7-1500 CPU as OPC UA client. In the case of the S7-1500 CPU client, the assignment of the DataValue elements to the corresponding instruction parameters of the "OPC_UA_ReadList" instruction is shown. You have full access to all elements of the DataValue structure.

The value of "Read" (-42) of the "OPC_UA_WriteList" instruction causes the server to write to local OPC UA tag nodes.

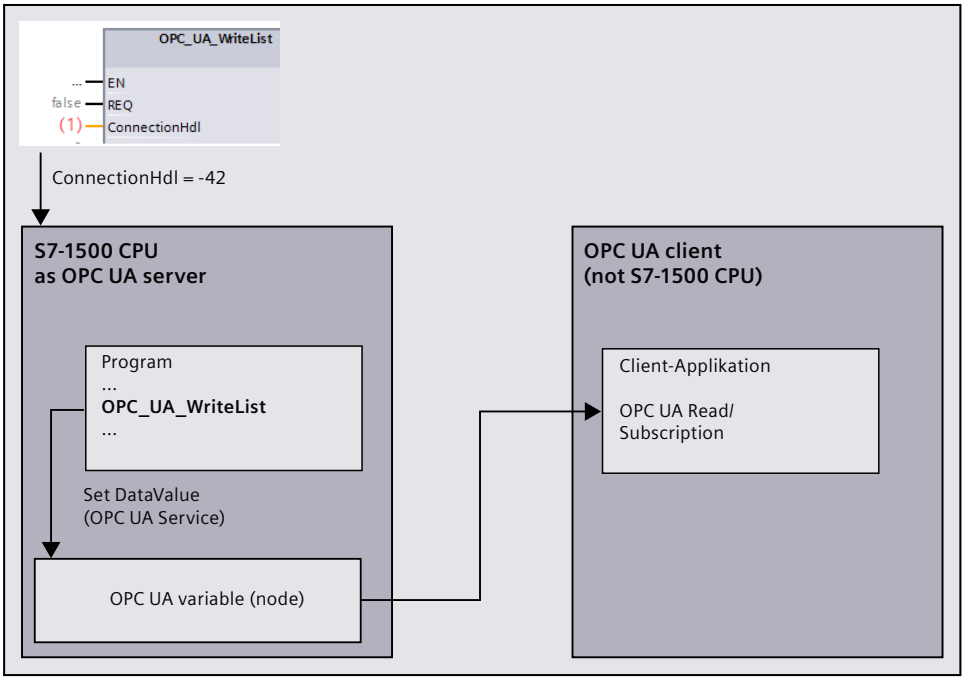


Figure 3-172 Set data value on local OPC UA tag of the server

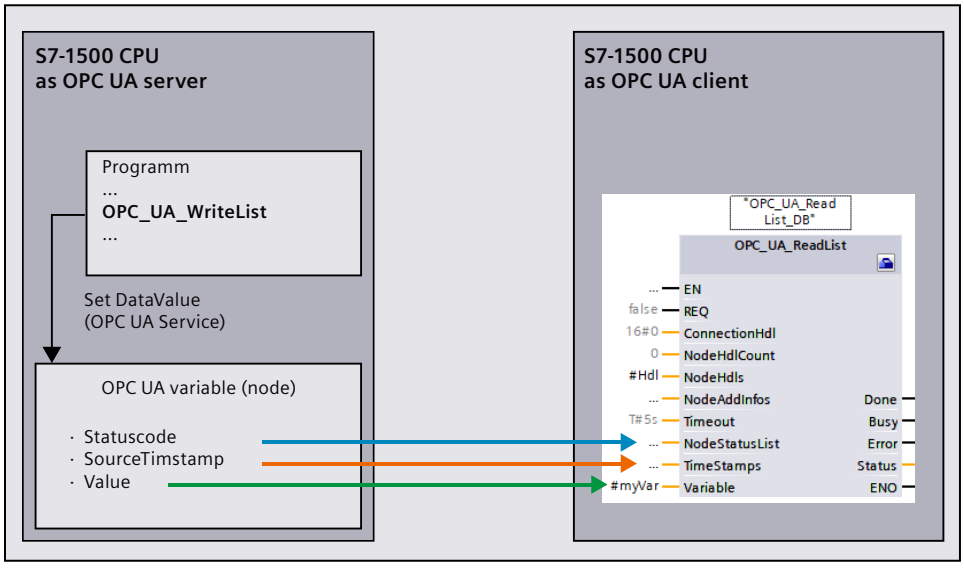


Figure 3-173 Client reads data value (OPC UA tag of the server of the S7-1500 CPU)

Other application options

If OPC UA clients log on with an S7-1500 CPU for value changes (monitored items) in the context of a subscription and you supply the corresponding DataValue with both the value and the additional information mentioned above, then changes to the additional information can also trigger a notification.

Example: A binary value changes so fast that it falls back to its original value in the sampling interval (fast change TRUE > FALSE > TRUE). A change of the value is not detected. But the change of the time stamp is detected. Similarly, a notification can be triggered when the StatusCode changes - even without the value changing.

Constraints

- OPC UA clients are only allowed to read the OPC UA tag; the "AccessLevel" attribute for read/write permissions must be set accordingly for the OPC UA tag.
- Only OPC UA tags of the user-defined server interfaces can be set locally.
- In the user-defined server interface, there must be no mapping to CPU tags for the directly written OPC UA tags.

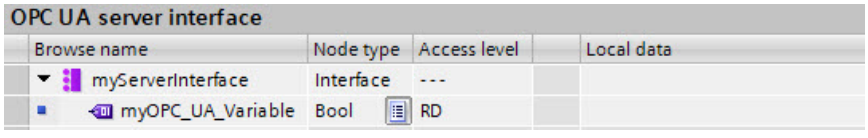


Figure 3-174 User-defined server interface

Details on how to use the "OPC_UA_WriteList" instruction in the "Set OPC UA DataValue" context can be found in the corresponding section of the communication instruction help.

Setting OPC UA DataValue attributes for arrays and structures

When OPC UA tags of type structure or array are set using "OPC_UA_WriteList" for setting OPC UA DataValue attributes, all elements of this structure or array are filled.

You should not model individual elements of structures or arrays additionally as lower-level OPC UA tags.
Reason: If you model individual elements of arrays or structures additionally as separate lower-level nodes in the address space of the server, then these nodes are **not** automatically filled. For the OPC UA server, these separate nodes are independent of the higher-level OPC UA tags of the structure or array type, because they are not mapped to CPU tags.

To fill these separately modeled nodes, you must create each individual element as its own DataValue structure in the program.

Tip: In order for OPC UA clients to be able to simultaneously learn about changes to relevant nodes in this case, set the values of all OPC UA tags involved in the same "OPC_UA_WriteList" call.

More information

An application example (https://support.industry.siemens.com/cs/us/en/view/109820694) is provided to assist you on the topic of "Setting OPC UA DataValue attributes".

You can find information on how to coordinate read and write permissions for CPU-tags in the Coordinating read and write permissions for CPU tags (Page 239) section.

You can find information how to create user-defined server interfaces in the Creating a user-defined server interface (Page 283) section.

11.3.2.2 Managing write and read rights

Enabling PLC tags and DB tags for OPC UA

OPC UA clients can have read and write access to PLC tags and DB tags if the tags are enabled for OPC UA (default setting). For an enabled tag the check box "Accessible from HMI/OPC UA" is activated.

You can change the default setting in the settings of the TIA Portal: Command "Settings > PLC programming > General" in "Options" menu. You will find the corresponding options in the "Block interface/data block elements" area.

The following example shows an array data block:

MyDB

Name	Data type	Accessible from HMI/OPC UA	Writable from HMI/OPC UA	Visible in HMI engineering
MyDB	Array[0..9] o...	☑	☑	☑
MyDB[0]	Int	☑	☑	☑
MyDB[1]	Int	☑	☑	☑
MyDB[2]	Int	☑	☑	☑
MyDB[3]	Int	☑	☑	☑
MyDB[4]	Int	☑	☑	☑
MyDB[5]	Int	☑	☑	☑
MyDB[6]	Int	☑	☑	☑
MyDB[7]	Int	☑	☑	☑
MyDB[8]	Int	☑	☑	☑
MyDB[9]	Int	☑	☑	☑

Figure 3-175 Enabling PLC tags and DB tags for OPC UA tags

This array can be read completely in one pass by OPC UA clients (see Addressing nodes (Page 174)). The check boxes at "Accessible from HMI/OPC UA" and "Writable from HMI/OPC UA" are activated for all the components of the array.

Result: OPC UA clients can both read and write these components.

Removing write rights

If you want to write-protect a tag, deselect the "Writable from HMI/OPC UA" option for that tag. This removes the write right for the OPC UA clients and HMI devices.

Result: Only read access by OPC UA clients and HMI devices is possible. OPC UA clients cannot assign values to this tag and therefore cannot influence execution of the S7 program.

Removing write and read rights

To write-protect and read-protect a tag, disable the "Accessible from HMI/OPC UA" option for that tag (checkbox not selected). This makes the OPC UA server remove the tag from its address space. OPC UA clients can no longer see that CPU tag.

Result: OPC UA clients and HMI devices can neither read nor write the tag.

Write and read rights of structures

If you remove the read or write right for the component of a structure, the structure or the data block cannot be written or read as a whole.

If you remove read and write rights for individual components of a PLC data type (UDT), the rights will also be removed from any data block based on that data type!

Visible in HMI engineering

The option "Visible in HMI Engineering" applies to Siemens engineering tools. If you disable the option "Visible in HMI Engineering" (check mark not set), you can no longer configure the tag in WinCC (TIA Portal).

The option does not have any effect on OPC UA.

Rules

- Only allow read access to PLC tags and tags of data blocks in STEP 7 if this is necessary for communication with other systems (controllers, embedded systems or MES).

  You should not enable other PLC tags.
- Only allow write access over OPC UA if write rights are genuinely necessary for specific PLC tags and tags of data blocks.
- If you have reset the "Accessible from HMI/OPC UA" option for all elements of a data block, the data block for an OPC UA client is no longer visible in the address space of the OPC UA server of the S7-1500 CPU.
- You can also prevent access to an entire data block centrally (see Managing write and read rights for a complete DB (Page 237)). This setting "overrules" the settings for the components in the DB editor.

More information

For information on how to coordinate write and read rights for CPU tags, refer to the section Coordinating write and read rights for CPU tags (Page 239).

11.3.2.3 Managing write and read rights for a complete DB

Hiding DBs or DB contents for OPC UA clients

You can easily prevent access to a complete data block by an OPC UA client.

With this option, the data of the corresponding DB, including instance DBs of function blocks, remains hidden for OPC UA clients.

In the default setting, data blocks can be read and written from OPC UA clients. You can change this default setting in the settings of the TIA Portal: Command "Settings > PLC programming > General" in "Options" menu. You will find the corresponding option in the "Default settings for new blocks" area.

Procedure

Proceed as follows to completely hide a data block for OPC UA clients or to protect a data block from write access from OPC UA clients:

1. Select the data block to be protected in the project tree.
2. Select the "Properties" shortcut menu.
3. Select the "Attributes" area.

4. Select/clear the "DB accessible from OPC UA" checkbox as required.

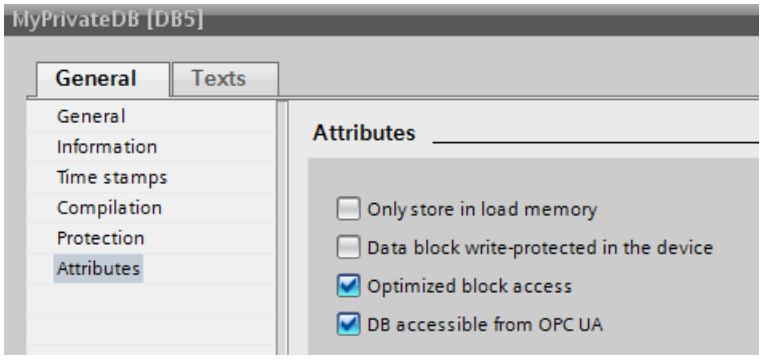


Figure 3-176 Hiding DBs or DB contents for OPC UA clients

NOTE

Effect on settings in the DB editor

If you hide a DB using the DB attribute described here, the settings for the components in the DB editor are no longer relevant; individual components can no longer be accessed or written.

Tip: Using the overview of all program blocks

If you are using multiple data blocks, it is appropriate to use the detailed overview of the "Program blocks" folder for selective activation or deactivation of the OPC UA accessibility.

Follow these steps:

1. Select the "Program blocks" folder in the project tree.
2. Select the "Overview" command in the "View" menu.
3. Select the "Details" tab.
   An overview of the blocks with their attributes is displayed.
4. Ensure that the "Data block accessible via OPC UA" column is selected.
5. Select only the data blocks that are to be accessible via OPC UA.

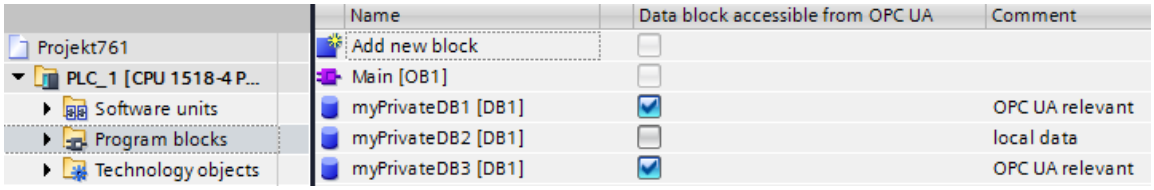


Figure 3-177 Overview of the program blocks

11.3.2.4 Coordinating write and read rights for CPU tags

Definition of write and read rights in the information model (OPC UA XML)

In the OPC UA information model, the attribute "AccessLevel" regulates access to tags.

AccessLevel is defined bit by bit:

Bit 0 = CurrentRead and Bit 1 = CurrentWrite. The meaning of the bit combinations is as follows:

- AccessLevel = 0: no access
- AccessLevel = 1: read only
- AccessLevel = 2: write only
- AccessLevel = 3: read+write

Example of the assignment of write and read rights (read+write)

```
<UAVariable NodeId="ns=3;s=&quot;Data_block_2&quot;.&quot;Static_1&quot;"
BrowseName="3:Static_1"
ParentNodeId="ns=3;s=&quot;Data_block_2&quot;"
DataType="INT"
AccessLevel="3">
    <DisplayName>Static_1</DisplayName>
```

Definition of write and read rights in STEP 7

When you define tags, you specify the access rights using the properties "Accessible from HMI/OPC UA" and "Writable from HMI/OPC UA".

Example of the assignment of write and read rights

Name	Data type	Accessible from HMI/OPC UA	Writable from HMI/OPC UA
Static_1	Int	☑	☑
<Add new>		☑	☑

Figure 3-178 Example of the assignment of write and read rights

Interaction between write and read rights

If you have imported an OPC UA server interface and AccessLevel attributes are set in this OPC UA XML file, the write and read rights are defined by the following rule: The least extensive access rights for each setting apply.

Example

- AccessLevel = 1 (read only) in the OPC UA server interface
- Both "Accessible from HMI/OPC UA" and "Writable from HMI/OPC UA" are selected in the PLC tag table

Result: This tag can only be read.

Rules

If write rights are required:

- AccessLevel = 2 oder 3
- "Writable from HMI/OPC UA" enabled

If read rights are required:

- AccessLevel = 1 (AccessLevel 3 is also possible, but misleading. The settings suggests that an OPC UA client has write and read rights)
- "Accessible from HMI/OPC UA" enabled, "Writable from HMI/OPC UA" disabled

If neither read nor write rights are to be granted (no access):

- AccessLevel = 0
- "Accessible from HMI/OPC UA" disabled

  Only one of the two conditions needs to be met to block all access. In this case, review whether the tag in the OPC UA server interface is actually necessary at all.

Access table

"Accessible from HMI/OPC UA" must be set if access over OPC UA is to be possible at all. "Writable from HMI/OPC UA" must be set to allow an OPC UA client to write a tag / DB element.

Please see the table for the resulting access right.

Table 3-26 Access table

OPC UA XML	**STEP 7 (TIA Portal), for example tag table**		
AccessLevel	**Accessible from HMI/OPC UA**	**Writable from HMI/OPC UA**	**Resulting access right**
0	x	x	No access
x	0	x	No access
1	Enabled	x	Read only
2	Enabled	Disabled	No access
3	Enabled	Disabled	Read only
2	Enabled	Enabled	Write only
3	Enabled	Enabled	Read+write

(x = don't care)

11.3.2.5 Consistency of CPU tags

"AccessLevelEx" attribute extends access properties

As of firmware version V2.6, the OPC UA server of the S7-1500 CPU supports not only the attribute "AccessLevel" (see Coordinating write and read rights for CPU tags (Page 239)) but also the attribute "AccessLevelEx" which, in addition to the already explained bits for read access and write access, provides information on the consistency of a OPC UA tag. The new attribute was introduced with version V1.04 of the OPC UA specification (Part 3, Address Space Model).

Reading consistency properties

In the OPC UA information model of the OPC UA server, the attribute "AccessLevel" defines the access.

AccessLevelEx is defined bit by bit; in this case the relevant bits are:

- Bit 0 = CurrentRead
- Bit 1 = CurrentWrite
- Bits 2 to 7 are not relevant for the OPC UA server of an S7-1500 CPU

The meaning of the bit combinations is explained in the section on read and write rights.

The following bits for consistency are also added:

- Bit 8 = NonatomicRead; the bit is set if the tag cannot be read consistently. For read consistency of tags, bit 8=0.
- Bit 9 = NonatomicWrite; is set if the tag cannot be written consistently. For write consistency of tags, or if no write access is granted, bit 9=0.

Examples

An OPC UA tag (structure) is readable and writable; but inconsistent for reading and writing access.

Consequently: Bits 0, 1, 8 and 9 are set: AccessLevelEx = "771" (1+2+256+512).

Another structure is read-only.

Consequently: Bits 0 and 8 are set, bit 1 and bit 9 are not set: AccessLevelEx = "257" (1+0+256+0).

Handling of the attribute in the server

The "AccessLevelEx" attribute is only available in the OPC UA server. The attribute is not present in a node set file (XML export file).

However, the attribute "AccessLevel", which is exported, includes the information from "AccessLevelEx", see next section.

Export

During XML export of the standard SIMATIC server interface, the server sets the "AccessLevel" attribute, which was expanded to 32 bits in V1.04 compared to V1.03, to the value of the "AccessLevelEx" attribute.

Import
When importing a node set file (e.g. from an export of a server interface), the S7-1500 CPU sets the attribute "AccessLevelEx" according to its own estimate of the consistency of the imported data type, see next section. The imported value is ignored.

Consistency of data types at the server interface

The consistency of tags ("atomicity" in the language usage of OPC UA) within a program cycle of an S7-1500 CPU is ensured at the nodes of the server interface for the following data types:

- BOOL, BYTE, WORD, DWORD, LWORD
- SINT, INT, LINT, DINT, USINT, UINT, ULINT, UDINT
- REAL, LREAL
- DATE, LDT, TIME, LTIME, TIME_OF_DAY, LTIME_OF_DAY, S5TIME
- CHAR, WCHAR
- System data types and hardware data types that are based on the above-mentioned data types are also consistent.
  Example: HW_ANY, derived from UINT (UInt16).

Tip: If you browse in the address space of the S7-1500 CPU (e.g. with the OPC UA Client UaExpert), you can find the consistent data types under Types > BaseDataType > Enumeration/Number/String.

Tags of the following data types are **not** consistent (in the language usage of OPC UA: "nonatomic"):

- SIMATIC structures are generally not consistent. This means that all tags which, for example, have unknown structures or a UDT data type are not consistent.
- System data types such as DTL, IEC_Counter, IEC_TIMER, etc. are data types that are derived from structures.
- Strings (Array of Char) are not consistent.

Tip: If you browse in the address space of the S7-1500 CPU (e.g. with the OPC UA Client UaExpert), you can find data types based on structures under Types > BaseDataType > Structure.

11.3.2.6 Write accesses to OPC UA variables from S7-1500 Motion Control.

In addition to the consistency of the data types, the CPU examines the variables of the technology objects for plausibility and validity.

If an OPC UA client writes an invalid or implausible value to a variable, the original value is retained in the variable of the technology object.

Despite an unsuccessful write access, the status "Good" is output.

Example 1

Interpolation type of the cyclic cam

The variable "Cam_1".InterpolationSettings.InterpolationMode is of type INT, but may only assume the values 1...2.

If you want to change the variable using OPC UA to an invalid value, for example, 3, then the status code "Good" is output, but the variable is not changed.

Example 2

Position the software limit switch at a positioning axis

The position of the positive HW limit switch must be more positive than the position of the negative SW limit switch.

"PosAxis_1".PositionLimits_SW.MaxPosition > "PosAxis_1".PositionLimits_SW.MinPosition

If you want to change the variable using OPC UA to a value that does not meet this condition, then the status code "Good" is output, but the variable is not changed.

Which values are valid for variables of the technology objects can be looked up in the documentation of the technology objects (https://support.industry.siemens.com/cs/ww/en/view/109751049).

11.3.2.7 Accessing OPC UA server data

High performance in line with application

OPC UA is designed for the transfer of a high volume of data within a short period of time. You can increase the performance significantly if you do not access individual PLC tags, but rather read and write arrays and structures as a whole.

It is fastest to access arrays. Therefore, you should combine the data for OPC UA clients into arrays.

Recommendations for access to the OPC UA server by the OPC UA client

- For one-off or infrequent data access, use standard read/write access.
- For cyclic access to small amounts of data (up to ca. every 5 seconds), use subscriptions.
  Optimize the settings for the smallest publishing interval and the smallest sampling interval at the OPC UA server.
- If you access specific tags regularly (recurring access), you should use the functions "RegisteredRead" and "RegisteredWrite".

Allow a greater communication load for the PLC by increasing the value for "Cycle load due to communication". Make sure that your application still works properly with the changed settings.

Procedure for creating an array DB

You can create arrays for example in global data blocks, in the instance data block of a function block or as an array DB . The following sections describe how to create an Array-DB.

To create a data block with an array (array data block), follow these steps:

1. Select the CPU with the OPC UA server in the project tree.
2. Double-click "Program blocks".
3. Double-click "Add new block".
4. Click "Data block".
5. Select a unique name for the data block and accept the name that is already entered.
6. Select the "Array DB" entry from the drop-down list for "Type".
7. Select the data type for the individual components of the array from the drop-down list for "Array data type".

8. Enter the high limit of the array for "Array limit".
9. Click "OK".

11.3.2.8 MinimumSamplingInterval attribute

MinimumSamplingInterval attribute of tags

In addition to "Value", "DataType" and "AccessLevel", you can also set the "MinimumSamplingInterval" attribute for a tag in the XML file that represents the server address space.

The attribute specifies how fast the server can sample the tag value.

The OPC UA server of the S7-1500 CPU handles the values for MinimumSamplingInterval as follows:

- Negative values and values greater than 4294967 are set to -1; this means: The minimum sampling rate is indeterminate. The server does not specify how fast the tag value can be sampled.
- Decimal numbers are rounded to three decimal places.

11.3.2.9 Export OPC UA XML file

Generating an OPC UA export file

The OPC Foundation has specified a standard XML-based format for describing information models. It allows the information model of an OPC UA server to be provided to a client in advance, or information models can be downloaded to an OPC UA server. A file in this format is called a node set file because it describes an information model as a set of nodes.

With STEP 7 (TIA Portal), you can easily export the standard SIMATIC information model of the S7-1500 CPU as a server to an OPC UA XML file (node set file); including the following elements that you have enabled for OPC UA:

- CPU variables (PLC tags and DB elements)
- Function blocks with their inputs/outputs

Elements that exist in the CPU but are not used in the program do not appear in the OPC UA XML file after the export. Examples of such unused elements are:

- UDTs that are not mapped to a data block
- Function blocks with inputs/outputs without assigning inputs/outputs to CPU tags

You use the OPC UA XML file for the offline configuration of an OPC UA client; it is structured according to the OPC UA specification and acts as a standard SIMATIC server interface.

To create and export the OPC UA XML file, follow these steps:

1. Select the CPU. Click on the CPU symbol (for example in the network view).
2. Click "General > OPC UA > Server > Export" in the properties of the CPU.
3. Click "Export OPC UA XML file".
4. Select the directory in which you want to save the export file.
5. Select a new name for the file or keep the name that is already entered.
6. Click "Save".

NOTE
As of STEP 7 (TIA Portal) V15.1, server methods are contained in the OPC UA export file (node set) together with their input and output parameters.

Exporting all array elements separately

If the "Export all array elements as separate nodes" option is selected in the CPU properties under "OPC UA > Server > Export", the OPC UA XML file contains all elements of arrays as individual XML elements. In addition, the arrays themselves are each described in an XML element in the XML file.

If an array contains many array elements, the XML file can be very large.

Tip

The following FAQ contains a converter with which you can convert the export file into CSV format. You then obtain a list of the tags of the CPU that can be accessed by OPC UA.

You can find the FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742903).

11.3.3 Configuring the OPC UA server

11.3.3.1 Enabling the OPC UA server

Requirement

- If you use **certificates** for secured communication, e.g. HTTPS, Secure OUC, OPC UA, make sure that the modules involved have the **current time of day and the current date**. Otherwise, the modules evaluate the used certificates as invalid and secure communication does not work.
- You have acquired a runtime license for the operation of the OPC UA functions, see License for OPC UA (Page 269).
- If access control is enabled and you are using user management (local or central): The users must have the "OPC UA server access" function right.
  You can find information on the assignment of the "OPC UA server access" function right in the Siemens Industry Online Support under the following entry ID: SIOS Entry ID 109954947 (https://support.industry.siemens.com/cs/us/en/view/109954947)

Commissioning an OPC UA server

By default, the OPC UA server of the CPU is not enabled for reasons of security: OPC UA clients have neither write nor read access to the S7-1500 CPU.

Follow these steps to activate the OPC UA server of the CPU:

1. Select the CPU in STEP 7. To do this, click the CPU symbol in the device or network view of STEP 7.
2. In the CPU properties, navigate to "OPC UA > Server".
3. Activate the OPC UA server of the CPU.
4. Confirm the security notes.
5. In the CPU properties, navigate to the "Runtime licenses" area and set the purchased Runtime license for the OPC UA server.
6. Compile the project.
7. Download the project to the CPU.
   The OPC UA server of CPU now starts.

Settings remain stored

If you have already enabled the server and made settings, those settings are not lost if the server is disabled. The settings are saved as before and are available when you enable the server again.

Application name

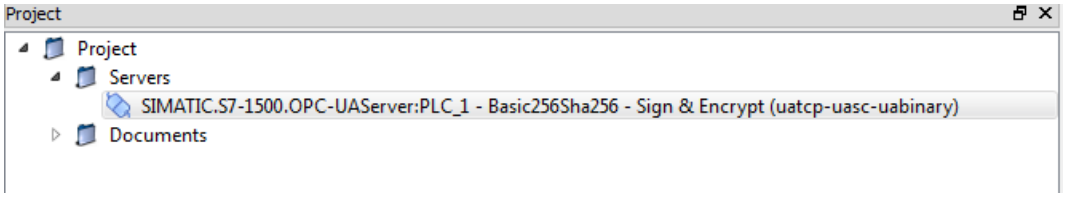
The application name is the name of the OPC UA application and applies to the server and the client. The name is displayed as follows under "OPC UA > General":

- Up to STEP 7 V20:
  - The default setting is made up of "SIMATIC.S7-1500.OPC-UA.Application:" and the name of the CPU as assigned under "General > Project information > Name".
  - If, for example, the name "PLC_1" has been assigned to the CPU, the default setting for the application name is: "SIMATIC.S7-1500.OPC-UA.Application:PLC_1".
- As of STEP 7 V21 and a CPU as of FW version V4.1:
  - The default setting for the application name is the name of the CPU as assigned under "General > Project information > Name", e.g. "PLC_1".
- The OPC UA server uses this application name to identify itself to a communication partner (OPC UA client), for example, when an OPC UA client uses the discovery service to detect accessible servers.
- The displayed application name uses the OPC UA client of the CPU to establish a connection to an OPC UA server. This means that the CPU automatically carries this application name as "ApplicationName" for the "OPC_UA_Connect" instruction ("OPC_UA_SessionConnectInfo" type variable at the "SessionConnectInfo" parameter of "OPC_UA_Connect").

  When you program the instruction "OPC_UA_Connect" you must therefore assign an empty string to the "ApplicationName". You can use the application name, for example, to identify the client with its sessions (SessionNames) for diagnostic purposes.

If you have activated the server, you can also use a different name that is meaningful in your project and that fulfills the requirements of your project, e.g. for worldwide uniqueness. The application name is also used for the server name. If you change the application name, the changes are automatically applied to the server name. Changes to the server name by the user are not possible.

The example below originates from UaExpert:



Application URI

The application URI is the unique identifier of the application and applies to the server. The structure of an application URI must comply with the syntactic rules specified for it. In STEP 7 from V21, CPUs as of FW version V4.1 are appended to the prefix "urn:" and the namespace identifier "SIMATIC:" is followed by the application name, e.g. "PLC_1". The application URI generated in this case is: "urn:SIMATIC:PLC_1". Special characters in the application name are encoded using the syntactic rules when the application URI is generated.
You can find information on the application name and the generated application URI in the CPU properties under "OPC UA > General".

The application URI is also used for the server URI. If you change the applications URI, the changes are automatically applied to the server URI. Changes to the server URI by the user are not possible. The server URI designates the namespace for the server and is located in the NamespaceArray under the fixed index 1. The client URIs are also derived from the server URI.

The server URI is also entered in the certificate (Subject Alternative Name). If the server URI changes, you must create a previously created certificate again so that the certificate contains the correct server URI.

Dependencies for name changes

In the basic settings, the following dependencies apply between the assigned CPU name, application name and application URI:

- The assigned CPU name is adopted as the application name.
- The application URI contains the application name that was taken from the assigned CPU name.
- If you change the CPU name, the changes are applied to the application name and consequently to the application URI.

If you change the application name or the application URI manually, the dependencies mentioned above will be lost. The changes have the following effect:

- Changes to the application name:
  - The application URI is regenerated with the changed application name.
  - The assigned CPU name remains unchanged.
  - Changes to the CPU name are no longer applied to the application name and therefore to the application URI.
- Changes to the application URI:
  - Changes to the application name are no longer applied to the application URI.

To restore the basic settings for the application name or URI text boxes, proceed as follows:

1. Select the CPU in STEP 7. To do this, click the CPU symbol in the device or network view of STEP 7.
2. In the CPU properties, navigate to "OPC UA > General".
3. Remove the entry in the "Application name" or "Application URI" field. Depending on which dependency you want to restore.
4. Confirm with the Enter key.
5. Optional: Repeat steps 3 and 4 to re-establish another dependency.

Result: You have restored the dependency or dependencies from the basic settings.

11.3.3.2 Access to the OPC UA server

Server addresses

The OPC UA server of the S7-1500 CPU can be reached over all integrated PROFINET interfaces of the CPU (firmware V2.0 and higher).

Direct access to the OPC UA server of the CPU over the backplane bus of the automation system is not possible via CPs under the following conditions:

- Configuration with TIA Portal Version V16 or higher, S7-1500 CPU firmware version 2.8 or higher and CP 1543-1 firmware version V2.2 or higher.

  For configuration, see Access to OPC UA applications (Page 170).

Direct access to the OPC UA server of the CPU over the backplane bus of the automation system is not possible via CMs.

With SIMATIC S7 1500 SW controllers, access to the OPC UA server is possible via PROFINET interfaces that are assigned to the software PLC.

Additional access options of SW controllers are described in the following application example: Internal and external OPC UA connection via the virtual Ethernet interface of the software controller V2.5 or higher (https://support.industry.siemens.com/cs/ww/en/view/109760541).

Example for URLs (Uniform Resource Locator) that can be used to set up connections to the OPC UA server of the CPU:

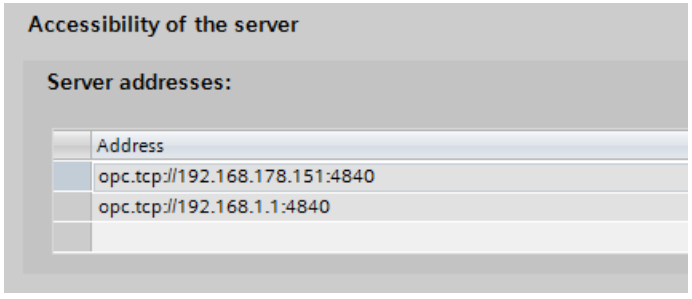


Figure 3-179 Display of the server addresses

The URLs are structured as follows:

- Protocol identifier "opc.tcp://"
- IP address
  - 192.168.178.151
    The IP address at which the OPC UA server can be accessed from the Ethernet subnet 192.168.178.
  - 192.168.1.1
    The IP address at which the OPC UA server can be accessed from the Ethernet subnet 192.168.1.
- TCP Port number
  - Default: 4840 (standard port)
    The port number can be changed under "OPC > UA > Server > Port".

Dynamic IP addresses

In the example below, the IP address for the PROFINET interface [X2] has not yet been specified.

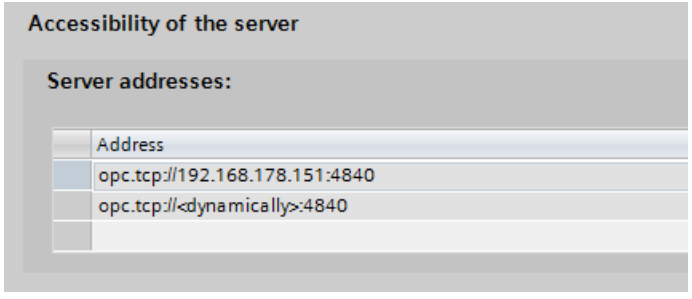


Figure 3-180 Display of the server addresses with dynamic IP address

The placeholder "<dynamically>" appears in the table.

The IP address of this PROFINET interface is set later on the device, e.g. via the display of the CPU.

Activating the standard SIMATIC Server interface

If the "Enable standard SIMATIC server interface" option is selected, the OPC UA server of the CPU provides the enabled PLC tags and server methods to the clients, as was specified by SIEMENS in the self-defined namespace.

This option is selected in the default setting.

Leave the option selected so that OPC UA clients can automatically connect to the OPC UA server of the CPU and exchange data.

If you do not select this option, you must add the server interface by entering the "OPC UA communication" entry in the project tree. This interface is then used as OPC UA server interface, see OPC UA server interface configuration (Page 270).

NOTE

General device information is readable even with deactivated standard SIMATIC server interface

Even if you disable the standard SIMATIC server interface, OPC UA clients can read general device information about the OPC UA server of the CPU.

Examples of such device information: DeviceManual, DeviceRevision, OrderNumber. In this case, however, all objects of the application program remain invisible to clients.

If you want to prevent that this device information is not visible, you have to disable the OPC UA server of the CPU.

11.3.3.3 General settings of the OPC UA server

TCP port for OPC UA

By default, OPC UA uses TCP port 4840. You can, however, select a different port. Entries from 1024 to 49151 are possible. You must, however, make sure that there are no conflicts with other applications. OPC UA clients must use the selected port when establishing a connection.

In the example below, port 48400 is selected:

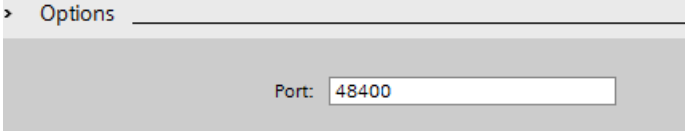


Figure 3-181 TCP port for OPC UA

An overview of the supported protocols and the port numbers used by the S7-1500 CPUs can be found in section Communications protocols and port numbers used for Ethernet communication (Page 35).

Settings for sessions

- Maximum timeout for sessions

  In this field, you specify the maximum time period before the OPC UA server closes a session without data exchange.

  Possible values between 1 and 600000 seconds.
- Maximum number of OPC UA sessions

  In this field, you specify the maximum number of sessions the OPC UA server starts and simultaneously operates.

  The maximum number of sessions is dependent on the performance capability of the CPU. Each session ties up resources.

Maximum number of registered nodes

In this field, you specify the maximum number of nodes the OPC UA server registers.

The maximum number of registered nodes depends on the capacity of the CPU and is displayed when you configure the field content (place cursor in field). Each registration ties up resources.

NOTE

No error message following attempt to register more than the configured maximum number of registrable nodes

If a client tries to register more nodes during runtime than the configured maximum number, the server of the S7-1500 CPU only registers the configured maximum number. Starting from the configured maximum number of registrable nodes, the server returns the regular string node IDs unchanged to the client so that the speed advantage gained by registration for these nodes is lost. The client does not receive an error message.

When configuring, make sure you have a sufficient reserve by taking into account the maximum number of nodes that can be registered (for example, using the technical data of the CPU).

Additional information

Details on which ports are used by the various services for data transfer via TCP and UDP, and what are the points to note when using routers and firewalls can be found in the FAQ (https://support.industry.siemens.com/cs/ww/en/view/8970169).

Backward compatible data type definitions according to OPC UA specification ≤ V1.03

The OPC UA specification (<= V1.03) defines mechanisms in order to read out data type definitions, for example for user-defined structures (UDTs), from a server by means of the TypeDictionaries.

In the OPC UA server properties of the CPU, you can set whether the CPU generates these backward compatible data type definitions according to the OPC UA specification ≤ V1.03 for the standard SIMATIC server interface or not.

Because TypeDictionaries are complex and result in large OPC UA XML files (server interfaces) which the client has to interpret, a simpler solution was introduced with OPC UA Specification

V1.04 (attribute "DataTypeDefinition" at the data type node). If your client supports the OPC UA specification V1.04 or higher, then disable the option.

Advantages of the data type definitions according to OPC UA specification as of V1.04:

- The server starts faster
- The memory is used more efficiently
- The "Browse" function is faster

11.3.3.4 Settings of the server for subscriptions

Subscription instead of cyclic queries

An alternative to cyclic queries for a PLC tag (polling) is to monitor this value. Use a Subscription: The server informs the client if the value of PLC tags changes.

One server usually monitors a large number of PLC values. For this reason, the server sends notifications to the client at regular intervals containing the new values of the PLC tags.

Advantages of subscriptions:

- The server starts faster
- The memory is used efficiently

How frequently does the server send notifications?

When a Subscription is set up, the OPC UA client specifies the intervals at which it wants to be sent the new values in the event of changes. To limit the communication load through OPC UA, set a minimum interval for the messages. For this purpose, use the parameters for the minimum publishing interval and the minimum sampling interval.

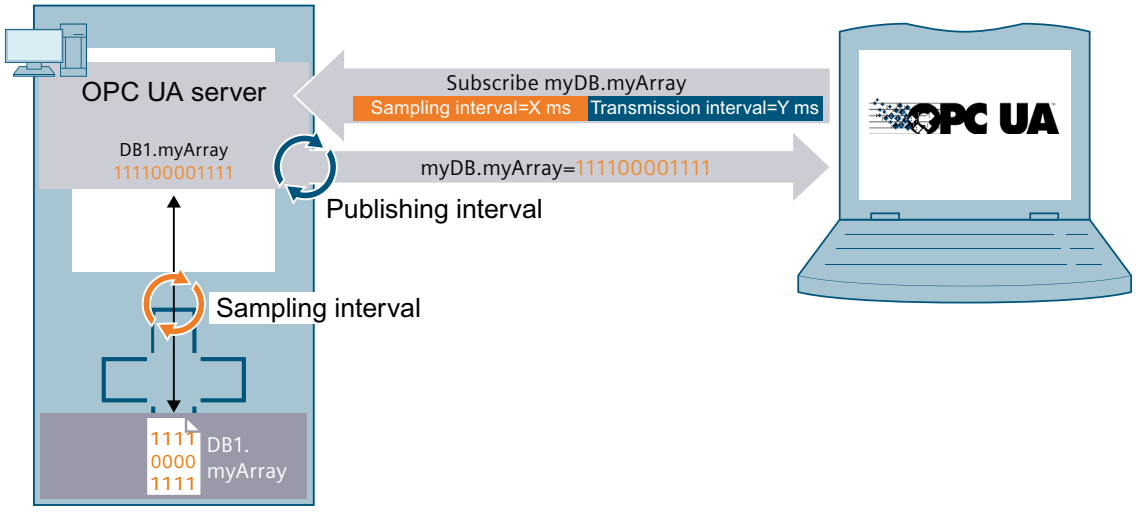


Figure 3-182 Principle of a subscription

Minimum publishing interval

With "Minimum publishing interval", you set the time intervals at which the server sends a message to the client with the new values in the event of changes.

250 ms is used as the "Minimum sampling interval" in the figure below. The value 200 ms is entered as the "Minimum publishing interval".

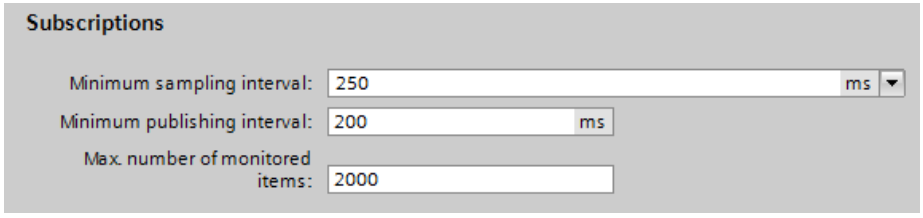


Figure 3-183 Subscription settings

In the example, following a value change the OPC UA server will send a new message every 200 ms if the OPC UA client requests an update.

If the OPC UA client requests an update every 1000 ms, the OPC UA server will only send a message with the new values once every 1000 ms (one second).

If the OPC UA client requests an update every 100 ms, the server will still only send a message every 200 ms (minimum publishing interval).

Minimum sampling interval

With "Minimum sampling interval", you set the time intervals at which the OPC UA server records the value of a CPU tag and compares it with the previous value to detect any changes.

If the sampling interval is selected smaller than the publishing interval and an OPC UA client requests a high sampling rate for certain PLC tags, two or more values may be measured during each publishing interval.

In this case, the OPC UA server writes the value changes into the queue and sends all value changes to the client after the completion of the publishing interval. If more value changes occur in the publishing interval than fit in the queue, the OPC UA server overwrites the oldest values (depending on the set "Discard Policy" of the client subscribing to the data, the option "Discard Oldest" has to be activated in this case). The most recent values are sent to the client.

Maximum number of monitored elements (monitored items)

In this field, you specify the maximum number of elements that the OPC UA server of the CPU simultaneously monitors for a value change.

The monitoring ties up resources. The maximum number of monitored elements is dependent on the utilized CPU.

More information

Information about the system limits of the OPC UA server of the S7-1500 CPUs (firmware V2.0 and V2.1) regarding subscriptions, sampling intervals and publishing intervals can be found in the following FAQ (https://support.industry.siemens.com/cs/ww/en/view/109755846).

When using subscriptions, certain status codes of errors provide information on the error that occurred. For information on causes and remedies for status codes of OPC UA client that appear, see the list of error codes in the online help of STEP 7 (TIA Portal) or in the following FAQ (https://support.industry.siemens.com/cs/ww/en/view/109755860).

The rules for subscriptions are available in section Rules for subscriptions (Page 380).

You will find information about the diagnostics of subscriptions in the section Subscription diagnostics (Page 341).

11.3.3.5 Using the TransferSubscription service

Useful information on transferring subscriptions

The OPC UA specification provides that OPC UA clients may transfer a subscription with its monitored items from one session to another session (see OPC 10000-4: UA Part 4: Services – in particular, "TransferSubscriptions" section).

The OPC UA server of an S7-1500 CPU supports the transfer of subscriptions as of firmware version V3.1.4.

Application examples:

- Interruption/timeout of an active session: e.g. due to a communication disruption: subscription transfer from an interrupted session to an active session to avoid data loss.
- A client is to be shut down; another client takes over the subscription.
- Load distribution: subscription transfer from one active session to another active session or to a new session.

Benefits of a subscription transfer:

- The transfer of a subscription prevents data loss (in the event of client failure, disconnection or overload).

  The TransferSubscription service enables the transfer of subscribed data. With this service, you solve the encountered connection termination problem in the following way:

  If the connection of the client taking over the subscription to the server has been established, it is not necessary to re-create the subscription with all monitored items. The accumulated, i.e. unsent, notification messages can be republished after the successful subscription transfer. See also OPC 10000-4: UA Part 4: Services, section "Re-establishing connections".
- The transfer of a subscription spares the OPC UA client the time- and resource-intensive process of creating a subscription.

  When a subscription with a large number of monitored items is created, a high CPU load is generated.

Requirement

A configuration for the S7-1500 OPC UA server is not required; the "TransferSubscription" service is provided on request of an OPC UA client.

All S7-1500 CPUs as of firmware V3.1.4 support the transfer of subscriptions.

Additional requirements:

- Users (clients) must have a role that grants them Read permission.
- If a subscription of an already closed session is to be transferred, the process must be completed within the subscription timeout.
- Subscriptions can be transferred both between sessions of an authenticated user and between sessions of anonymous users.
  - For authenticated users, both sessions must be assigned to the same user.
  - For anonymous users, the connection must also be encrypted and the sessions must have been created by clients with identical application URIs.

11.3.3.6 Handling client and server certificates

A secure connection between the OPC UA server and an OPC UA client is only established when the server can prove its identity to the client. This is done with the server certificate.

Certificate of the OPC UA server

When you have activated the OPC UA server and have confirmed the security prompts, STEP 7 automatically generates the certificate for the server and saves it in the local certificate directory of the CPU. You can view and manage this directory with the local certificate manager of the CPU (exporting or deleting certificates).

The figure below shows the local certificate manager of the CPU with the automatically generated certificate for the OPC UA server:



Figure 3-184 Local certificate manager of the CPU

Alternatively, you can also generate a server certificate yourself.

The certificate of the server is transferred from the server to the client during establishment of a connection. The client checks the certificate.

The client user decides whether the server certificate is to be trusted.

The user at the client side now has to decide whether the server certificate is to be trusted. If the user trusts the server certificate, the client stores the server certificate in its directory containing the trusted server certificates.

The following example shows a dialog of the client "UA Sample Client". When the user clicks the "Yes" button, the client trusts the server certificate:

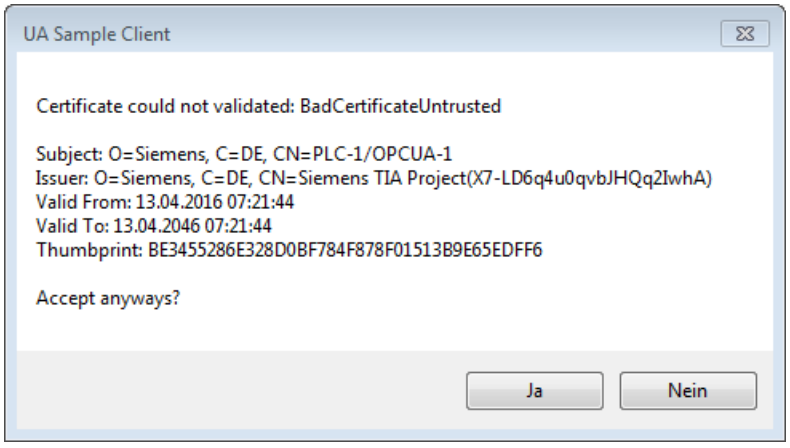


Figure 3-185 Dialog of the client "UA Sample Client"

Where does a client certificate come from?

Client of the S7-1500

If you are using the OPC UA client of an S7-1500 CPU (OPC UA client enabled), you can create certificates for these clients with STEP 7 as of V15. As of STEP 7 V21 and FW version V4.1 of a CPU, you can also manage the client certificates via a GDS (Global Discovery Server).

If you want to configure and manage the client certificates via GDS, continue reading in the section Handling client certificates during runtime (Page 371).

To create a local client certificate, proceed as follows:

1. In the "Project navigation", select the CPU that functions as the client.
2. Double-click "Device configuration".
3. In the properties of the CPU, click "Protection & Security > Certificate manager".
4. In the "Device certificates" table, double-click "<Add new>".
   STEP 7 opens a dialog.
5. Click the "Create" button.
6. Select the "OPC UA client" entry from the "Usage" list.
   Note:
   The URI and IP addresses under which the CPU can be accessed in your system must be entered under "Subject Alternative Name (SAN)".
   You must therefore configure the name and the IP interfaces of the CPU before you generate a client certificate.
7. Click "OK".
   STEP 7 now shows the client certificate in the "Device certificates" table.

8. Right-click this line and select the "Export certificate" entry from the context menu.
9. Select a directory where you will store the client certificate.

Clients of other manufacturers
When you use UA clients from manufacturers or the OPC Foundation, a client certificate is generated automatically during installation or upon the first program call. You have to import these certificates via the global certificate manager in STEP 7 and use them for the corresponding CPU (as shown above).

When you program an OPC UA client yourself, you can have the certificates generated by the program; see the section "Instance certificate for the client". Alternatively, you can generate certificates with tools, for example with OpenSSL or the certificate generator of the OPC Foundation:

- The procedure for OpenSSL is described here: "Generating PKI key pairs and certificates yourself".
- Working with the certificate generator of the OPC Foundation is described here: "Creating self-signed certificates".

Announcing client certificates to the server

You need to send client certificates to the server to allow a secure connection to be established.

To do this, follow these steps:

1. Select the "Use global security settings for certificate manager" option in the local certificate manager of the server. This makes the global certificate manager available.
   You will find this option under "Protection & Security > Certificate manager" in the properties of the CPU that is acting as server.
   If the project is not yet protected, select "Security settings > Settings" in the STEP 7 project tree, click the "Protect this project" button and log on.
   STEP 7 now displays the entry "Security functions" in the "Project navigation" under "Security settings".
2. Double-click "Security functions".
3. Double click "Certificate manager".
   STEP 7 opens the global certificate manager.
4. Click on the "Trusted certificates" tab.
5. Right-click in the tab on a free area (not on a certificate).
6. Select the "Import" command from the context menu.
   The dialog for importing certificates is displayed.
7. Select the client certificate that the server is to trust.
8. Click "Open" to import the certificate.
   The certificate of the client is now contained in the global certificate manager.
   Note the ID of the client certificate just imported.
9. Click the "General" tab in the properties of the CPU that is acting as server.
10. Click the area "OPC UA > Server > Security > Certificates".
11. In the Inspector window, scroll down to the "Trusted clients" section.

12. In the table, double-click on the empty row with "<Add new>". A browse button is displayed in the row.
13. Click this button.
14. Select the client certificate that you have imported.
15. Click the button with the green check mark.
16. Compile the project.
17. Load the configuration onto the S7-1500 CPU.

Result:
The server now trusts the client. If the server certificate is also considered trusted, the server and client can establish a secure connection.

Accepting client certificates automatically

When you select the option "Automatically accept all client certificates during runtime" (below the "Trusted clients" list), the server automatically accepts all client certificates.

NOTICE
Setting after commissioning In order to avoid security risks, deactivate the "Automatically accept client certificates during runtime" option again after commissioning.

Configuring security settings of the server

The figure below shows the available server security settings for signing and encrypting messages.

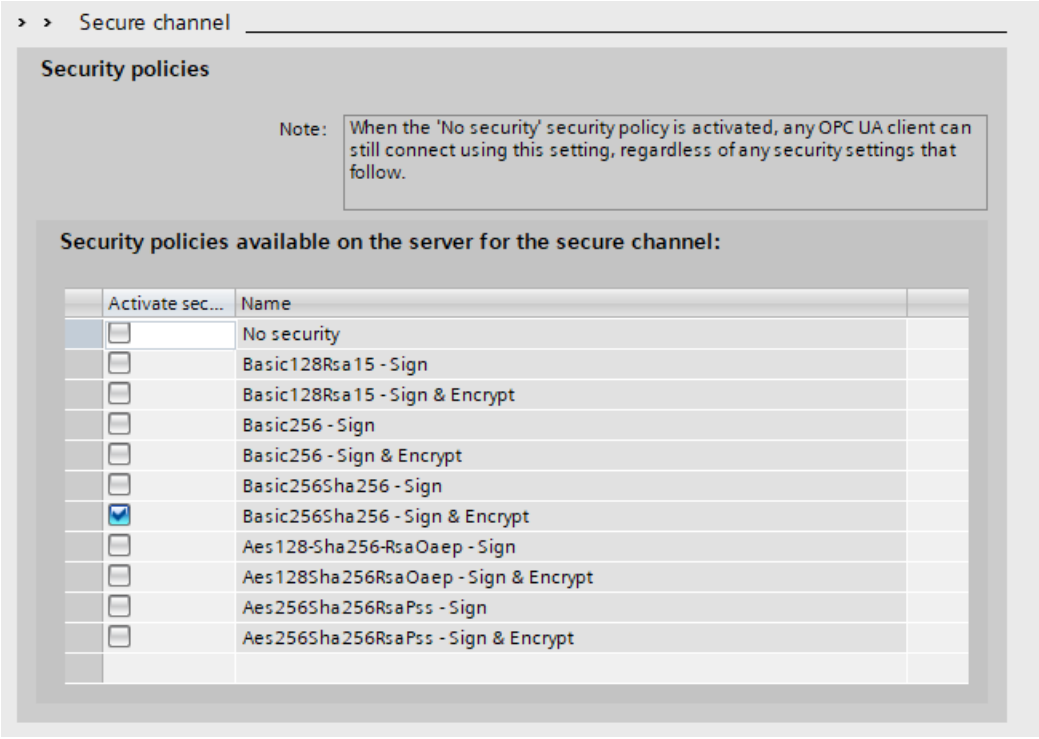


Figure 3-186 Configuring security settings of the server

By default, a server certificate is created that uses SHA256 signing. The following security policies are enabled:

- None
  Unsecured end point

  NOTE

  Disabling security policies you do not want
  If you have enabled all security policies in the secure channel settings of the S7-1500 OPC UA server – including the "No security" endpoint – data traffic between the server and client can also be unsecured (neither signed nor encrypted). The identity of the client remains unknown with "No security". Each OPC UA client can then connect to the server irrespective of any subsequent security settings.
  When configuring the OPC UA server, make sure that only security policies that are compatible with the security concept of your machine or plant are selected. All other security policies should be disabled.
  Recommendation: If possible, use the setting "Aes256Sha256RsaPss".

- Basic128Rsa15 -Sign
  Insecure end point, supports a series of algorithms that use the hash algorithm RSA15 and 128-bit encryption.
  This endpoint protects the integrity of the data through signing.

- Basic128Rsa15 -Sign & Encrypt
  Secure endpoint, supports a series of algorithms that use the hash algorithm RSA15 and 128-bit encryption.
  This endpoint protects the integrity and confidentiality of the data through signing and encrypting.
- Basic256 - Sign
  Secure endpoint, supports a series of algorithms that use the hash algorithm RSA15 and 256-bit encryption.
  This endpoint protects the integrity of the data through signing.
- Basic256 - Sign & Encrypt
  Secure endpoint, supports a series of algorithms that use the hash algorithm RSA15 and 256-bit encryption.
  This endpoint protects the integrity and confidentiality of the data through signing and encrypting.
- Basic256Sha256 - Sign
  Secure endpoint, supports a series of algorithms for 256-bit hashing and 256-bit encryption.
  This endpoint protects the integrity of the data through signing.
- Basic256Sha256 - Sign & Encrypt
  Secure endpoint, supports a series of algorithms for 256-bit hashing and 256-bit encryption.
  This endpoint protects the integrity and confidentiality of the data through signing and encryption.
- Aes128Sha256RsaOaep - Sign
  Secured endpoint, supports a range of algorithms for 256-bit hashing and 128-bit encryption.
  All certificates must use at least Sha256 signatures. This endpoint protects the integrity of the data by signing it.
  For high security requirements. PKI infrastructure required.
- Aes128Sha256RsaOaep - Sign & Encrypt
  Secured endpoint, supports a range of algorithms for 256-bit hashing and 128-bit encryption.
  All certificates must use at least Sha256 signatures. This endpoint ensures the integrity and confidentiality of the data by signing and encrypting it. For high security requirements. PKI infrastructure required
- Aes256Sha256_RsaPss - Sign
  Secured endpoint, supports a range of algorithms for 256-bit hashing and 256-bit encryption.
  All certificates must use at least Sha256 signatures. This endpoint protects the integrity of the data by signing it.
  For high security requirements. PKI infrastructure required.
- Aes256Sha256_RsaPss - Sign & Encrypt
  Secured endpoint, supports a range of algorithms for 256-bit hashing and 256-bit encryption.
  All certificates must use at least Sha256 signatures. This endpoint protects the integrity and confidentiality of data by signing and encrypting it.
  For high security requirements. PKI infrastructure required.

To enable the security setting, click the check box in the relevant line.

NOTE

If you use the settings "Basic256Sha256 -Sign" and "Basic256Sha256 -Sign & Encrypt", the OPC UA server and OPC UA clients must use "SHA256"-signed certificates.

For the settings "Basic256Sha256 -Sign" and "Basic256Sha256 -Sign & Encrypt", the certificate authority of STEP 7 automatically signs the certificates with "SHA256".

"No Security" security policy and authentication via user name and password

You can set the following combination:

Security policy = "No Security" and authentication via user name and password.

- The OPC UA server of the S7-1500 supports this combination. OPC UA clients can connect and encrypt the authentication data or not.
- OPC UA client of the S7-1500 CPU also supports this combination: However, in runtime it only connects if it can send the authentication data encrypted via cable!

11.3.3.7 Generating server certificates with STEP 7

The description below shows the procedure for generating new certificates with STEP 7 and applies in principle to various uses of the certificates. STEP 7 sets the appropriate purpose depending on which area of the CPU properties is used to start the following dialog.

Recommendation: To use the full functionality for the security of the OPC UA server, use the global security settings.

The global security settings are enabled in the CPU properties under "Protection & Security > Certificate manager".

Customizing server certificates

STEP 7 automatically generates a certificate for the OPC UA server of the S7-1500 when you activate the server (see "Activating the OPC UA server (Page 245)"). In the process STEP 7 uses the default values for the parameters of the certificate. If you want to change the parameters, follow these steps:

1. Click the three-dot button in the properties of the CPU under "General > OPC UA > Server > Security > Certificates".
   A dialog appears showing locally available certificates.
2. Click the "Create" button.

3. The dialog for generating new certificates is displayed (figure below). The values for an example are already entered:

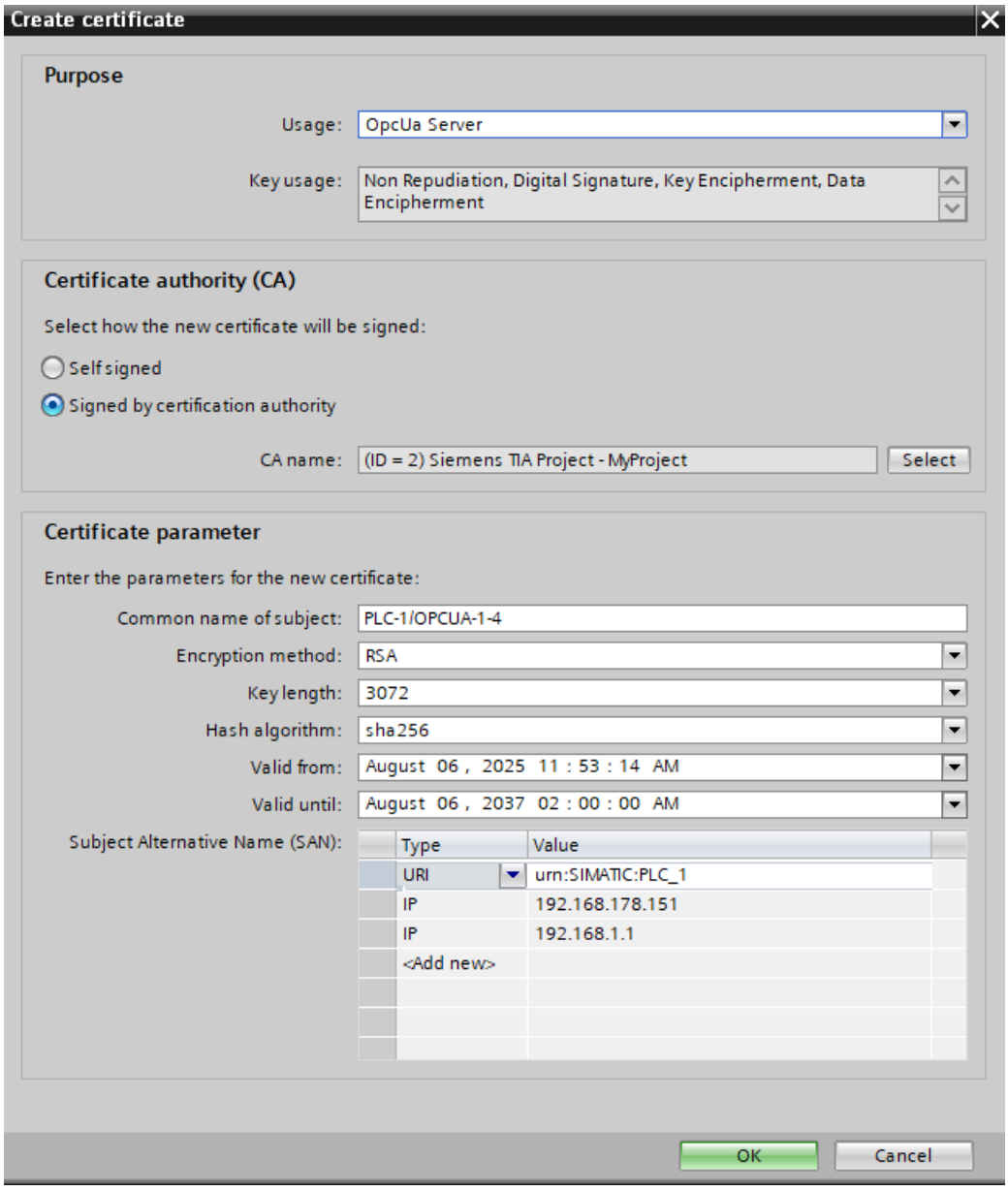


Figure 3-187 Customizing server certificates

4. Use other parameters if this is necessary in accordance with the security specifications in your company or your customer.

Explanation of fields for certificate generation

- Usage

  The default setting is "OPC UA server". Keep this default for the OPC UA server. The "Create a new certificate" dialog can be called up from several places in STEP 7. For example, if you open this dialog for the web server of the CPU, "Web server" is entered under "Usage". The following entries are available in the Usage drop-down list:

  – "OPC UA client"
  – "OPC UA client & server"
  – "OPC UA server"
  – "TLS"
  – "Web server"

- Certificate authority (CA)

  Select whether the certificate is to be self-signed or signed by one of the CA certificates of the TIA Portal. The certificates are described under "Certificates with OPC UA". If you want to generate a certificate that is to be signed by one of the CA certificates of the TIA-Portal, the project must be protected and you must be logged in as a user with all the required function rights. Further information can be found under "Basics of user administration in the TIA Portal".

- Common name of subject

  The default setting always consists of the name of the project and "\OPCUA-1". In the example, the project name is "PLC1". In the properties of the CPU set the project name under "General > Project information" > Name". Keep the default or enter a different name that is more meaningful for the OPC-UA server under "Certificate holder".

- Encryption methods

  The encryption method determines the algorithm (RSA or EC) for which the corresponding keys are to be generated.

- Key length

  Select the key length to be used when signing the certificate. The following entries are available:

  – "1024"
  – "2048"
  – "3072"
  – "4096"
  – "8192"

  You can find information on supported key lengths in the section Device-dependent security features (Page 54).

- Hash algorithm

  Select the hash algorithm to be used when signing. The following entries are available:

  – "sha1"
  – "sha256"
  – "sha384"
  – "sha512"

- Valid from

  Here you enter the date and time for the beginning of the validity of the server certificate.

- Valid until

  Here you enter the date and time for the end of the validity of the server certificate. Ensure that the certificate is valid not only for one year or a few years. In the example the certificate is valid for 30 years. However, for reasons of security you should renew the certificate at much shorter intervals. The long period of validity gives you the opportunity to decide when a suitable moment would be, for example, when the system is being serviced.
- Subject Alternative Name (SAN)

  The following is entered in the example above: "URI:urn:SIMATIC:PLC1,IP:192.168.178.151,IP:192.168.1.1". This URI must be correctly entered because it is checked against the communicated application description.

  The following entry would also be valid: "IP: 192.168.178.151, IP: 192.168.1.1". The important thing here is that the IP addresses via which the OPC UA server of the CPU can be accessed are entered here.

  See "Access to the OPC UA server (Page 248)".

  This allows OPC UA clients to verify whether a connection to the OPC UA server of the S7-1500 is really to be established or whether in fact an attacker is trying to send manipulated values from another PC to the OPC UA client.

11.3.3.8 User authentication

Types of user authentication

For the OPC UA server of the S7-1500, you can set what authentication is required for a user of the OPC UA client wishing to access the server.

You have the following options:

- **Guest authentication**

  The user does not have to prove their authorization (anonymous access). The OPC UA server does not check the authorization of the client user

  For CPUs up to firmware version V3.0: If you want to use this type of user authentication, select the "Enable guest authentication" option under "OPC UA > Server > Security > User authentication".

  For CPUs as of firmware version V3.1: Use the local user management to implement the guest authentication via the "Anonymous" user.

NOTE

To increase security, you should only allow access to the OPC UA server with user authentication.

- **User name and password authentication**

  The user has to prove their authorization (no anonymous access). The OPC UA server checks whether the client user is authorized to access the server. Authorization is given by the user name and the correct password.

  For CPUs up to firmware version V3.0: If you want to use this type of user authentication, proceed as follows:

  – Select the "Enable user name and password authentication" option under "OPC UA > Server > Security > User authentication".
  – Deactivate the guest authentication.
  – Enter the user in the "User management" table.

    To do so, click the "<Add new user>" entry. A new user is created with an automatically assigned name. You can edit the user name and enter the password for the user name. You can add a maximum of 21 users.

- **Additional user administration via the security settings of the project**

  For CPUs up to firmware version V3.0, the "Enable additional user management via project security settings" option is available. You can find this setting under the general OPC UA settings (CPU properties: OPC UA > General). If you select this option, the user management for the open project will also be used for user authentication for the OPC UA server: The same user names and passwords are then valid in OPC UA as in the current project.

  Proceed as follows to activate user management for the project:

  – Click "Security settings > Settings" in the project tree.
  – Click the "Protect this project" button.
  – Enter your user name and your password.
  – Enter additional users under "Security settings > Users and roles".

  If you configure an additional OPC UA server in your project, also select the option "Enable additional user administration via the security settings of the project". Repeated input of user names and passwords is then unnecessary.

Transfer of user authentication via the secure channel

In OPC UA, identification data for user authentication, such as user name and password, is transferred with a separate security policy. This security policy is referred to as the "UserTokenPolicy".

Regardless of the configured security policies for the secure channel, an OPC UA client selects an appropriate "UserTokenPolicy" during connection establishment when user authentication is required. This UserTokenPolicy ensures that a UserIdentityToken (e.g. user name and password) is always transferred with adequate security settings.

The OPC UA client is then able to transfer the user name and password with encryption if "No security" applies for the secure channel based on the configured security policy. For information on the process of establishing a secure connection in OPC UA, see Secure transfer of messages (Page 190).

11.3.3.9 Users and roles with OPC UA function rights

The following options for user authentication use central project settings for project users:

- For the server:
  For configuration of CPU properties (OPC UA > Server > Security > User authentication). Option: "Enable additional user administration via the security settings of the project"
- For the client:
  For configuration of client interface ("Configuration" tab, "Security"). Option: "User (TIA Portal - security settings)"

Requirement

Before you can edit the security settings, the project must be protected and you must be logged on with sufficient rights, for example as administrator.

Settings in the project tree > "Security settings"

You access the central user settings and roles in the protected project in the project tree under "Security settings". This is where you centrally define users with user name, password and function rights. You can simply use these settings elsewhere.

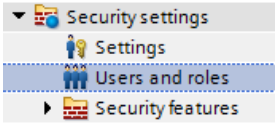


Figure 3-188 Setting user and roles

Reusing central security settings

Examples for reusing elsewhere:

- User selection for user authentication for OPC UA server
  With this setting, you tell the server which client (user) with which user name and which password is allowed to access the server.
- User selection for OPC UA client authentication
  With this setting, you tell the client the user name and password that it is to use for client authentication for the server.

The settings for the client and server must correspond: The user name and password used by the client to log on must have been set up on the server and assigned the required authorizations.

Function rights for server and client

The corresponding function rights for the client or the server must also be enabled for users of the client function and users of the server function on an S7-1500 CPU. It is not enough simply to save the user name and password centrally.

Here is an example to illustrate this type of rights use.

1. Under "Security settings > Users and roles", you define a new role in the "Roles" tab with the name "PLC-opcua-role-all-inclusive", for example.
   Tip: The tab may be covered by an information window ("The current status has not yet been checked..."). In this case, first close the information window.
2. In the "Function rights categories" section, you navigate to the runtime rights and then to the CPU function rights, and select the CPU whose function rights you want to set.
3. You will find the following function rights in the "Function rights" section:
   - **OPC UA server access**
     This function right applies on the OPC UA server of the S7-1500 CPU. Only when this option is selected, can the user with the role "PLC-opcua-role-all-inclusive" transfer certificates, CRLs or trusted lists to the CPU at runtime (push function). This function right is required for automated certificate handling, for example, in the context of GDS (Global Discovery Service).
   - **Managing certificates**
     This function right applies on the OPC UA server of the S7-1500 CPU. Only when this option is enabled, can the user with the role "PLC-opcua-role-all-inclusive" transfer certificates, CRLs or trusted lists to the CPU at runtime (push function). This function right is required for automated certificate handling, for example, in the context of GDS (Global Discovery Service).
   - **User authentication of the OPC UA client**
     This function right applies on the OPC UA client of the S7-1500 CPU (with client instructions). Only when this option is selected, can the user with the role "PLC-opcua-role-all-inclusive" use the user name and password for authentication to establish a session with a server.

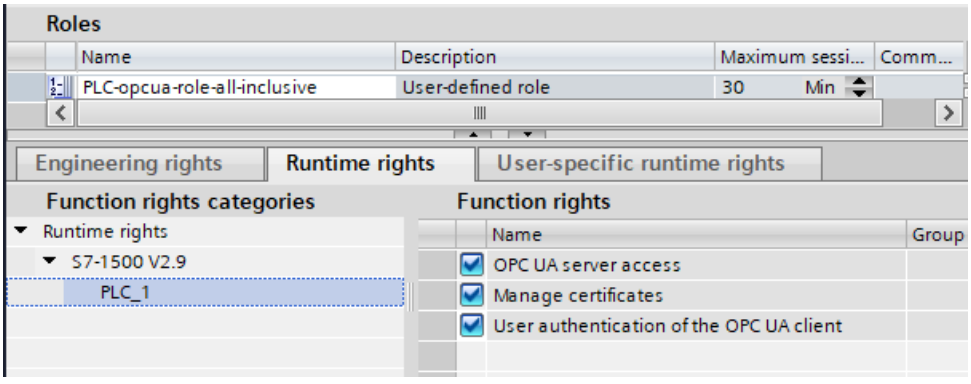


Figure 3-189 Setting function rights

4. The role "PLC-opcua-role-all-inclusive" still needs to be assigned to the relevant users ("Users" tab under "Security settings" in the project tree).

NOTE

"Runtime timeout" for users with OPC UA function rights

The value in the column "Runtime timeout" (max. session duration) in the table for user configuration does not evaluate the CPU for OPC UA runtime rights.

Therefore, a user is not automatically logged out after a certain period of time. For this purpose use OPC UA specific mechanisms such as the parameter "Max. session timeout" (area OPC UA > Server > Settings).

11.3.3.10 Diagnostic settings of the server

Diagnostics

You can specify the scope of the diagnostics of the OPC UA server in the CPU settings.

To change the diagnostics scope, navigate to the "OPC UA > Server > Diagnostics" area.

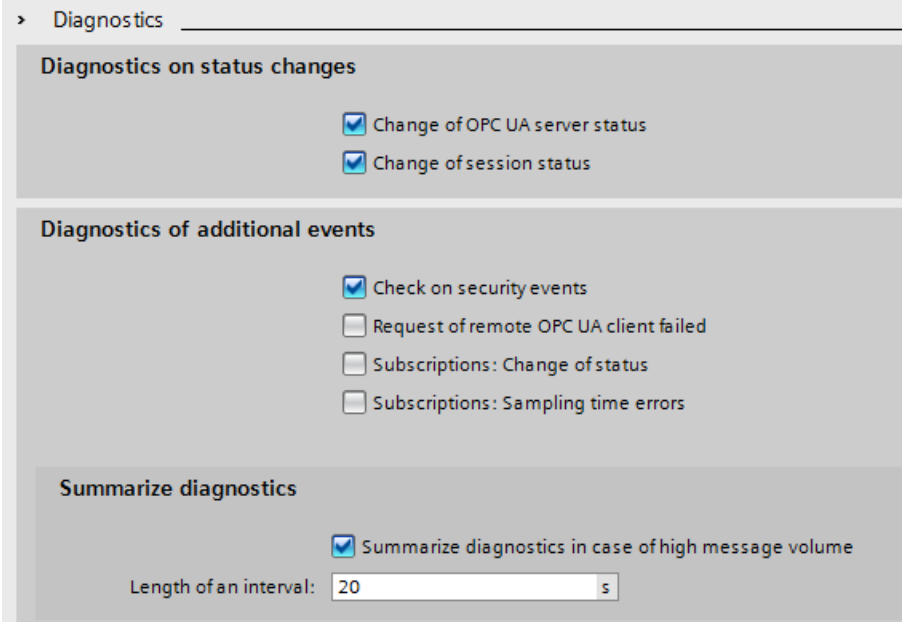


Figure 3-190 Diagnostic settings of OPC UA server

Default setting

The default setting is a diagnostics behavior that supports the most important diagnostics without appreciably increasing the communication load.

You enable diagnostics for subscriptions when the OPC UA server also uses subscriptions, i.e. if necessary during the commissioning phase only.

Reason: A large volume of diagnostic activity generates a high communication load in the CPU and may suppress other important messages. Or, the high volume of diagnostics may result in important messages disappearing in the mass of messages and being ignored.

Additional information

You will find additional information on the meaning and effect of the settings shown above here (Page 335).

11.3.3.11 License for OPC UA

Runtime licenses

A license is required to run the OPC UA server of the S7-1500 CPU. The type of license required depends on the performance of the respective CPU. The following license types are differentiated:

- SIMATIC OPC UA S7-1500 small (required for CPU 1511, CPU 1512, CPU 1513, ET 200SP CPUs, CPU 1515SP PC)
- SIMATIC OPC UA S7-1500 medium (required for CPU 1515, CPU 1516, Software Controller CPU 1507, CPU 1516pro-2PN)
- SIMATIC OPC UA S7-1500 large (required for CPU 1517, CPU 1518)

The required license type is displayed under "Properties > General > Runtime licenses > OPC-UA > Type of required license":

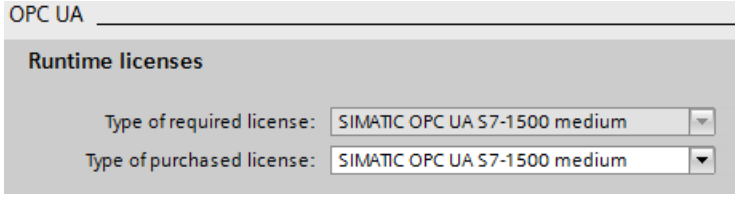


Figure 3-191 OPC UA server Runtime licenses

To confirm purchase of the required license, follow these steps:

1. Click "Runtime licenses > OPC UA" in the properties of the CPU.
2. Select the required license from the "Type of purchased license" drop-down list.

11.3.4 OPC UA server interface configuration

11.3.4.1 What is a server interface?

Definition

A server interface combines nodes of an OPC UA address space of a CPU into a unit, so that a specific view on this CPU is provided for OPC UA clients.

Each server interface defines one or more namespaces in the OPC UA server of the CPU.

STEP 7 (TIA Portal) differentiates between the following types of server interfaces:

- Companion specification

  For this type of server interface, you use a Companion Specification created by a workgroup, for example.

  The workgroup is typically composed of members of the OPC Foundation and another industry organization who have jointly specified an OPC UA information model for a specific purpose (for example, for data exchange with RFID devices or with injection molding machines).

  This information model is realized in the form of OPC UA nodes in the address space of an OPC UA server. OPC UA clients can access these OPC UA nodes.

  You can also use the server interface type "Companion specification", for example, to download company-internal information models, e.g. in SiOME.

  If you implement a certain companion specification in your project, you apply the specifications of this companion specification into your project as server interface.

  For "Companion specification"-type server interfaces, you can import multiple namespaces which the Companion specification uses.

  Additional information on companion specifications is available here (Page 271).

  Additional information on SiOME is available here (https://support.industry.siemens.com/cs/ww/en/view/109755133).

  – When companion specifications refer to type definitions in dependent specifications, use the reference namespaces for this. You import reference namespaces as you would the actual companion specifications.

    See Creating a server interface for companion specification (Page 278).

  – If you want to make instance data from FBs or UDTs of the CPU accessible to OPC UA clients, you can have these instance data assignments automatically made as of TIA Portal version V17. You only need to map the FB types or the UDTs to suitable OPC UA data types of an imported reference namespace. For this mapping to be possible, enable the option "Generate OPC UA nodes based on the local data mapping" in the dialog for creating an OPC UA server interface of the type companion specification/reference namespace.

    See Generating OPC UA nodes based on local data mappings of FB types and UDTs (Page 301)

- User-defined server interface:

  For this type of server interface you combine OPC UA nodes of an OPC UA server into a unit.

  To do this, use the specifications for your project or the requirements for your machine or your plant as a basis.

  Additional information on the user-defined server interface is available here (Page 283).

Injection molding machine as an example for companion specification

In this example, a server interface contains the following elements:

- OPC UA nodes which you can write with an OPC UA client to receive information about this injection molding machine (in readable PLC tags)
- OPC UA nodes which you can write with an OPC UA client to transfer values to the injection molding machine (in writable PLC tags)
- OPC UA nodes which you can call with an OPC UA client to start functions of the injection molding machine (via server methods)

This server interface enables a default view of a CPU, which can be used to control an injection molding machine.

For injection molding machines, the companion specifications "OPC UA specifications for plastics and rubber machines" (previously "Euromap") define a whole series of OPC UA nodes which you can apply as a server interface.

Other OPC UA nodes of the CPU are not included in this server interface. This provides a better overview.

Example of user-defined server interface

A CPU should control the production of workpieces. Production begins when a production job arrives from the higher-level control system.

The production jobs are transferred via a server method: A control system transmits information on a workpiece by calling the server method in the CPU. This server method also starts production.

The control system, i.e. the connected OPC UA client, should only see this one server method. Therefore, you create a user-defined server interface in the CPU and assign the server method to this server interface. You enable only this server interface for OPC UA clients and thus limit the view of the CPU to this one function.

11.3.4.2 Using OPC UA companion specifications

Introduction

OPC UA is universally applicable: The standard itself does not, for example, specify how PLC tags are to be named. It is also up to the individual user (application developer) to program and name server methods that can be called over OPC UA.

Information modeling and standardization for devices and sectors
For applications of the same kind, it is worth standardizing your device or machine interface with the "OPC UA toolkit".

Many different bodies and working groups have driven forward standardization and developed a range of companion specifications.

These specifications define:

- The objects, methods and tags with which a typical device or machine is to be described.
- The namespace intended for the specified objects.

Machines are typically structured in functional or technological units, and these units are then standardized.

Companion specifications offer machine and plant operators the benefits of a standardized interface. For example, all RFID readers that comply with the AutoID specifications can be integrated in the same way. This means that all RFID readers that comply with the AutoID specifications can be addressed by OPC UA clients in the same way irrespective of manufacturer.

Another example of companion specifications is the Euromap 77 Companion Specifications from the injection molding machinery sector.

The following section uses the example of Euromap 77 to detail how to apply companion specifications in STEP 7 (TIA Portal) and create the necessary PLC tags.

NOTE

EUROMAP and the OPC Foundation have established the Joint Working Group "OPC UA Plastics and Rubber Machinery".

The existing EUROMAP recommendations EUROMAP 77 (data exchange between injection moulding machines and MES), 82.1 (temperature control devices) and 83 (general definitions) were published under the neutral umbrella of the OPC Foundation as OPC 40077, 40082-1 and 40083.

A major change it the change of the namespace, for example, for EUROMAP 77: Currently "http://opcfoundation.org/UA/PlasticsRubber/IMM2MES/".

The examples listed below use the previously valid designations and references.

Example Euromap 77 (currently: OPC 40077)

Euromap 77 or the successor standard OPC 40077 standardizes the exchange of data between injection molding machines and the higher-level MES (Manufacturing Execution System). This allows the MES to connect all lower-level injection molding machines in the same way.

The standardized data interface facilitates the integration of injection molding machines into a plant.

Using companion specifications: Overview

Euromap 77 is described in the OPC UA XML file "Opc_Ua.EUROMAP77.NodeSet2.xml".

NOTE

Euromap 77, Euromap 83 and OPC UA for Devices (DI)

With Release Candidate 2, some of the Euromap definitions have been transferred from Euromap 77 to Euromap 83 (currently OPC 40083). You will therefore also need to import the OPC UA server interface of Euromap 83.

"OPC UA for Devices" is a generally applicable information model for the configuration of hardware and software components. The information model also serves as the basis for other companion standards and is therefore also imported.

The OPC UA XML files are available here:

Euromap77 (https://www.euromap.org/euromap77)

Euromap83 (https://www.euromap.org/euromap83)

OPC UA for Devices (https://opcfoundation.org/UA/schemas/DI/)

These XML files define an OPC UA interface of an injection molding machine that complies with Euromap 77.

Using Euromap 77: Overview

To use Euromap 77, proceed as follows:

1. Generate an XML file by creating an instance of the type "IMM_MES_InterfaceType" using the SiOME program.
   How to proceed is described below in "Step 1: Create instances in SiOME".
2. In STEP 7 (TIA Portal), create PLC tags and server methods that correspond to the instance of the type "IMM_MES_InterfaceType" (created in Step 1).
   See below for information on how to proceed in "Step 2: Create PLC tags in STEP 7".
   An example of OPC UA nodes and the corresponding PLC tags can be found in section "Creating a server interface for companion specification (Page 278)".
3. In STEP 7 (TIA Portal), add a new server interface of companion specification type and import the XML file you created in step 1.
   The "Creating a server interface for companion specification (Page 278)" section describes how to proceed.
4. Assign the OPC UA nodes of the new server interface to the corresponding PLC tags, which you created in step 2.
   The "Creating a server interface for companion specification (Page 278)" section describes how to proceed.

Step 1: Create instances in SiOME

The following section describes how to use the free program "SiOME", the "Siemens OPC UA Modeling Editor".

With SiOME, you can create an OPC UA XML file, which describes the server interface (an information model).

Download link and explanations about SiOME are available here (https://support.industry.siemens.com/cs/ww/en/view/109755133).

Procedure in STEP 7

To use the new server interface, import the server interface into the STEP 7 project, see section "Creating a server interface for companion specification (Page 278)".

When the project is loaded into the CPU, the new server interface is available for OPC UA clients.

Procedure in SiOME 1.7.3

NOTE
The following description shows the work steps in SiOME 1.7.3.
Follow-up versions of SiOME make it easier for you, for example, to create corresponding DBs, structures, variables or methods in the user program. Using a drag-and-drop operation, you can transfer data, for example, from SiOME to the TIA Portal (user program). In this case, the variables, etc. are already mapped correctly or, for methods, the corresponding FB elements are also generated correctly in the user program.
Download the current SiOME version using the download link listed above, and follow the instructions in the documentation included in the download.

The following description shows the work steps in SiOME 1.7.3.

To use Euromap 77, create an XML file with an instance of "IMM_MES_InterfaceType".

The object type must be instantiated in order for the information model of the specific machine to appear in the address space of the OPC UA server.

The object type "IMM_MES_InterfaceType" is the root object type of Euromap 77. "IMM" stands for "Injection Moulding Machine".

Follow these steps:

1. Download the files "Opc_Ua.EUROMAP77.NodeSet2.xml" and "Opc_Ua_EUROMAP83_NodeSet2.xml" from the Euromap website (see above).
2. Download the file "Opc.Ua.Di.NodeSet2.xml" from the OPC Foundation website.
   The "Opc.Ua.Di.NodeSet2.xml" file contains type definitions which Euromap 77 uses.
3. Start SiOME.
4. First, import the namespace "http://opcfoundation.org/UA/DI/".
   To do so, click the "Import XML" button in the "Information model" area.

   Figure 3-192 "Import XML" button in SiOME

   SiOME displays the dialog for the opening files.
5. To import the file, select the "Opc.Ua.Di.NodeSet2.xml" file and click "Open".
   Result: SiOME imports the XML file and shows the namespace "http://opcfoundation.org/UA/DI/" in the "Namespaces" area.
   The standard namespace "http://opfoundation.org/UA/" is always available in SiOME and does not have to be imported.
6. Now import the namespace "http://www.euromap.org/euromap83/"
   To do so, click the "Import XML" button again in the "Information model" area.
   Select the file "Opc_Ua.EUROMAP83.NodeSet2.xml".
   Result: SiOME imports the XML file and shows the namespace "http://www.euromap.org/euromap83/" in the "Namespaces" area.
7. Now import the namespace "http://www.euromap.org/euromap77/"
   To do so, click the "Import XML" button again in the "Information model" area.
   Select the file "Opc_Ua.EUROMAP77.NodeSet2.xml".

8. Create your own namespace for your project.
   To do this, right-click in the "Namespaces" area on "OPC UA Modelling Editor Project" or on "Namespaces" and select "Add Namespace".
   SiOME opens the "Add Namespace" dialog.
9. Enter the name of a new namespace.
   The "YourCompany.org" namespace is used in the example.
   SiOME now also displays the new namespace:

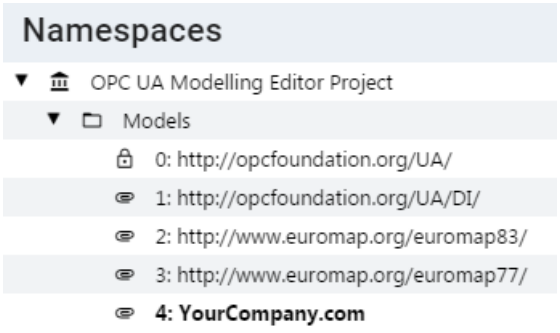


Figure 3-193 Display of the namespace in SiOME

10. Create an instance from the root object type IMM_MES_InterfaceType of the Companion specification Euromap 77.
    To do so, in the "Information model" area, right-click the "DeviceSet" directory and select "Add Instance".
    SiOME displays the "Add Instance" dialog.
11. For "Name", enter a meaningful name for your instance.
    In the example, enter "IMM_Manufacturer_01234".
    For "TypeDefinition", select "IMM_MES_InterfaceType".
    This object type is the root object type of Euromap 77: If you generate an instance of this object type, then use the Euromap 77 once in the address space of your OPC UA server.

12. Click "OK".
    SiOME shows the new instance "IMM_Manufacturer_01234" in the "Information model" area under "DeviceSet":

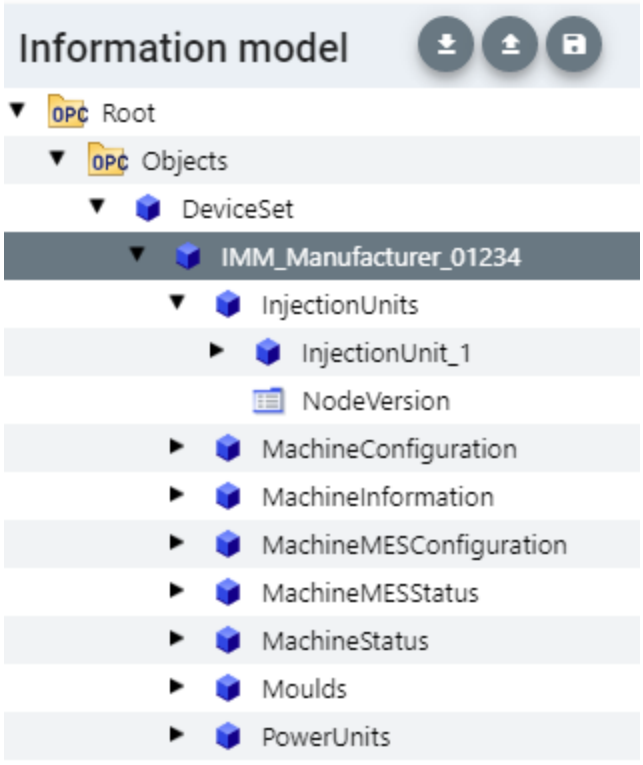


Figure 3-194 Display information model

13. Create an instance of the data type "InjectionUnitType".
    To do this, right-click on the "InjectionUnits" directory in the "Information model" area and select "Add Instance".
    SiOME displays the "Add Instance" dialog.
    For "Name", enter a meaningful name for the instance.
    In the example, enter "InjectionUnit_1".
    For "TypeDefinition", select "InjectionUnitType".
    Click "OK".
14. Create a new "Mould_1" instance of the "MouldType" object type in the "Moulds" directory.
15. Create a new instance "PowerUnit_1" of the "PowerUnitType" object type in the "PowerUnits" directory.
16. Save the XML file.
    To do so, click the "Quick save" button in the "Information model" area:



Figure 3-195 "Quick save" button in SiOME

17. Export the XML file.
    To do so, click the "Export XML" button in the "Information model" area.



Figure 3-196 "Export XML" button in SiOME

SiOME shows the "Export XML" dialog.

18. Leave all namespaces activated and click "OK".
    SiOME displays the "Save as" dialog.
19. Select a meaningful name and save the exported file.
    In the example, name the XML file "IMM_Manufacturer_01234".

Result:

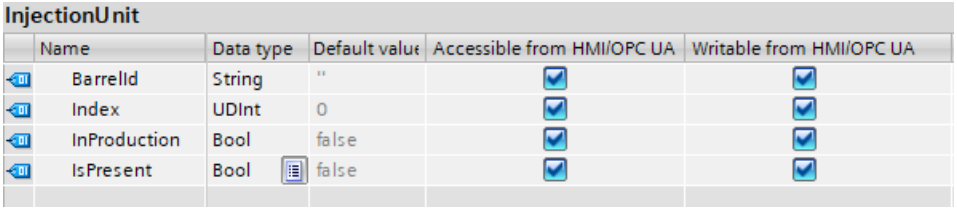
You have now created an XML file which uses the companion specification "Euromap 77" once (with one instance).

Step 2: Creating PLC tags for the Euromap 77 instance in STEP 7.

For Euromap 77, you must provide PLC tags and server methods in your user program and assign the instance of the "IMM_MES_InterfaceType" type.

To create PLC tags for the instance of the "IMM_MES_InterfaceType" type, proceed as follows.

1. Create a user-defined data type (UDT).
   The figure below shows the beginning of the user-defined data type "InjectionUnit" as example.
   This data type has the same structure as "InjectionUnit" in the type "IMM_MES_InterfaceType".
   Make sure that you use SIMATIC data types that are compatible with the OPC UA data types (see "Mapping of data types" below).



InjectionUnit

	Name	Data type	Default value	Accessible from HMI/OPC UA	Writable from HMI/OPC UA
	BarrelId	String	''	☑	☑
	Index	UDInt	0	☑	☑
	InProduction	Bool	false	☑	☑
	IsPresent	Bool	false	☑	☑

Figure 3-197 Creating a UDT in STEP 7

2. Add a new global data block to your STEP 7 project.
   In the example, name the data block "IMM_Manufacturer_01234", so that there is a reference to the injection molding machine of the respective manufacturer and the serial number.
3. Create a new element in this data block.
   In the example, name this element "InjectionUnit_1"
4. Assign the new user-defined data type "InjectionUnit" to this element.

Result

In your STEP 7 project, you have created a tag for the Euromap 77 in the "IMM_Manufacturer_01234" data block.

11.3.4.3 Creating a server interface for companion specification

For basic information on companion specifications, refer to the section "Using OPC UA companion specifications (Page 271)". The benefits of the Euromap 77 companion scpecification, which provides a model for injection molding machines, is also discussed in detail there.

Using this companion standard, the S7-1500 CPU can control an injection molding machine, for example, and provide an OPC UA client, such as a higher-level MES system, with an interface for accessing the functions and tags of injection molding machine.

An OPC UA server interface of the type "Companion Standard" limits the access of clients to exactly those functions and tags that are required, for example, for higher-level systems (MES systems).

The following description shows how to create a server interface in STEP 7 (TIA Portal) which contains only the Euromap 77 companion specification.

If you want to make OPC UA clients accessible to other tags or methods than those required for the management of an injection molding machine, simply create another OPC UA server interface. In this way, you can clearly arrange the functionality of the CPU as OPC UA server.

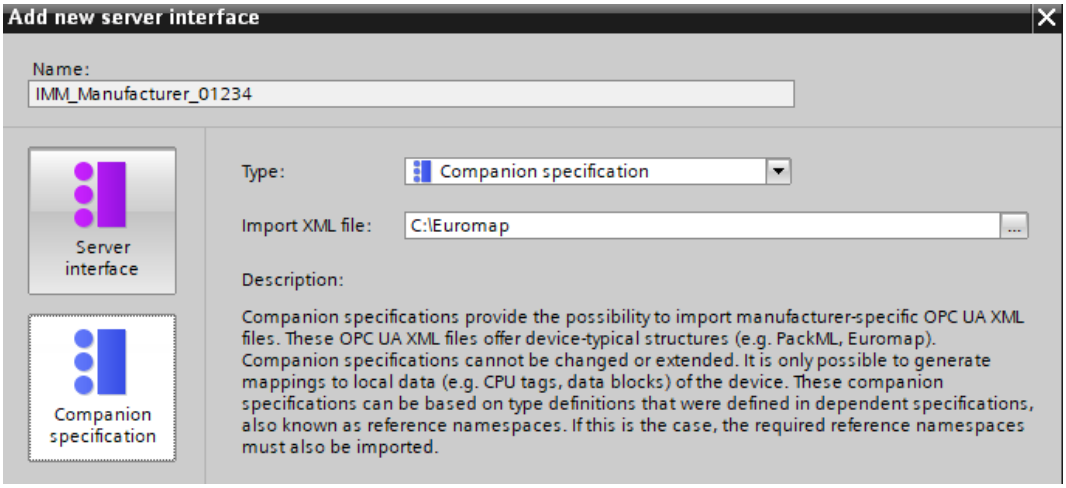
Creating a server interface for a companion specification

To create a server interface for a companion specification with STEP 7 (TIA Portal), proceed as follows:

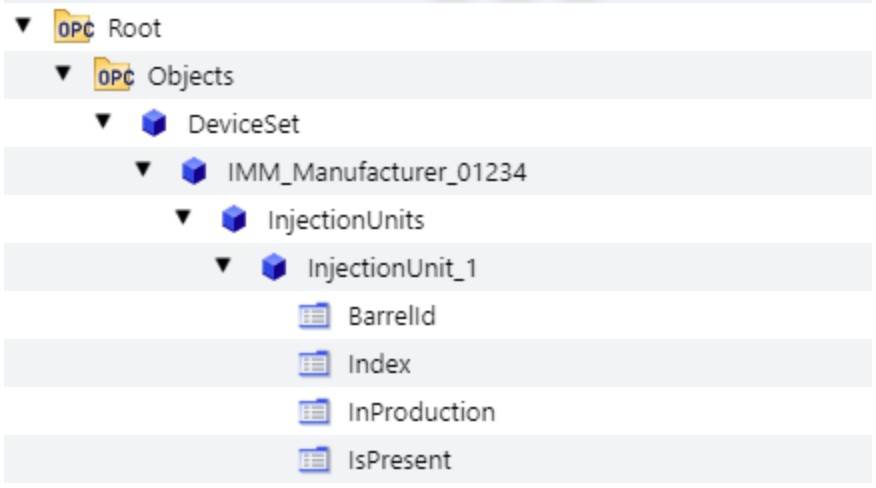
1. Select the CPU that you want to use as an OPC UA server.
2. In the project tree, click "OPC UA communication > Server interfaces".
3. Double-click "Add new server interface".
4. To select this type of server interface, click "Companion specification".

   A general name for the new server interface is entered in the dialog, for example "Server_Interface_1".

5. Change the name of the new server interface so that it is descriptive in your project.
   The name should have the following structure according to Euromap 77:
   "IMM_<Manufacturer>_<Serial number>".
   The example uses the name "IMM_Manufacturer_01234".



6. In the "Import XML file" field, select an XML file that describes an information model.
   The "Using OPC UA companion specifications (Page 271)" section describes how to create such an XML file with the SiOME tool.
   The figure below shows a section from the information model:
   "IMM_MANUFACTURER_0123456" an instance (use) of the type "IMM_MES_InterfaceType" which was defined by Euromap 77 . "InjectionUnit_1" is an instance of the "InjectionUnitType" type of Euromap 77.



7. Click "OK".

   STEP 7 (TIA Portal) imports the information model described in the selected XML file.

   An error occurs when type definitions are used in the imported XML file that are not yet present in STEP 7 (TIA Portal) and that are also not contained in the imported XML file.

   In the example, an XML file is imported that uses type definitions defined in the following namespaces (Namespaces):

   – http://opcfoundation.org/UA/DI/
   – http://www.euromap.org/euromap83/
   – http://www.euromap.org/euromap77/

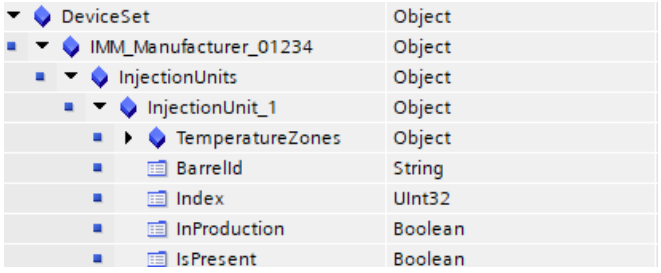
   Tip: STEP 7 displays missing namespaces in the lower area of the OPC UA interface editor ("Properties" tab).

   To do this, select the server interface in the project tree (here: IMM_Manufacturer_01234) and select the "Namespaces" area in the inspector window. Missing namespaces are selected.

   If one or more namespaces are missing in your STEP 7 project, create a new server interface of the "Reference namespace" type for each namespace.

   The "Creating a server interface for reference namespace (Page 299)" section describes the procedure.

   If all reference namespaces are available, STEP 7 displays the table without errors:



8. Drag the OPC UA elements from the right area of the table (OPC UA elements) to the left part of the table (OPC UA server interface) so that the respective OPC UA elements (the local PLC tags) are assigned to the respective OPC UA nodes of Euromap 77.

   The figure below shows a section from the assignment of the local data (PLC tags) to the OPC UA nodes of the Euromap 77:

OPC UA-Server-Schnittstelle

Name	Node type	Local data	Data type
DeviceSet	Object		
IMM_Manufacturer_01234	Object		
InjectionUnits	Object		
InjectionUnit_1	Object		
TemperatureZones	Object		
NodeVersion	String		
BarrelId	String	"IMM_Manufacturer_01234"."InjectionUnit_1"."BarrelId"	String
Index	UInt32	"IMM_Manufacturer_01234"."InjectionUnit_1"."Index"	UDInt
InProduction	Boolean	"IMM_Manufacturer_01234"."InjectionUnit_1"."InProduction"	Bool
IsPresent	Boolean	"IMM_Manufacturer_01234"."InjectionUnit_1"."IsPresent"	Bool

NOTICE
Checking the mapping of CPU local data on nodes of the OPC UA server interface When invalid assignments (mappings) exist in the server interface, they can result in incorrect read and write operations. Check the assignments and run a consistency check.

Information on the server interface

The editor for configuring the OPC UA server interface is structured as a table and provides the following information:

- **Name**

  The top node (root node) is named "IMM_Manufacturer_01234" in the example. If a client browses in the address space of the server, this node is the container for all lower-level nodes. BrowseName and the DisplayName of this node depend on the name you have assigned for the server interface.

  In this case, for example, this name stands for the injection molding machine as a whole. It is the name of the instance of the Euromap 77 companion specification that is used here. According to the companion specification, the instance name should begin with "IMM", followed by the name of the manufacturer of the injection molding machine; the serial number of the machine is added to the end. This allows a unique identification of the machine.

  The names of all other (lower-level) nodes are defined by the specification (in the example above by Euromap 77). These node names must not be changed. This ensures a uniform view of all injection molding machines, which complies with the specification.

- **Node type**

  Type of the OPC UA node. The type is specified by the companion specification that is used.

  In the following cases, STEP 7 marks a node type in the table in color:

  – No definition is included for this in the imported XML file or

  – The namespace in which the type was defined is not available in STEP 7.

  In this case, create a server interface of the "Reference namespace" type for the missing namespace or for each of the missing namespaces.

  The missing namespaces can be found under "Namespaces" in the properties of the server interface.

- **Local data**

  STEP 7 displays the data block which is assigned to the OPC UA node: The CPU reads the value of the OPC UA node from this data block.

  If a data block is highlighted in color (e.g. after a consistency check), the specified data block is not available in the CPU.

  In this case, you have to create the missing data block in the CPU (of user program) and supply it with values.

- **Data type**

  The SIMATIC data type of the PLC tag (e.g. element of a data block) in the CPU, from which the value of an OPC UA node (UAVariable type) is read, or to which a value is assigned.

Updating the interface

You can update the server interface for companion specifications.

Example: After importing companion specifications and then importing reference namespaces on which the companion specifications depend, the type definitions of the reference namespaces do not take effect immediately.

When you click the "Update interface" button, the missing type definitions of the companion specifications are resolved.

"Update interface" button:



Generate local data

You have the option of generating local data for all or for selected nodes of the server interface that are not already assigned ("mapped") to local data of the CPU. The newly created local data are mapped automatically.

You trigger the automatic generation of local data by clicking the "Generate local data" button (all nodes that are not already mapped) or by selecting individual nodes and then clicking the "Generate local data" shortcut menu.

"Generate local data" button:

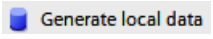


Figure 3-198 "Generate local data" button:

You can only generate nodes that can be mapped to local data, which means no objects, no folders, no methods or input/output arguments of methods.

After you have clicked the button or selected the shortcut menu, you must select in the follow-up dialog box whether the local data should be created in a new DB or in an existing DB.

Consistency check

You have the option to check the server interface.

STEP 7 (TIA Portal) checks whether the OPC UA node of the server interface PLC tags (data blocks) has been assigned compatible SIMATIC data types.

To check the consistency of the server interface, click on the following icon in the toolbar of the OPC UA server interface editor:

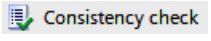


Figure 3-199 "Consistency check" button

Export interface

You have the option of exporting the OPC UA server interface as an XML file. This XML file contains all data type definitions referenced by the server interface.

To export the OPC UA server interface, click on the following icon in the toolbar of the OPC UA server interface editor:

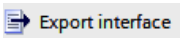


Figure 3-200 "Export interface" button

11.3.4.4 Creating a user-defined server interface

Introduction

The description is based on the following example:

A protective fence surrounds the production cell "Cell_1". The fence is equipped with the gate "Gate_1".

An S7-1500 CPU controls the entire production cell and also controls access through Gate_1.

A robot packs drugs into boxes in the production cell and then stacks the boxes on pallets.

Self-driving vehicles for automated material transport move the pallets to the central warehouse, thereby passing through Gate_1.

The CPU publishes a server interface via which the driverless transport systems arrange for Gate_1 to open.

The server interface contains the server method "smOpenGate" for opening the gate and the tag "Gate_1_State" which indicates the status of the gate (open or closed).

Creating a user-defined server interface

To create a server interface, follow these steps:

1. Select the CPU that you have used and configured as OPC UA server.
2. Click "OPC UA communication > Server interfaces".
3. Double-click "Add new server interface".
   STEP 7 displays the following dialog.

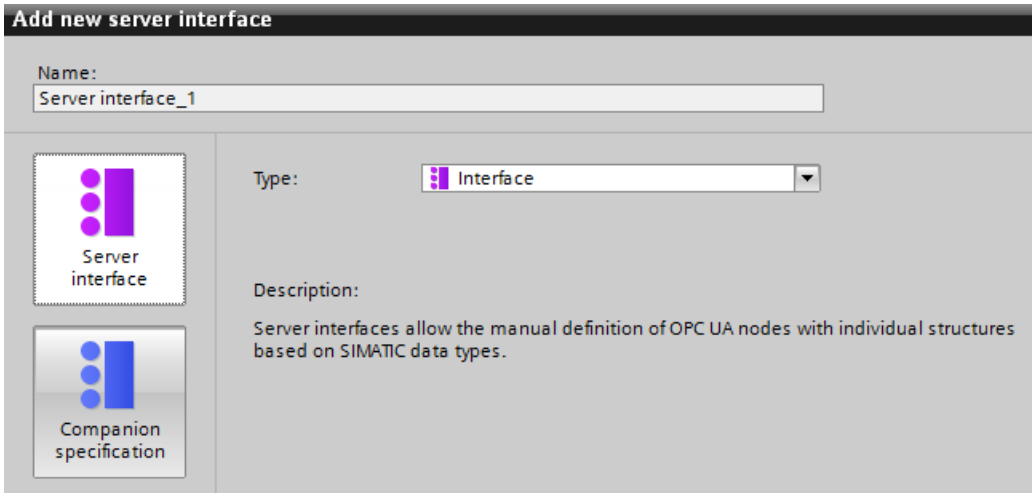


Figure 3-201 Adding the server interface

4. Change the name of the new server interface so that it is descriptive in your project.
   In the example, change the name "Server-interface_1" suggested by STEP 7 to "Cell_1".
5. Click "Server interface" and then "OK".
6. Click on the triangle in front of "Program blocks" in the area "OPC UA elements" to open the "Program blocks" folder.
   STEP 7 displays the following table for editing:

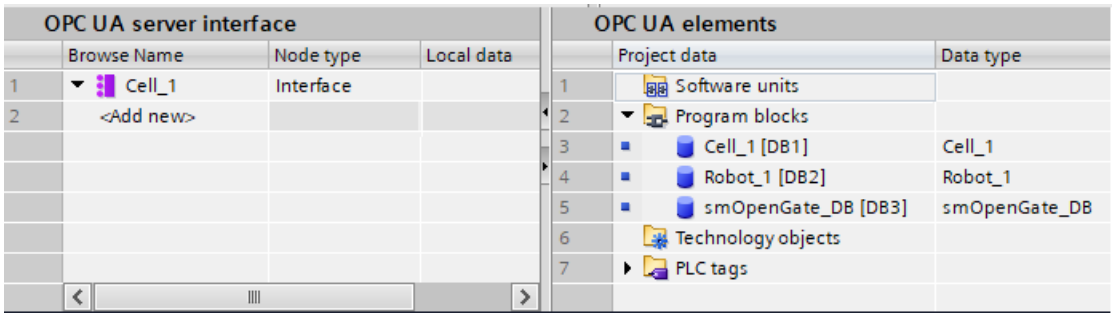


Figure 3-202 Editing the server interface

The editor is divided into two areas.

- **OPC UA server interface**
  On the left is the root node of the server interface "Cell_1".
  This interface is currently still empty: No OPC UA elements have been added to the server interface yet.
- **OPC UA elements**
  On the right are the OPC UA elements.
  OPC UA elements are objects that have been created so far in the STEP 7 project and have the property "Accessible from HMI/OPC UA".
  You can add the OPC UA elements to the new server interface "Cell_1".

7. Drag the OPC UA elements into the "<Add new>" line of the new server interface.

NOTE
The following applies in general: If you store data blocks or technology objects in the left area of the table, STEP 7 (TIA Portal) creates an object in the server interface. The elements of the data blocks are arranged as separate nodes below this.
If you store structures in the left area of the table, STEP 7 creates a node for the structure as a whole and nodes for each element of the structure.
The same applies to arrays: Again, STEP 7 creates a node for the array as a whole and nodes for each element of the array.
When you place a method in the left area of the table, STEP 7 creates a single node; the arguments of the inserted method are displayed for information purposes.

In the example, you drag the "Gate_1_State" tag from the right area to the left area to "<Add new>".
Then, drag the server method into the left area.
This server method is located within the "smOpenGate_DB [DB3]" data block in the right area.
STEP 7 (TIA Portal) displays the dialog as follows:

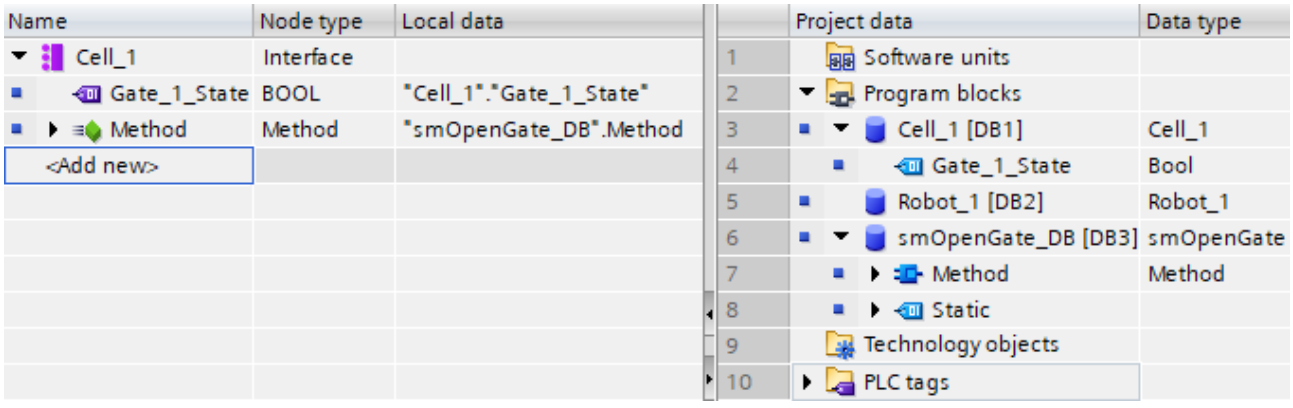


Figure 3-203 Adding OPC UA elements to the server interface

NOTICE
Checking the mapping of CPU local data on nodes of the OPC UA server interface When invalid assignments (mappings) exist in the server interface, they can result in incorrect read and write operations. Check the assignments and run a consistency check. Since the TIA Portal only generates warnings and not errors for invalid assignments, you can proceed step-by-step as follows: For example, in the first step, you can modify the program/local data so that the program runs without errors. The next step is to modify the OPC UA server interface and eliminate the inconsistencies. At the points at which the TIA Portal generates warnings, the OPC UA server interface does not function during runtime. The OPC UA server generates runtime errors.

Limiting the view to OPC UA servers

By selecting the OPC UA elements, you limit the view to the OPC UA server and the options of the OPC UA clients.

In the server interface of the example, the "Robot_1" data block is missing because industrial trucks do not need access to the server methods and tags of the robot.

In this case, it is best to disable the standard server interface (SIMATIC namespace) in the OPC UA properties of the S7-1500 CPU so that the filtered nodes cannot be accessed any other way.

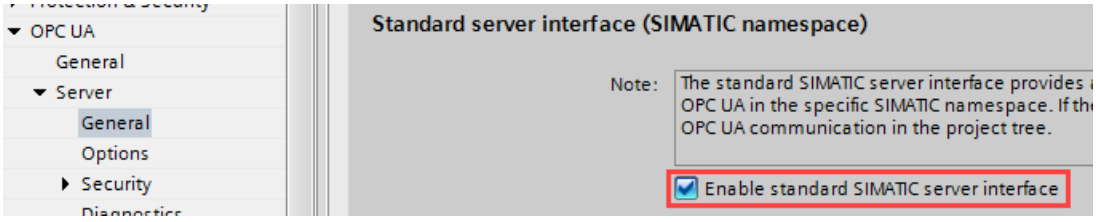


Figure 3-204 Disabling the standard server interface

You can also disable the visibility of each configured OPC UA server interface in the properties of the server interface and thus prevent that this server interface can be used by clients during operation.

- To do this, select the server interface and right-click on the "Properties" command.

This option lets you define multiple server interfaces centrally, for example, and enable and download only the required server interface.

Once a server interface has been defined, you can drag it to another CPU in the project tree.

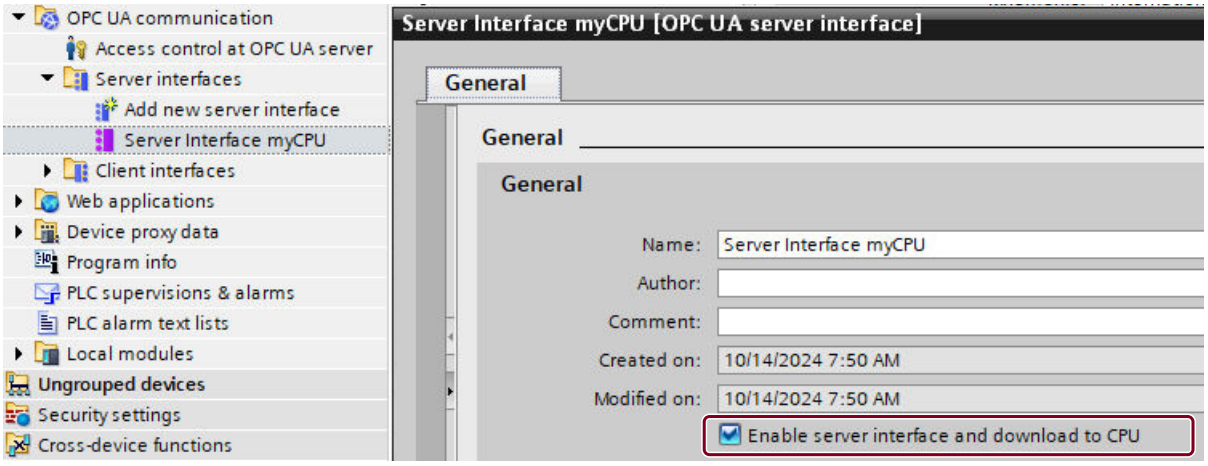


Figure 3-205 Disabling the visibility of the server interface

Information on the server interface

The "OPC UA Server Interface" editor is structured as a table and provides the following information:

Note that not all columns are displayed initially. You determine what is displayed by right-clicking on the header line of the table.

When a row is selected, you can display the OPC UA attributes of the node in the Inspector window ("OPC UA attributes" area), such as node ID, node class, node type, and description.

- **BrowseName**

  The language neutral name of the user-defined server interface is at the top (BrowseName). This name can be freely selected.

  The names (BrowseNames) of the individual OPC UA nodes that have been added to the server interface are under the name of the interface.

  You cannot change the name of an OPC UA node in this dialog. The names come from the STEP 7 project.

  You can delete an OPC UA node from the table. This means that it no longer belongs to the server interface and is no longer visible to OPC UA clients.

- **DisplayName**

  Similar to BrowseName. However, the name can be translated and is displayed, if available, in the corresponding language.

- **Node ID**

  NodeId of the OPC UA node, e.g. http://Server-Node_1; i=1

- **Node type**

  Type of the OPC UA node, for example BOOL, BYTE, INT.

  These node types were defined by Siemens, not by the OPC Foundation. For example, the OPC Foundation uses the Boolean node type for BOOL. BOOL is directly derived from Boolean.

The specified node type cannot be changed in this dialog: If you want to use a different node type, you must change the type of the respective PLC tags in the STEP 7 project.

- **Data type**
  The SIMATIC data type used in the STEP 7 project is specified, for example, Bool, Byte, Int. etc.
- **Access level**
  - If an OPC UA node is a tag (UAVariable type), the node can only be readable (RD) or readable and writable (RD/WR).
  - If an OPC UA node is a method (UAMethod type), this node can always be called.
- **Local data**
  The SIMATIC data type of the data block in the CPU, from which the value of an OPC UA node (UAVariable type) is read, or to which a value is written.

Generate local data

You have the option of generating local data for all or for selected nodes of the server interface that are not already assigned ("mapped") to local data of the CPU. The newly created local data are mapped automatically.

You trigger the automatic generation of local data by clicking the "Generate local data" button (all nodes that are not already mapped) or by selecting individual nodes and then clicking the "Generate local data" shortcut menu.

"Generate local data" button:

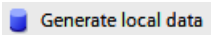


Figure 3-206 "Generate local data" button:

You can only generate nodes that can be mapped to local data, which means no objects, no folders, no methods or input/output arguments of methods.

After you have clicked the button or selected the shortcut menu, you must select in the follow-up dialog box whether the local data should be created in a new DB or in an existing DB.

Consistency check

You have the option to check the consistency of the server interface.

During the consistency check, STEP 7 checks whether the OPC UA nodes of the server interface are each assigned to a suitable OPC UA element (identical data type) or whether the used element still exists in the CPU.

To check the consistency of the server interface, click on the following icon in the toolbar of the OPC UA server interface editor:



Figure 3-207 "Consistency check" button

Export interface

You have the option of exporting the OPC UA server interface as an XML file. This XML file contains all data type definitions referenced by the server interface.

To export the OPC UA server interface, click on the following icon in the toolbar of the OPC UA server interface editor:

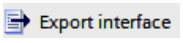


Figure 3-208 "Export interface" button

More information

You can find information on master copies for the OPC UA communication in the section Master copies for OPC UA communication (Page 382).

See also

Client accesses and local accesses to the OPC UA server (Page 231)

11.3.4.5 Data types for companion specifications

Mapping of data types

The table below shows the compatible SIMATIC data type for each OPC UA data type.

Assign the data types as shown below (SIMATIC data type - OPC UA data type). Other assignments are not permitted. STEP 7 does not check the observance of this rule and does not prevent an incorrect assignment. You are responsible for the rule-compliant selection and assignment of the data types.

You can also use the listed data types, for example, as elements of structures/UDTs for input and output parameters of self-created server methods (UAMethod_InParameters and UAMethod_OutParameters).

Table 3-27 Mapping of data types

SIMATIC data type	OPC UA data type
BOOL	Boolean
SINT	SByte
INT	Int16
DINT	Int32
LINT	Int64
USINT	Byte
UINT	UInt16
UDINT	UInt32
ULINT	UInt64
REAL	Float
LREAL	Double
LDT	DateTime
WSTRING	String

SIMATIC data type	OPC UA data type
DINT	Enumeration (Encoding Int32) and all derived data types
User-defined data type required (UDT, user-defined data type) The user-defined data type must be created with the prefix "Union_", for example "Union_MyDatatype". See example below the table. The first element (Selector) in this UDT must have the data type "UDINT".	UNION and all derived data types
See LocalizedText and ByteString data types (Page 290)	LocalizedText ByteString

User-defined data type for UNION required

The figure below shows the tag "MyVariable", which has the "Union_MyDatatype" data type.

This SIMATIC data type corresponds to an OPC UA tag with the data type UNION.

The figure shows an example of the declaration: When Selector = 1, Union takes a ByteArray; when Selector = 2, Union takes a WString.

Name	Data type
Static	
Selector	UDInt
ByteArray	Array[0..1] of Byte
WString	WString[42]

11.3.4.6 LocalizedText and ByteString data types

As of TIA Portal version V17 and S7-1500 CPU firmware version V2.9, the two OPC UA Built-in data types "LocalizedText" and "ByteString" are available for mapping to corresponding SIMATIC data structures. For the definition of these OPC UA data types, see also OPC 10000-3 DataType definitions.

These data types are used in companion specifications, for example, and can be easily handled by the user program with the OPC UA interface editor.

LocalizedText

A structure containing a string with locale identifier (e.g. 'en-US').

The structure has three elements with a defined order and the following structure in SIMATIC:

- **Encoding** (data type OPC_UA_LocalizedTextEncodingMask): Indicates in bit 0 whether the "Locale" field has a content and in bit 1 whether the "Text" field has a content. Both fields should have a content. We therefore recommend setting the "Encoding" value for SIMATIC to 2#00000011.
- **Local** (WString data type): Locale, for example, 'en-US'.
- **Text** (WString data type): Text box, for example, 'Text'.

ByteString

A sequence of octets.

The structure is built up as follows:

- **ActualLength** (data type "OPC_UA_ByteStringActualLength"): Length of the ByteString array that is filled
- **ByteString** ("Array of Byte" data type): Byte array

Requirement

An OPC UA server interface has been created.

Application

You can import a companion specification or a reference namespace that contains definitions of the "LocalizedText" or "ByteString" type.

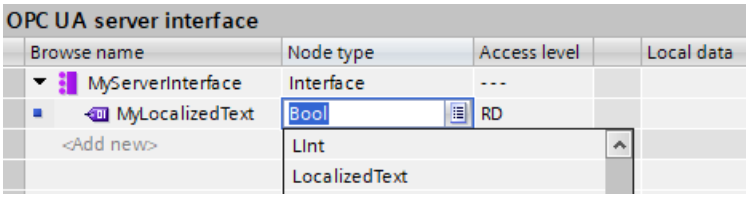
Likewise, you can create a server interface and define an address model yourself with the data types "LocalizedText" or "ByteString". The procedure is described in the next section.

Procedure

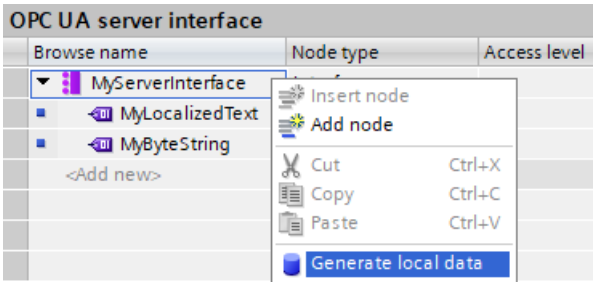
You will learn how to create a node of the type "LocalizedText" or "ByteString" with the interface editor and then have a SIMATIC data structure created automatically for this node in the paragraphs below.

To define OPC UA nodes of the type "Localized Text"/"ByteString" in a server interface, follow these steps:

1. Create nodes of the type "LocalizedText" or "ByteString" in the "OPC UA server interface" area. These node types are included in the list of selectable node types.



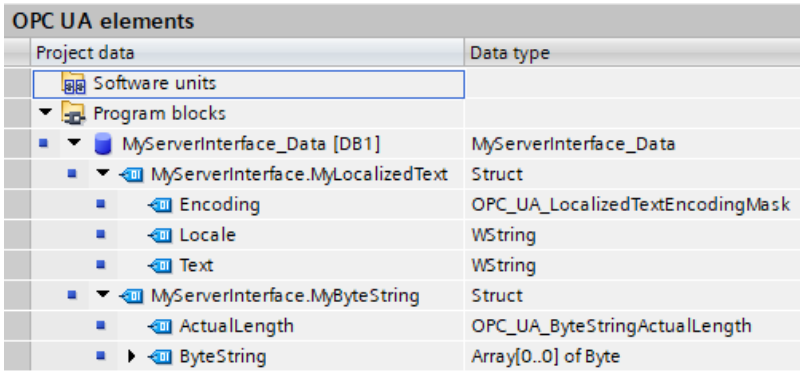
2. Select the "Generate local data" command from the shortcut menu. To generate the local data, select a data block, for example, a new DB with the name "MyServerInterface_Data".



Result: STEP 7 generates the corresponding structure for the mapping in which you still need to adjust the required text length (Text) and the required locale (Locale) for "LocalizedText".

The same is true for "ByteString"; in this case, you must adjust the length and the array.

The consistency check generates a warning to indicate the required adjustments.



Rules

- You can also create UDTs with the structure as shown above for the node types "LocalizedText" or "ByteString" and use them for DB elements.
- You can use the node types "LocalizedText" or "ByteString" in other structures (nests).
- The SIMATIC structures for "LocalizedText" or "ByteString" may only be used completely; an isolated data type, such as "OPC_UA_LocalizedTextEncodingMask" for other purposes, is not provided.
- Input and output parameters of methods can also be of the data type/node type "LocalizedText" or "ByteString".

11.3.4.7 Using additional OPC UA data types for companion specifications

Apart from the OPC UA data types listed in the section "Mapping of data types" and their correspondences on the SIMATIC side, there are the following OPC UA basic data types which you can also use:

- OpcUa_NodeId
- OpcUa_QualifiedName
- OpcUa_Guid
- OpcUa_XmlElement
- OpcUa_ByteString (Page 290)
- OpcUa_LocalizedText (Page 290)

Requirement for the use of the basic data types listed above as variables in the application program: The basic data types have to exist as complex data types that are structured exactly like the corresponding OPC UA basic data types.

- OpcUa_NodeId and OpcUa_QualifiedName exist as system data types; that's why you can use these data types not only for single variables but also as elements of a structure.
- For the basic data types or built-in data types GUID and XmlElement you have to create a PLC data type in accordance with the OPC UA specification and subsequently use it as an element in a structure so that the data types of the elements can be resolved. What each PLC data type must look like is described below for every single basic data type.

- For OpcUa_ByteString and OpcUa_LocalizedText, the requirements have been created in TIA Portal V17 to simply use these data types in the server interface of the "Companion Specification" type:
  - You create the corresponding node type in the server interface (for example, OpcUa_LocalizedText)
  - You click on "Generate local data"

  STEP 7 then automatically generates the appropriate data structures in a DB.
- For OpcUa_Guid, these requirements have been met in TIA Portal V19. Proceed as described in the previous section.

System data type "OPC_UA_NodeId"

For the OPC UA basic data type "OpcUa_NodeId", please refer to the following table for the meaning of the parameters. Use OPC_UA_NodeId for the identification of a node in the OPC UA server.

Parameter	S7 data type	Meaning
NamespaceIndex	UINT	Namespace index of the node in the OPC UA server. A node can, for example, be a tag.
Identifier	WSTRING[254]	The designation of the node (object or tag) depends on the identifier type: • Numeric identifier: The node is labeled with a number, for example "12345678". • String identifier: The node is labeled with a name, for example "MyTag". No distinction is made between upper and lower case.
IdentifierType	UDINT	Type of identifier • 0: Numeric identifier • 1: String identifier • 2: GUID • 3: Opaque

System data type "OPC_UA_QualifiedName"

See the following table for the structure of the system data type "OPC_UA_QualifiedName":

Name	S7 data type	Meaning
NamespaceIndex	UINT	The namespace index of the name.
Name	WSTRING[64]	Name of the node or tag.

System data type "GUID"

The "Guid" data type is available as a node type as of TIA Portal V19. For the definition of this OPC UA data type, see also OPC 10000-6 mappings.

The figure shows the assignment of the "Guid" data type for a tag node in a server interface.

The next figure shows the data block with the GUID elements that is created automatically with "General local data".

OPC UA server interface

Browse name	Node type	Access level	Local data	Data type
myServerInterface	Interface	---		
GUID-1	Guid	RD	"myServerInterface_Data"."myServerInterface.GUID-1"	GUID

Figure 3-209 GUID node in the server interface

The next figure shows the data block with the GUID elements that is created automatically with "General local data".

Name	Data type	Start value
Static		
myServerInterface.GUID-1	GUID	
Data1	UDInt	16#C4965784
Data2	UInt	16#0DFE
Data3	UInt	16#4B8F
Data4	Array[0..7] of Byte	
Data4[0]	Byte	16#87
Data4[1]	Byte	16#0A
Data4[2]	Byte	16#74
Data4[3]	Byte	16#52
Data4[4]	Byte	16#38
Data4[5]	Byte	16#C6
Data4[6]	Byte	16#AE
Data4[7]	Byte	16#AE

Figure 3-210 Data block with SDT GUID

UDT for basic data type XmlElement

An XmlElement is a serialized XML fragment (UTF-8 string).

For the basic data type "XmlElement", create the following PLC data type:

XmlElement

	Name	Data type	Default value
1	XmlElement	WString	WSTRING#''

11.3.4.8 Dynamic arrays

Useful information on dynamic arrays

As of TIA Portal V19 and S7-1500 CPU FW version V3.1, you can use so-called "dynamic arrays" for your OPC UA server and OPC UA client interfaces. The following description explains the principle and functionality of the server interface. The structure of the structure/UDT for a dynamic array is identical for client and server applications.

With dynamic arrays, it is possible to define data structures whose number of elements can be changed at runtime on the server interface side. On the CPU side, the dynamic array is mapped to a fixed-size structure.

Example: Process data from production for quality assurance purposes is transferred to a higher-level management system. The number of process data elements is different, depending on the product type. If the product type is changed during runtime, the number of process data elements needed also changes.

In STEP 7 (TIA Portal), an array is a data type that you can assign to a tag. An array represents a data structure that consists of a fixed number of components of the same data type. All data types except ARRAY are permitted for the components.

By contrast, OPC UA does not define an array as a data type. Any variable value (Value) can be an array. The following attributes and properties of Variable NodeClass are used in OPC UA to define how a variable is structured with respect to its "geometry" as an array (excerpt from https://reference.opcfoundation.org/Core/Part3/v104/docs/5.6):

Attribute / Property	Data type	Possible values, meaning
ValueRank (Mandatory)	Int32	• n > 1: Value is an array with dimension n. • 1: Value is an array with one dimension • 0: Value is an array with one or more dimensions • -1: Value is a scalar (not an array) • -2: Value is a scalar or an array with any number of dimensions • -3: Value can be a scalar or a one-dimensional array
ArrayDimensions (Optional)	UInt32[]	Maximum supported length of each dimension. 0 or empty: Unknown length.
MaxArrayLength (Optional)	UInt32	For DataVariables with ValueRank attribute not set to scalar: Maximum length of the array. Example: A three-dimensional array with lengths 2x3x10 has the length 60.

The name "dynamic array" is used here to establish a counterpart on the SIMATIC data type end for the dynamics of the variable geometry defined in OPC UA, so that mapping of array data is possible. You can change the geometry of a mapped array during runtime using your STEP 7 program. On the OPC UA end, you define a node in the OPC UA server interface via which a client can access the mapped CPU data (the dynamic array).

Principle

In order for OPC UA variables to be mapped to CPU tags of Array type, you use a structure or UDT with the new system data type "OPC_UA_ArrayBoundaries".

The structure or UDT has the following structure elements and is structured as follows:

- The first structure element (array size) is itself an array and defines the current size of the dynamic array. The system data type "OPC_UA_ArrayBoundaries" defines the index range available in the server interface for each dimension (with lower and higher boundary elements in each case).
- The second structure element (array data) contains all array elements with a selectable data type permitted for OPC UA.

STEP 7 (TIA Portal) automatically ensures that, for example, negative indexes on the SIMATIC end are converted to non-negative indexes (starting at "0") on the OPC UA end (server interface).

Example of one-dimensional array

The following example shows the structure for a simple, one-dimensional array with a maximum of 10 elements. The current size of the array is set to 3 elements [0..2].

Name	Data type	Possible values / Description
1-Dim-Struct	Struct (UDT)	
- **ArraySizeAct**	Array [0..0] of OPC_UA_ArrayBoundaries	**Current array size**
- - ArraySizeAct[0]	OPC_UA_Boundaries	One dimension
- - - Lower	DInt	0 (lower index)
- - - Upper	DInt	2 (possible upper index values: 0..9)
- **MyDataArray**	Array[**0**..9] of Byte	**Array data (all array elements)**
- - MyDataArray[0]	Byte	First element
...	...	...
- - MyDataArray[9]	Byte	Last element

Example of two-dimensional array

The following example shows the structure for a two-dimensional array with 10x6 = 60 elements. The lower indexes of both dimensions are not "0" in this case. The current size of the array is set to 2x6 = 12 elements.

Name	Data type	Possible values / Description
2-Dim-Struct	Struct (UDT)	
- **ArraySizeAct**	Array [0..1] of OPC_UA_ArrayBoundaries	**Current array size**
- - ArraySizeAct[0]	OPC_UA_Boundaries	First dimension
- - - Lower	DInt	**-9** (lower index)

Name	Data type	Possible values / Description
- - - Upper	DInt	-8 (possible upper index values: -9..0)
- - ArraySizeAct[1]	OPC_UA_Boundaries	Second dimension
- - - Lower	DInt	**5** (lower index)
- - - Upper	DInt	10 (possible upper index values: 5..10)
- **MyDataArray**	Array[-**9**..0, **5**..10] of Byte	**Array data (all array elements)**
- - MyDataArray[-9,5]	Byte	First element
- - MyDataArray[-9,6]	Byte	Second element
...	...	...
- - MyDataArray[0,9]	Byte	Second to last element
- - MyDataArray[0,10]	Byte	Last element

Effects on the server interface

Appearance in the server interface: If you drag a dynamic array (e.g. 2-Dim-Struct) and drop it onto the server interface in the editor for the server interface, STEP 7 (TIA Portal) creates a node of the same name without the subelements. The node indicates type "ARRAY" in the "Node type" column with the maximum possible lengths of the array.

Browse: The dynamic array is available as a node in the OPC UA address space. Unlike for static arrays, the subelements of the array are not visible as child nodes.

Read: The dynamic array can be read with the Read service. The client can specify whether it wants to read the entire array or only parts of it (IndexRange). Only the read parts that lie within the boundaries of the current array range return the status "Good". If the array size is "0" in every dimension, an empty array is returned with status "Good".
If an array of size "0" is read in a dimension, then an empty array with status "Good" is returned.

Write: If the range to be written is less than or equal to the maximum array size, all elements are written (status "Good"). If the range to be written is greater than the maximum array size, nothing is written and status 8074_0000 is returned (OpcUa_BadTypeMismatch). If part of an array is written (IndexRange), the behavior is exactly the same: All dimensions of the array range to be written must lie completely within the maximum array size. Only then is the data written and the status "Good" returned.
If an array of size "0" is written in at least one dimension, then this value is set correctly in the CPU data. The elements "Lower" and "Upper" in the corresponding OPC_UA_ArrayBoundaries structure are adjusted accordingly ("Upper" = "Lower-1").

Rules and specific features

- You can also use dynamic arrays for input parameters and output parameters in methods.
- Avoid inconsistencies caused by changing the current size of the array while a client is accessing the array. The result of the access is undefined in this case.
  Use the uninterruptible instruction UMOVE_BLK for changing the current array size.

- In contrast to the SIMATIC data type Array, there can be "empty" arrays in OPC UA. You define an array with 0 elements in one dimension with OPC_UA_ArrayBoundaries by setting the highest index value (Upper) less than the lowest index value (Lower), e.g. with the following values: Upper = Lower-1.

  If you define a multidimensional array in the server interface (or client interface) and at least one dimension is "0" (empty), then by definition it is an empty array (all dimensions are 0).
- The values for the current array size and the values for the array data must be consistent. Otherwise, error code 803A_0000 (OpcUa_BadNotReadable) is output.
  - The values you set for "Lower" for the current array size in a dimension must also be set as the lower index value in the range of the array data in the corresponding dimension.
  - The values you have set for "Upper" for the current array size for a dimension must also lie within the range of the array data for this dimension.
- If an OPC UA client writes a dynamic array in the server, the client must write an array with the same dimension (ValueRank). Otherwise, the status 8074_0000 is returned (OpcUa_BadTypeMismatch).

11.3.4.9 Rules for OPC UA XML files

Importing exported OPC UA XML files to an S7-1500 CPU

Please note the following information when importing server interfaces that come from the OPC UA XML export of an S7-1500.

NOTE

Import blocked for namespace "http://www.siemens.com/simatic-s7-opcua"
You cannot import server interfaces with the namespace "http://www.siemens.com/simatic-s7-opcua" to an S7-1500 CPU because this namespace is reserved for S7-1500 CPUs (standard SIMATIC server interface) and is not available for imports.
If you want to import a server interface with the namespace "http://www.siemens.com/simatic-s7-opcua", open the server interface to be imported (OPC UA XML file) and change the namespace in the relevant places. The file thus changed can then be imported.

Integrity of the OPC UA XML files

OPC UA XML files represent the server address space. These files are, for example, imported by you in the context of OPC UA Companion specifications as a server interface after adaptation to the application, loaded into the S7-1500 CPU and tested.

⚠ WARNING

No checking of imported OPC UA XML files
Protect these OPC UA XML files against unauthorized manipulation since STEP 7 does not check the integrity of these files.

Recommendation
To minimize risks in the case of an extension or adaptation of the server address space, follow these steps:

1. Protect the project (project navigation: Security settings > Settings).
2. Export the corresponding server interface before the extension or adaptation.
3. Revise this OPC UA XML file.
4. Import the file again as a server interface.

11.3.4.10 Creating a server interface for reference namespace

Companion specifications and referenced namespaces

A series of OPC UA object types (as well as additional definitions) are defined in a companion specification. These object types are each defined in namespaces so that the names of the object types (type definitions) are unique.

To use a companion specification in your project, create instances of object types of this companion specification.

To do this the object definitions must be available in your STEP 7 project. If this is not the case, you must import the object definitions. To import all definitions of a namespace, create a server interface of type "Reference namespace" for each namespace in STEP 7.

NOTE

EUROMAP and the OPC Foundation have established the Joint Working Group "OPC UA Plastics and Rubber Machinery".
The existing EUROMAP recommendations EUROMAP 77 (data exchange between injection moulding machines and MES), 82.1 (temperature control devices) und 83 (general definitions) were published under the neutral umbrella of the OPC Foundation as OPC 40077, 40082-1 and 40083. However, the examples listed below use the previously valid designations and references.

Example Euromap 77 (currently OPC 40077)

You have added a server interface for the companion specification Euromap 77 (currently OPC 40077).

The server interface uses object types defined in OPC UA DI as well as in Euromap 83 and Euromap 77 in their corresponding namespaces.

Therefore, in addition to the server interface Euromap 77 of the "Companion Specification" type, create additional server interfaces of "Reference namespace" type in STEP 7, in each case for the following namespaces:

- http://opcfoundation.org/UA/DI/
- http://www.euromap.org/euromap83/
- http://www.euromap.org/euromap77/

The following description shows you how to proceed.

Creating a server interface for a reference namespace

To create a server interface for a namespace, proceed as follows:

1. Select the CPU that you want to use as an OPC UA server.
2. Click "OPC UA communication > Server interfaces".
3. Double-click "Add new server interface".
   STEP 7 (TIA) now displays the dialog "Add new server interface".
   A general name for the new server interface is entered in the dialog, for example "Server_Interface_1".
4. Assign a descriptive name for the new server interface.
   In the example, select the name "OPC.Ua.Di" or a similar name that clearly references the namespace "http://opcfoundation.org/UA/DI/".
   This namespace must be imported first. It contains basic definitions (for example, the UAObjectType "DeviceType").
5. Click the "Companion specification" button and select the "Reference namespace" type.
6. Click the three dots next to the "Import XML file" field.
7. Select an XML file that contains the definitions of the namespace "http://opcfoundation.org/UA/DI/".
   Select the file "Opc.Ua.Di.NodeSet2.xml" in the example. You can download this file here:
   Opc.Ua.Di.NodeSet2.xml (https://opcfoundation.org/UA/schemas/DI/)
   Note: If the file cannot be imported, this may be because the OPC UA ("CORE") model version available in TIA Portal does not match the OPC UA for Devices ("DI") model version. In this case, select a different version of the DI model (for example a previous version).
   The figure below shows the dialog with the entries:

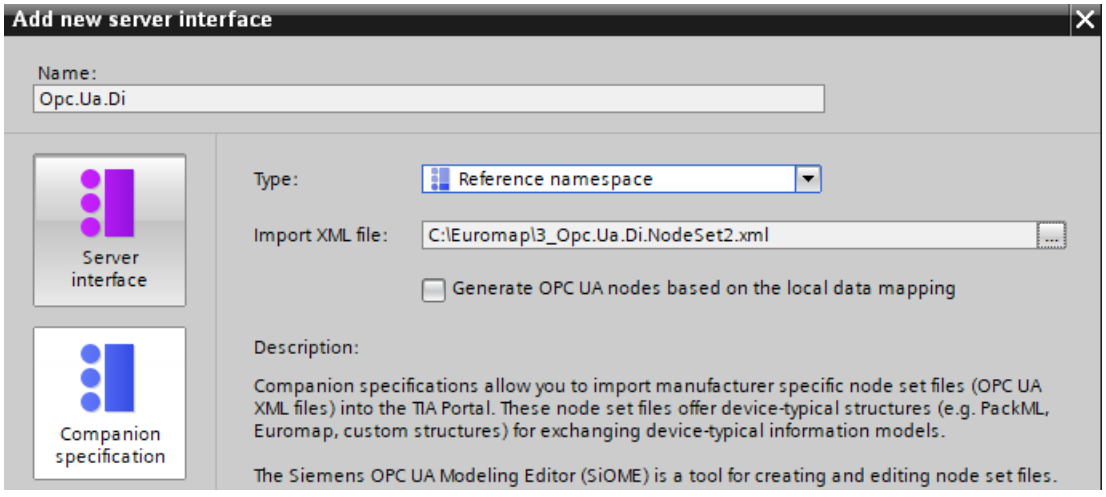


Figure 3-211 Adding a reference namespace

8. Click "OK".
   STEP 7 (TIA) now generates the new server interface.

You can find the server interface in the project tree of STEP 7 (TIA Portal) under "OPC UA Communication > Server interfaces > Reference namespace".

If a companion specification uses additional namespaces, add a new server interface for each namespace.

Add additional server interfaces for Euromap77
For Euromap 77, you still need the following namespaces:

- http://www.euromap.org/euromap83/
- http://www.euromap.org/euromap77/

First, add a server interface for the namespace "http://www.euromap.org/euromap83/".

This namespace contains basic definitions for Euromap 77, therefore it is required here first. All definitions of this namespace are included in the XML file "Opc_Ua.EUROMAP83NodeSet2.xml", which you can download from the Euromap website (https://www.euromap.org/en/euromap83).

Then add a server interface for the namespace "http://www.euromap.org/euromap77". All definitions of this namespace are included in the XML file "Opc_Ua.EUROMAP77.NodeSet2.xml", which you can also download from the Euromap website (https://www.euromap.org/en/euromap77).

11.3.4.11 Generating OPC UA nodes based on local data mappings of FB types and UDTs

If you want to make instance data from FBs or UDTs of the CPU accessible to OPC UA clients you can, as of TIA Portal version V17, have these instance data assignments automatically made.

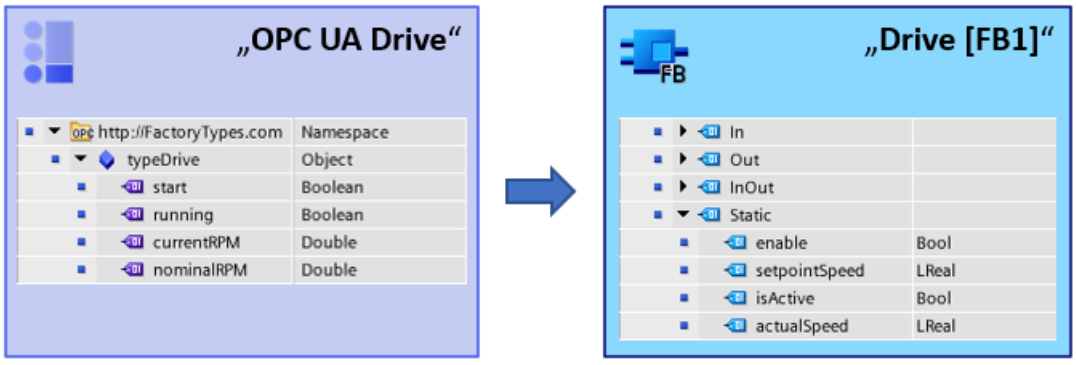
You only have to map the FB types or the UDTs to suitable OPC UA data types of imported reference namespaces. Based on these mappings, STEP 7 (TIA Portal) then generates the required nodes in the server interface for each FB instance or for each UDT usage during compilation.

If you extend your program and add more FB instances or UDT usages, or if you add existing instances delete, you do not need to worry about adapting the server interface: STEP 7 automatically adjusts the server interface when compiling the program.

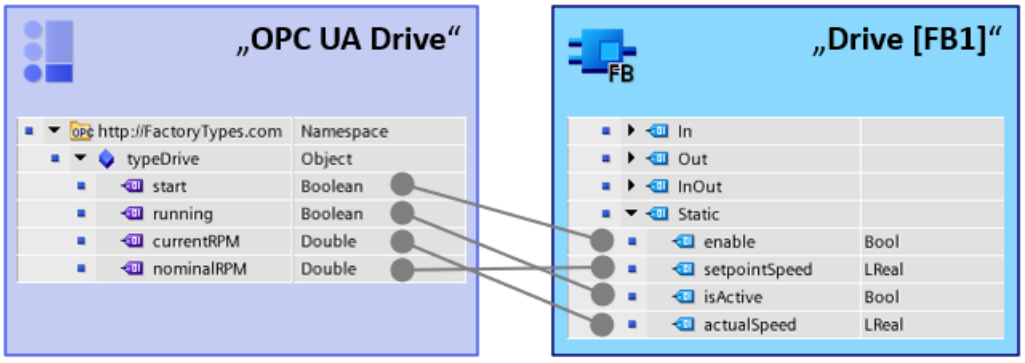
Example

- You create a function block (FB) in the user program of the CPU and define in the "Static" area of the interface of the FB the parameters that form the "memory" of the FB. The instances (values) of this parameter are to be accessible for OPC UA clients.
- You create an OPC UA data type (e.g. with SiOME) with elements that correspond to the data type the parameters in the static area of interface of the FB. The order of the elements does not matter. Then import the reference node set file (reference namespace) as a reference name space.

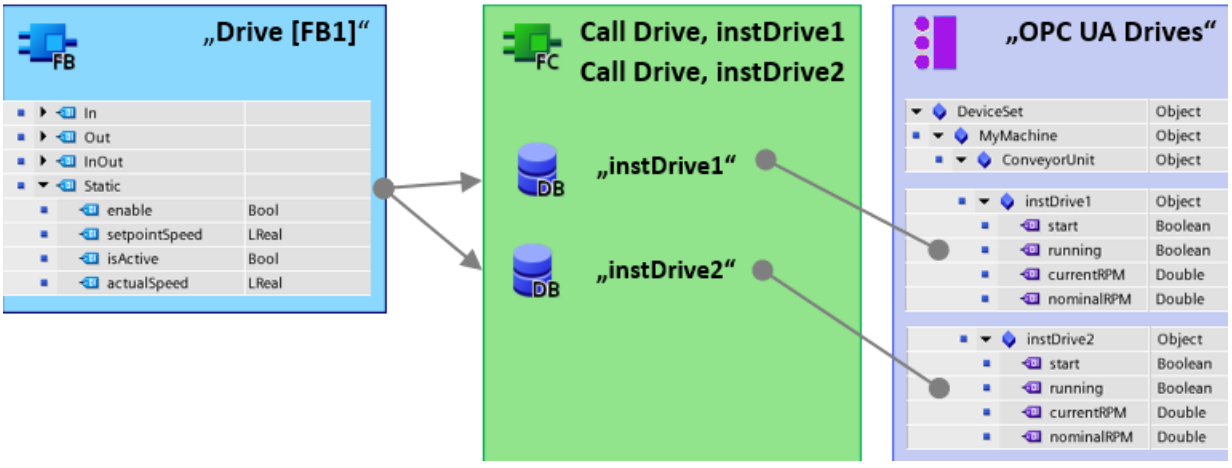
The following figure shows the assignment of elements as comparison of the reference namespace view (server interface) and the OPC UA elements view (program).



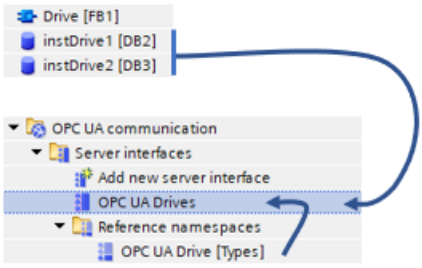
Mapping of data types (FB interface - OPC UA interface): Principle
The following figure shows the assignment of the elements from the user program of the CPU to the elements of the OPC UA server interface. The order of the elements does not have to match.



Automatic generation of the OPC UA server instances in the server interface: Principle
The figure below shows the compilation of the project. The instances of the user program are also generated in the server interface.



By mapping between FB type information / UDT type information and OPC UA type information, STEP 7 is able to create all instances present in the program as nodes in the server interface.



Rules

- Only the FB elements in the "Static" area of an FB interface can be mapped to OPC UA type descriptions.
- When mapping the data types, OPC UA elements from the same FB interface or from the same UDT must always be selected for an object. Mapping from different FBs or UDTs to an object is not permitted.

Requirement

- The FB types used, defined in the "Static" area of an FB, must be configured as "Accessible for OPC UA".
- The UDTs used must be configured as "Accessible for OPC UA".
- A nodeset file (XML file) is available with OPC UA data type definitions that match the FB types or UDTs defined in user program (can be mapped).
  Use the "SiOME" tool to create your node set file (Siemens Industry Online Support).
- The user program with the FB instances and UDT usages is available.

Procedure

To map a data type from a reference namespace to an FB type or UDT data type, follow these steps:

1. Select the CPU that you want to use as an OPC UA server.
2. Import the prepared node set file (XML file) with the type definitions as a reference namespace.
   - In the "Add new server interface" dialog, enable the option "Generate OPC UA nodes based on the local data mapping".

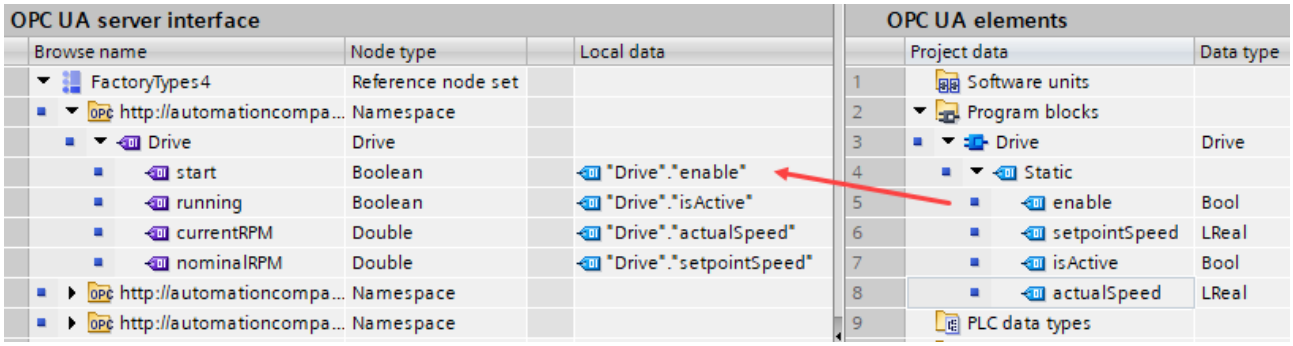
     Only when this option is enabled can you map FB types or UDTs by dragging them to the OPC UA type descriptions.

3. Double-click the icon for the server interface of the "Reference namespace" type that you just generated.

   The editor for mapping between OPC UA server interface and OPC UA elements opens. In the properties area of the editor, in the "Mapping of local data" area, the option "Generate OPC UA nodes based on the local data mapping" is enabled. If not, enable the option now.

   In the "Interface name" field, adapt the name of the server interface to be created. A new server interface of the "Companion specification" type with this name is created during the compile.

4. Assign the existing FB types or UDTs to the nodes of the server interface (reference namespace) by dragging the OPC UA element (right side of the editor) to the corresponding node of the server interface (reference namespace, "Local data" column).



5. Compile the project.

   After compilation, the newly generated nodes of the instances are located in the generated server interface of the "Companion specification" type. STEP 7 creates an object for each instance DB. The generated elements are located under each of these objects.

   Similarly, STEP 7 also creates an object for each global DB that is created when a UDT is instantiated.

   The generated companion specification interface cannot be changed (no longer possible: generating local data, importing companion specification). This measure provides protection against data loss in the event that the server interface was manually added and is then overwritten by a recompilation. Only the name of the generated companion specification interface can be modified.

   Furthermore, group folders that you have created to structure your data in the project tree of your TIA project are applied as "Folder" (node type) in the generated companion specification interface.

Create user program with FB types or UDT

How to create FBs and UDTs is not explained in detail here; for this purpose use the description for creating a user program, e.g. declare block interface and declare PLC data types (UDT).

Consistency check

The consistency check ("Consistency check" button of the editor) also checks the mapping of the data types and updates the display of the data types in the corresponding column of the editor.

Mapping FBs/UDTs to OPC UA type information

By mapping function blocks (FBs) or UDTs to suitable OPC UA data types / OPC UA object types from imported reference namespaces, TIA Portal can provide the following function when compiling:

For each FB instance (instance DB) and each UDT instance in global DBs or instance DBs, the TIA Portal generates the required OPC UA nodes in the generated companion specification during compiling based on the reference namespace.

A generated OPC UA node always has the same access level in the server interface that the corresponding FB/UDT has.

Example: If the FB (type)/UDT has the read and write access level, the created OPC UA node has the access level "RD/WR".

New as of TIA Portal V20

For certain use cases it may be required that the tag nodes within OPC UA object types determine the access level and this is not determined by UDTs or FBs.

As of TIA Portal V20, you can set the access level for tags within OPC UA object types (not within OPC UA data types!) in the reference namespace.

The nodes created in the server interface also have this access level then.

Requirement

- A server interface of the "Reference namespace" type was imported.
- In the reference namespace, the tag to be mapped (an instance declaration within an object type) is provided with the desired access level, e.g. "RD" for readable.

  The access level is visible in the "General" area in the properties of the selected UA tags.
- The program contains the corresponding OPC UA elements (UDTs, FBs), which can be mapped to UA tags below object types.

Procedure

The description of the procedure uses a UDT as an example. The same procedure applies to FBs (types).

To put the "AccessLevel" attribute of OPC UA tags into effect within object types for the generation of tags in a server interface, follow these steps:

1. Open the server interface of "Reference namespace" type.
2. Drag a UDT (under PLC data type) from the "OPC UA elements" area to the corresponding UA tag within a UA object type in the OPC UA server interface area ("Local data" column).
3. Compile the configuration.

The access levels that were set in the reference namespace apply to generated OPC UA nodes that are based on local data mapping.

Using string node IDs for generated nodes

For reference namespaces, as of TIA Portal version V20, you can specify whether the node ID should be generated as a string node ID in the generated server interface.

As of TIA Portal version V21, you can also activate string node IDs for server interfaces.

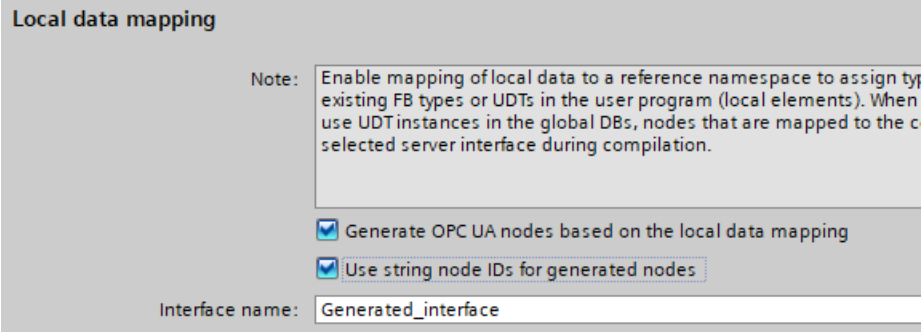


Figure 3-212 OPC UA local data mapping with string node IDs

11.3.4.12 Notes on configuration limits when using server interfaces

When you use OPC UA server interfaces, you must comply with limits for the following objects in line with the S7-1500 CPU performance class:

- Number of server interfaces
- Number of OPC UA nodes
- Load object data volume
- If you have implemented methods: Number of server methods or server method instances

Configuration limits for OPC UA server interfaces and methods

The configuration limits of the OPC UA server interfaces and the methods can be found in the technical specifications of the Equipment Manuals for the respective CPUs. Up-to-date technical specifications of the CPUs can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/td).

A violation of configuration limits results in an error message.

11.3.5 Providing methods on the OPC UA server

11.3.5.1 Useful information about server methods

Providing user program for server methods

On the OPC UA server of an S7-1500 CPU (as of firmware V2.5), you have the option of providing methods via your user program. These methods can be used by OPC UA clients, for example to start a manufacturing job using the method call of the S7-1500 CPU.

OPC UA methods, an implementation of "Remote Procedure Calls", provide an efficient mechanism for interactions between different communication nodes. The mechanism provides both job confirmation and feedback values so you no longer have to program handshaking mechanisms.

Using OPC UA methods, you can transfer data consistently without trigger bits/handshaking, for example, or trigger specific actions on the controller.

How does an OPC UA method work?
An OPC UA method in principle operates like a know-how protected function block that is called by an external OPC UA client in runtime.

The OPC UA client only "sees" the defined inputs and outputs. The content of the function block, the method or algorithm, remains hidden to the external OPC UA client. The OPC UA client receives feedback on successful execution and values returned by the function block (method), or an error message if execution has not been successful.

As the programmer, you have full control over and responsibility for the program context in which the OPC UA method runs.

Rules for programming a method and runtime behavior

- Make sure that the values returned by the OPC UA method are consistent with the input values provided by the OPC UA client.
- Follow the rules on assigning name and the structure of parameters, and the permitted data types (see description of the OPC UA server instructions).
- Behavior during runtime: The OPC UA server accepts **one** call per instance. The method instance is not available for other OPC UA clients until the call has been processed by the user program or has timed out.

The basic procedure for implementing a user program as a server method is set out below.

Implementing a server method
A program (function block) for implementing a server method is structured as follows:

1. **Querying the server method call with OPC_UA_ServerMethodPre**

   You first call the "OPC_UA_ServerMethodPre" instruction in your user program (i.e. in your server method).

   This instruction has the following tasks:

   – With this instruction you ask the OPC UA server of the CPU whether your server method was called from an OPC UA client.
   – If the method was called and the server method has input parameters, your server method now receives the input parameters.

     The input parameters of the server method come from the calling OPC UA client.

2. **Editing the server method**

   In this section of the server method, you provide the actual user program.

   You have the same options as in any other user program (for example, access to other function blocks or global data blocks).

   If the server method uses input parameters, these parameters are available to you.

   This section of the server method should only be executed if an OPC UA client has called the server method.

   After successful execution of the method, you set the output parameters of the server method if the method has output parameters.

3. **Responding to server method with OPC_UA_ServerMethodPost**

   To complete the server method, call the "OPC_UA_ServerMethodPost" instruction.

   Use the parameters to notify the "OPC_UA_ServerMethodPost" instruction whether or not the user program has been processed.

   If the user program has been successfully executed, the OPC UA server is notified via the relevant parameters. The OPC UA server then sends the output parameters of the server method to the OPC UA client.

Always call the instructions "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost" as a pair irrespective of whether the user program is processed by both instructions or continued in the next cycle.

You will find an example of a server method implementation in the STEP 7 online help.

Integrating the server method

The diagram below shows how an OPC UA client (A) calls the server method "Cool":

The CPU executes the instance "Cool1" of the server method "Cool" in the cyclic user program ⑥.

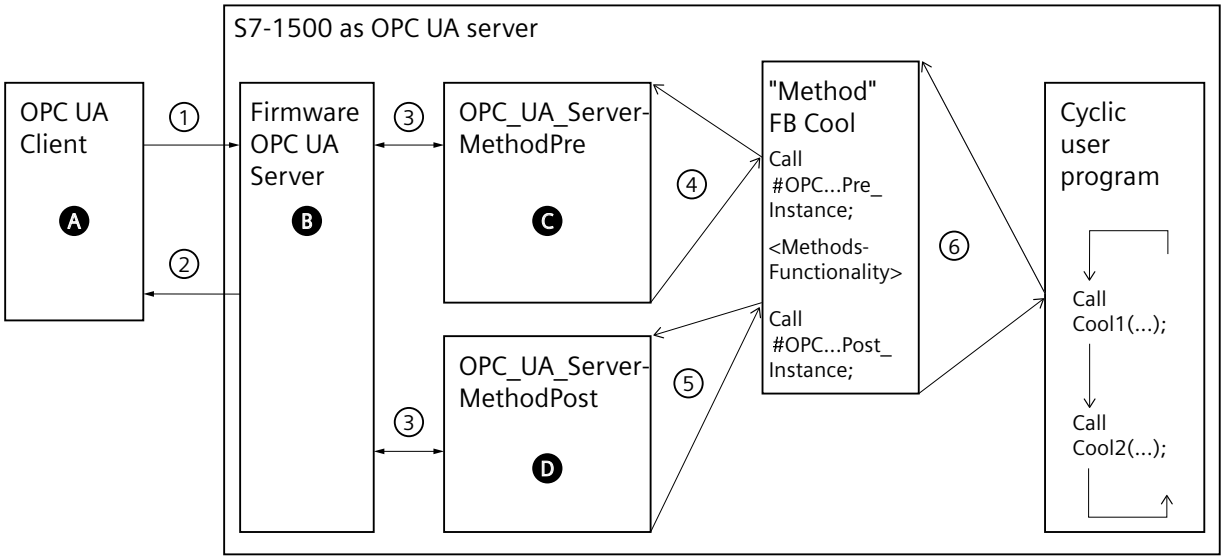
The CPU first uses the instruction "OPC_UA_ServerMethodPre" to query ④ whether an OPC UA client has called the server method "Cool" ①.

- If the server method has not been called, program execution returns directly to the cyclic user program over ④ and ⑥. The CPU resumes the cyclic user program after "Cool1".
- If the server method has been called, this information is returned to the server method "Cool" over ④. The actual functionality is now executed in the Cool server method, see"<Method Functionality>" in the graphic.

  The server method then uses the instruction "OPC_UA_ServerMethodPost" ⑤ to notify the firmware (B) that the instruction has been executed ③.

  The firmware returns this information over ② to the calling OPC UA client (A).

  The CPU resumes the cyclic user program after "Cool1".



A Call of the server method and management of the "Done" information (method complete)

① Asynchronous call of the server method

② Asynchronous "Done" information for the method called (method complete)

B Wait for OPC UA client calls, management of calls in the queue, forwarding of "Done" information from the cyclic user program to the OPC UA client

③ Data transfer from the OPC UA server to the method instances of the user program and vice versa

C Check whether method has been called.
If it has, forwarding of input data from the OPC UA server to the method instance of the user program and feedback to the method instance that the method has been called ("called")

④ Synchronous call of the instruction OPC_UA_ServerMethodPre as a multi-instance stating the storage area for the input data from the OPC UA server.
The return value indicates whether or not the method has been called by the OPC UA client.

⑤ Check whether the method has been completed or is still active ("busy").

D Check whether the method has been completed.
If it has, the output data of the method instance is forwarded to the OPC UA server and the method instance is notified that the method has been completed. The OPC UA server is notified.

⑥ Call of the method FB (in this case: FB Cool) with the required instance and the process parameters

Figure 3-213 Example: Calling the "Cool" server method

Information about server instructions

The "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost" are described in detail in the help to the Instructions > Communication > OPC UA > OPC UA server.

11.3.5.2 Boundary conditions for using server methods

Permitted data types

If you provide server methods, observe the following rule:

- Assign the data types as shown below (SIMATIC data type - OPC UA data type). Other assignments are not permitted.

STEP 7 does not check the observance of this rule and does not prevent an incorrect assignment. You are responsible for the rule-compliant selection and assignment of the data types.

You can also use the listed data types, for example, as elements of structures/arrays/UDTs for input and output parameters of self-created server methods (UAMethod_InParameters and UAMethod_OutParameters).

SIMATIC data type	OPC UA data type
BOOL	Boolean
SINT	SByte
INT	Int16
DINT	Int32
LINT	Int64
USINT	Byte
UINT	UInt16
UDINT	UInt32
ULINT	UInt64
REAL	Float
LREAL	Double
LDT	DateTime
WSTRING	String
DINT	Enumeration (Encoding Int32) and all derived data types
User-defined data type required (UDT, user-defined data type) The user-defined data type must be created with the prefix "Union_", for example "Union_MyDatatype". The first element (Selector) in this UDT must have the data type "UDINT".	UNION and all derived data types
See LocalizedText and ByteString data types (Page 290)	LocalizedText ByteString
GUID See Using additional OPC UA data types for companion specifications (Page 292)	GUID

Number of implementable server methods and number of arguments

If you implement server methods via your user program, the number of usable methods is limited depending on the CPU type. You can find this information in the equipment manuals of the corresponding CPUs or the latest technical specifications of the CPUs on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/td).

Error message when exceeded
If the maximum number of server methods is exceeded, the OPC_UA_ServerMethodPre or OPC_UA_ServerMethodPost instructions report the error code 0xB080_B000 (TooManyMethods).

Amount of data which can be transferred using server method to an S7-1500 CPU

Max. 2097152 bytes (= 2.1 megabytes MaxMessageSize).

Supply of structured data types with nested arrays

If a structured data type (Struct/UDT) contains an array, the OPC UA server does not provide information about the length of this array.

If you use such a structure as the input or output parameter of a server method, for example, you must ensure that the nested array is supplied with the correct length when the method is called.

If you do not adhere to this rule, the method fails with the error code "BadInvalidArgument".

11.3.6 Providing alarms on the OPC UA server

11.3.6.1 Useful information on alarms

Alarms allow you to detect errors in process control in the automation system quickly, to localize them precisely, and to eliminate them. This leads to a significant reduction in downtimes in a plant. The OPC UA information model "Alarms & Conditions" provides a standardized and platform-independent way of message processing.

As of firmware version V2.9, the OPC UA server of an S7-1500 CPU supports the OPC UA information model "Alarms and Conditions". In this way, the OPC UA server provides access to controller alarms.

The following sections describe which alarm types available in SIMATIC are supported at the OPC UA interface of the OPC UA server.

The following sections also describe how you configure the OPC UA server of the S7-1500 CPU for Alarms & Conditions, the main points of how the Alarms & Conditions model is structured with OPC UA, and which special points must be taken into consideration when using alarms from the address space of the OPC UA server as compared to the SIMATIC controller alarms of the CPU alarm system.

Basis for the converting alarms to OPC UA Alarms & Conditions

The Alarms and Conditions information model is specified in the "OPC 10000-9: OPC Unified Architecture Part 9: Alarms & Conditions" specification.

Controller alarms in SIMATIC

The OPC UA server of the S7-1500 CPUs supports the controller alarms listed below, which are available to S7-1500 CPUs. You configure or program these alarms in the usual way, without the need to consider additional rules for use of these alarms by OPC UA clients.

The added benefit of OPC UA Alarms and Conditions is that these alarm types can be displayed not only by HMI devices, web browsers, the CPU display or the TIA Portal, but also by all OPC UA clients that support OPC UA Alarms and Conditions.

- PLC supervision alarms with ProDiag
  You can integrate simple supervisions in your program with just a few configuring steps and without having to change the program code. The configuration of the supervisions is independent of the programming languages of the TIA Portal because only individual operands are supervised, and you do not need any additional programming sections.
- System diagnostics alarms
  Configuration-dependent module events are known by the hardware configuration of the CPU and can be evaluated by connected display devices. They can only be viewed in the alarm editor and cannot be edited.
- Program alarms (Program_Alarm instruction)
  For reporting program synchronous events, program alarms are assigned to one block at a time. They are created in the program editor and edited in the alarm editor (TIA Portal).
- GRAPH alarms
  For GRAPH function blocks, you can also enable alarms; e.g. for interlocks, supervisions and GRAPH warnings (step-time supervisions).

Important information on the alarm types

The following characteristics are significant to the differences in the behavior of alarms:

- Do alarms have a state (e.g. are they incoming, outgoing - with the corresponding time stamps)?
- Do alarms require acknowledgment?

If none of these characteristics apply, which means the alarms have no state and do not require acknowledgment, alarms simply provide information about an event that has occurred ("Fire and Forget"). It is up to the device receiving the alarm to buffer the alarm for further use or only for display.

Alarm class determines acknowledgment behavior

This section covers the setting options for program alarms. You can also set the behavior of the alarms for system diagnostics alarms and PLC supervision alarms (e.g. ProDiag supervision settings) - refer to the linked more information for details.

You can find the setting options for program alarms in the alarm editor (double-click on "PLC supervisions and alarms" in the project tree, select the "Alarms" tab).

For the S7-1500 CPU, you set here via the alarm class whether an alarm needs to be acknowledged or not. In addition to the acknowledgment behavior, when creating a new alarm class, you define the default priority of alarms of this alarm class.

You set whether an alarm has a state or not by means of the "Information only" option, for example, at the alarm type; this results in "Fire-and-Forget" behavior of the alarm.

Here is an example with settings in the alarm editor with different alarm classes ("PLC supervisions and alarms" in the project tree):

- First line "Program_Alarm": Does not require acknowledgment, information only ("Fire and Forget").
- Second line "Program_Alarm_1": Requires acknowledgment and has a state, which means the alarm includes information on whether it is incoming or outgoing.
- Third line "Program_Alarm_2": Does not require acknowledgment and has a state, which means the alarm includes information on whether it is incoming or outgoing.

Alarm types

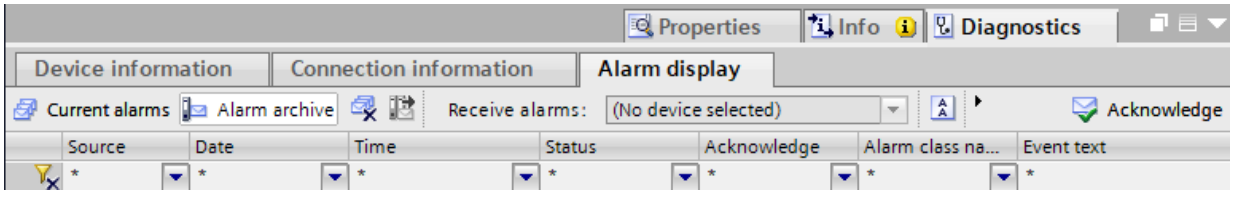
Name	Type	ID	Location	Alarm text	Info text	Alarm class	Acknowle...	Information only
Program_Alarm	PLC alarm		AlarmType	myText	myINFO	No Acknowledgement	☐	☑
Program_Alarm_1	PLC alarm		AlarmType			Acknowledgement	☑	☐
Program_Alarm_2	PLC alarm		AlarmType			No Acknowledgement	☐	☐

Display of alarms in the TIA Portal

During runtime, you have the option of viewing the alarms in the TIA Portal: The alarm display is located directly under the alarm editor ("Diagnostics" tab > "Alarm display" tab).

The following applies to the state and acknowledgment behavior:

- When you click on the "Current alarms" button, alarms that have been recently incoming, outgoing or acknowledged are displayed. Only alarms with a state and alarms requiring acknowledgment are displayed here. You can also acknowledge an alarm requiring acknowledgment (blue font) in this view via the shortcut menu or using the "Acknowledge" button.
- If you want to observe the chronological development (e.g. alarm came in, was acknowledged and went out), you need to click the "Alarm archive" button. The three events that belong to this alarm are listed one after another only in this view. You can only find the current state in the "Current alarms" view.
- Info reports (alarms with the "Information only" property) are only displayed in the "Alarm archive" view. Because these alarms are only triggered once and not buffered, they do not appear in the "Current alarms" view.
- PLC supervisions are also shown in the alarm display.
- System alarms usually belong to the "No Acknowledgment" alarm class with the "Information only" option. These alarms are logged in the diagnostics buffer in the CPU and thus allow the sequence of system alarms to be analyzed over a limited period. In contrast, operating state changes that are also logged in the diagnostics buffer have a state, which means it is indicated that or when a CPU went into STOP state and if or when it exited this state again, for example, entered RUN state. This information is displayed with the states "incoming/outgoing".



Provision of controller alarms by the OPC UA server

When an OPC UA client wants to receive alarms of the S7-1500 CPU, it needs to subscribe to OPC UA events (MonitoredEventItems).

For this purpose, the address space of the OPC UA server of the S7-1500 CPU contains corresponding nodes that are "Event-Notifiers" and create a subscription for the OPC UA clients to receive the alarms.

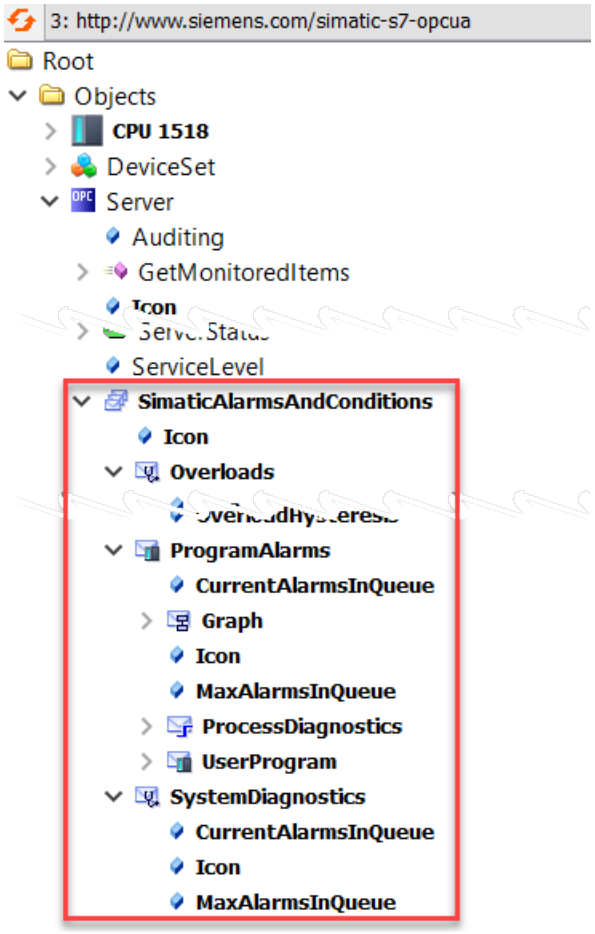
For completeness, we also mention that further type definitions are contained in the server address space for this purpose as nodes under "Types". Type definitions under "BaseEventType" and "ConditionType" ensure that the fields used by SIMATIC alarms are also provided in the OPC UA server.

After the activation of OPC UA Alarms and Conditions (CPU properties in the hardware configuration), the OPC UA address space of the S7-1500 CPU thus reflects the various alarm types (controller alarms) as described above:

- ProcessDiagnostics
  Corresponds to the PLC supervision alarms with ProDiag
- SystemDiagnostics
  Corresponds to the system diagnostics alarms
- UserProgram
  Corresponds to the program alarms
- Graph
  Corresponds to GRAPH alarms

By selecting the node for a subscription, you determine which alarm types are received by the OPC UA client. For example, the "Server" node enables receipt of all alarms, the "UserProgram" node only the receipt of program alarms.

Details about the OPC UA model for Alarms and Conditions are given in the next selection, especially for the "Overloads" node, you can find more information here: Handling memory limits for OPC UA Alarms and Conditions (Page 332).



More information on the alarm types

The concepts and configuration options for controller alarms are not described further here. For information on alarm configuration, alarm display and the associated instructions, such as "Program_Alarm", refer to the STEP 7 online help.

11.3.6.2 OPC UA Events

The basic concepts for alarm processing in OPC UA are expanded on here - the basic concept of "Events" is covered here. The terms used in the various parts of the OPC UA specification have been retained here.

Properties of events

In the address model of the OPC UA server, as of CPU firmware version V2.9, you not only have the option to access PLC tags (read, write) via nodes and to use methods - you can also receive events or alarms via nodes. In OPC UA terminology, these are called "events".

An event includes an event text (Message), time stamp (Time) and event source (SourceNode).

The information supplied with an event from the server depends on the event type. OPC UA defines a BaseEventType in part 5 of the specification (Information Model).

Other event types that provide different alarm behavior are derived from the BaseEventType. This type information of the different event types is visible in the address space of an OPC UA server ("Types" folder). This also applies, for example, to the event types of "Conditions" and "Alarms", which are discussed in the next section.

The OPC UA specification defines for the BaseEventType and for derived EventTypes which properties (fields) of an event are mandatory and which are optional.

The following figure shows the hierarchical structure of BaseEventType.

The following sections show how specialized EventTypes are derived from the root of the derivation hierarchy, the BaseEventType. The SIMATIC-specific derivations ensure that the information supplied in SIMATIC with an alarm and displayed on an HMI device, for example, can also be subscribed to by an OPC UA client in the address space of the OPC UA server.

An event itself is not available as a node in the address space. Events are only triggered by nodes or objects that have the "Event-Notifier" property. These nodes are often also referred to as event signaling objects. Only nodes with this property can be specified as EventMonitoredItem in a subscription to receive corresponding events in the client.

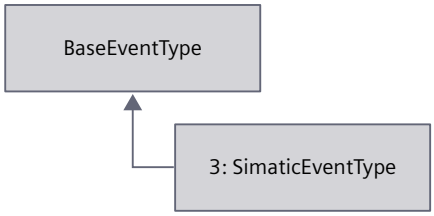
Nodes that can trigger events with an S7-1500 CPU are objects such as "Server", the "SimaticAlarmsAndConditions" object below it, and the three objects below that, ProcessDiagnostics, SystemDiagnostics and UserProgram. The "EventNotifier" attribute is set for these objects in the address space of the OPC UA server of the CPU.

Definition of SimaticEventType

The figure below shows that the type "SimaticEventType" is derived directly from BaseEventType.

BaseEventType is the basic type definition for events with OPC UA.

All event types for OPC UA can be defined, directly or indirectly, based on BaseEventType.



The "SimaticEventType" type is defined in the SIMATIC namespace (http://www.siemens.com/simatic-s7-opcua).

SimaticEventType has all properties of BaseEventType as well as the special properties which are an image of the field structure of SIMATIC alarms.

Description of the event fields for SimaticEventType

The following table contains information on the fields of SimaticEventType for alarms of the type "Information only". Fields that are optional according to OPC UA and are not used by the OPC UA server of the CPU are omitted. You can also find a general description of the fields in the specification OPC 10000-5: OPC Unified Architecture, Part 5: Information Model, Release 1.04.

BrowsePath	DataType	Explanations
EventId	ByteString	Unique Event ID of the event
EventType	NodeId	Node ID of the event type
Time	UtcTime	Time stamp of the event (Event occurrence)
ReceiveTime	UtcTime	Current time stamp at which the OPC UA event was generated.
Message	LocalizedText	Event text
Severity	UInt16	Priority of the alarm from SIMATIC (0..16), spread into a range from 1..1000 with OPC UA, see following table. The priority indicates the urgency with which the event needs a response.
3:AdditionalText_01	LocalizedText	Optional additional text 1
...	...	...
3:AdditionalText_09	LocalizedText	Optional additional text 9
3:AssociatedValue_01	3:SimaticAssociatedAlarmValue	Optional associated value 1 (not for system diagnostics)
...	...	...
3:AssociatedValue_10	3:SimaticAssociatedAlarmValue	Optional associated value 10 (not for system diagnostics)
3:InfoText	LocalizedText	Info text
3:ID	UInt16	Alarm number - A number (ID) assigned by the system that is unique within the CPU and identifies an alarm.
3:DisplayClass	UInt16	Display class (used by HMI devices. Determines the events displayed on specific HMI devices.
3:GroupID	UInt8	Acknowledgment group for alarms that are acknowledged together.

Assignment of Priority (SIMATIC) - Severity (OPC UA)

The following table shows how the 17 priorities that you can assign to alarms in the SIMATIC environment are mapped to the 1000-level Severity with the OPC UA server of the S7-1500 CPU.

This assignment depends on the manufacturer. Different assignments may apply to other devices.

OPC Range	Priority 0..16 (SIMATIC)	Severity 1..1000 (OPC UA)
HIGH (667 – 1 000)	16	1000
	15	930
	14	860
	13	790
	12	720
MEDIUM (334 – 666)	11	650
	10	600
	9	550
	8	500
	7	450
	6	400
	5	350
LOW (1 – 333)	4	300
	3	225
	2	150
	1	75
	0	1

11.3.6.3 OPC UA conditions and OPC UA alarms

The following goes further in depth about the basic concepts for OPC UA Conditions and OPC UA Alarms based on the explanations of events in the previous sections. Again, the terms used in the various parts of the OPC UA specification have been retained here.

Properties of Conditions

A prerequisite for understanding is the concept of "Events" in OPC UA.

In OPC UA, if an event alarm object provides status information in addition to its ability to fire Events, we speak of Conditions. Conditions represent a state of a system or one of its components. Basic states are "enabled" and "disabled", other state definitions are also possible.

In turn, interested OPC UA clients are notified of state changes by means of events (Condition Events).

An example of a Condition is state information, for example, that a device requires maintenance.

Properties of Alarms

However, the properties of ConditionType are not sufficient to completely map the characteristics of SIMATIC alarms in the OPC UA server.

From the ConditionType, which is derived from the BaseEventType, OPC UA defines further derived event types such as AcknowledgeableConditionType and AlarmConditionType.

AcknowledgeableConditionType supplements the properties of ConditionType with the "Acknowledgeable" characteristic (AckedState).

AlarmConditionType thus adds the "ActiveState" characteristic to the properties of ConditionType and the AcknowledgeableConditionType. In SIMATIC terminology, this is an incoming alarm. The ActiveState signals that the situation, which the Condition represents, is currently present or has occurred.

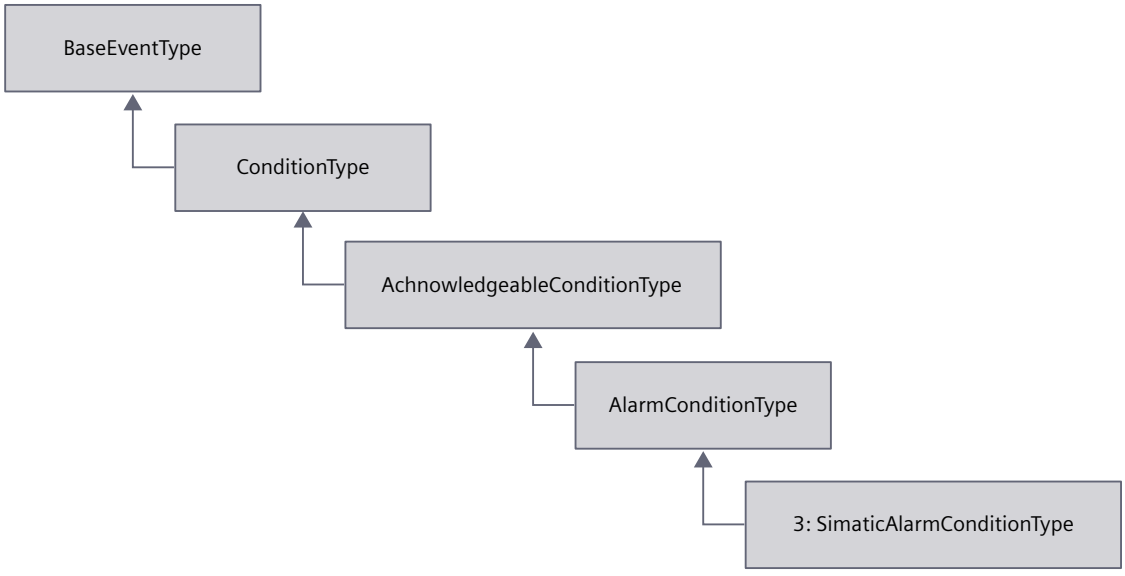
Example: A temperature has exceeded a limit. If "ActiveState" is not set, the situation that represents the condition no longer exists - this is usually referred to as a "normal state". In SIMATIC terminology, this corresponds to an outgoing alarm.

In OPC UA, other statuses such as SilenceState and ShelvingState are defined, but these are not relevant to mapping to the SIMATIC alarm system and will therefore not be described further here.

The SimaticAlarmConditionType is derived from the AlarmConditionType and contains all event fields to map the state and acknowledgment information of SIMATIC messages.

Definition of SimaticAlarmConditionType

The following figure shows how events of the type "SimaticAlarmConditionType" are defined by a series of expansions to the OPC UA "BaseEventType".



Description of the event fields for SimaticAlarmConditionType

The following table contains information about the fields of SimaticAlarmConditionType for stateful and acknowledgeable alarms, which are added to the event fields such as SimaticEventType. Fields that are optional according to OPC UA and are not used by the OPC UA server of the CPU are omitted. You can also find a description of the fields in the specification OPC 10000-9: OPC Unified Architecture, Part 9: Alarms & Conditions, Release 1.04.

BrowsePath	DataType	Explanations
ConditionClassId	NodeId	Node IDs for SystemConditionClassType, ProcessConditionClassType or BaseConditionClassType are possible
ConditionClassName	LocalizedText	Display name of the ConditionClassId
Retain	Boolean	Indicates that the alarm is still relevant for OPC UA clients (set if alarm is still pending and not acknowledged).
Comment	LocalizedText	• Most recent comment entered using the "AddComment" or "Acknowledge" method. • ZERO after a server restart and if no comment was entered.
Comment.SourceTimestamp	UtcTime	Time stamp for the last change of the comment field
AckedState	LocalizedText	"Acknowledged" or "Unacknowledged"
AckedState.Id	Boolean	Set, if acknowledged
AckedState.TransitionTime	UtcTime	Time at which the alarm was acknowledged. ZERO if not acknowledged or not acknowledgeable.
ActiveState	LocalizedText	"Active" or "Inactive"
ActiveState.Id	Boolean	Set when "active"

11.3.6.4 Activating Alarms and Conditions

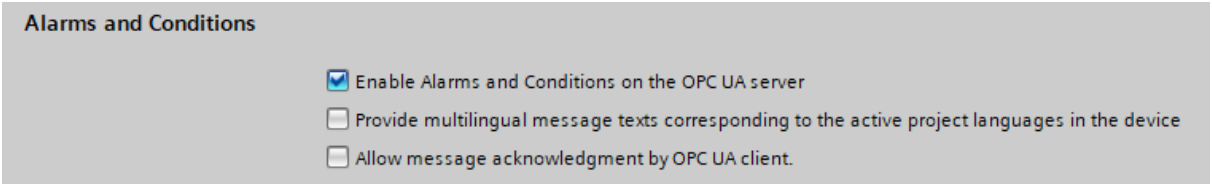
Requirements

- S7-1500 CPU firmware version V2.9 or higher.
- Runtime license for OPC UA purchased according to the license specifications and set in the CPU properties.
- "Central alarm management in the PLC" parameter is enabled ("PLC messages" area in the CPU properties).

Procedure

To activate alarms through OPC UA Alarms and Conditions, follow these steps:

1. In the CPU properties, go to the "OPC UA > Server > General" area.
2. Select the "Enable alarms and conditions on the OPC UA server" option.
   The corresponding types and objects that can trigger events only become visible in the address space when the option is activated.
3. If required, also activate the option "Allow message acknowledgment by OPC UA client".
   In this case, any connected OPC UA client can acknowledge an alarm requiring acknowledgment with the "Acknowledge" method.



Recommendation: Activate diagnostics "Requests of a remote OPC UA client failed"

When the OPC UA server cannot allocate sufficient memory, it is not possible to generate OPC UA alarms in this state; message loss for OPC UA clients may occur.

Therefore, you should activate the diagnostics "Requests of a remote OPC UA client failed" to diagnose this state (Properties of the CPU > OPC UA > Server > Diagnostics).

In addition, you should also activate the option "Summarize diagnostics in case of high message volume".

As soon as sufficient memory is available again, OPC UA clients should call the ConditionRefresh method to receive the current state of the alarm system.

More information

You can find information on methods for OPC UA Alarms and Conditions in the section Methods for OPC UA Alarms and Conditions (Page 329).

You can find information on failed requests of a remote client in the section Request of a remote client failed (Page 340).

11.3.6.5 Subscribing to events of an OPC UA server

Subscribing to all events via the "Server" node

OPC UA servers provide events via the "Server" node and lower-level nodes. When OPC UA clients subscribe to the "Server" node, they receive all events and alarms of the OPC UA server.

The "Server" node is located in the "Objects" folder below "Root".

OPC UA servers inform OPC UA clients which event types they use (under "Root > Types > EventTypes" in the address space).

Filter options for events

OPC UA clients can choose and only subscribe to specific nodes under the "Server" node and thus to specific event types, for example, only the "UserProgram" node. This reduces the number of events from the OPC UA server to program alarms.

Another way of filtering is to select the event fields, known as "Select Clause" in OPC UA terminology.

This means that in the subscription, the OPC UA client makes a selection of the event fields in addition to the event alarm object (e.g. the "UserProgram" node). You select the event fields via the browse name of the corresponding field.

OPC UA also defines so-called "Where Clauses". A Where Clause in the event filter is used to further limit the number of events that are supplied by the OPC UA server for the selected object, for example, by filtering to a severity range.

Configure Where Clause for event filter

To configure a Where Clause for an event filter, you need operands and operators. The operands provide the required values or data. The operators determine the filter criteria for the operands and thus limit the number of events.

If you configure a filter for the events of the OPC UA server of a CPU on the OPC UA client, only one filter may be active for Where Clauses. Otherwise, no messages are issued by the OPC UA server of the CPU. If several filters are active, the OPC UA server returns the error code "BadFilterElementInvalid".

The following tables show the operands and operators from the OPC UA specification Part 4 and which of them are supported by the OPC UA server of a CPU.

Table 3-28 Operands for Where Clauses of an event filter

Operand	Description	Supported by the OPC UA server of a CPU
ElementOperand	Refers to the position of another operand via an index in the element array. In this way, a logical tree structure of linked sub-elements can be created.	Yes[1]
LiteralOperand	Refers to a fixed, directly entered value (literal), e.g: • Number • String • Boolean value	Yes
AttributesOperand	Refers to any attribute of an object or variable node using a node in the type system and a path constructed from ReferenceTypes and BrowseNames.	No
SimpleAttributeOperand	Refers to any attribute of an object or variable node using a TypeDefinition and a path constructed from BrowseNames.	Yes

[1] When using "ElementOperand", the error code "BadFilterElementInvalid" is returned, as the filter depth on the OPC UA server of a CPU is limited to 1.

Table 3-29 Operators for Where Clauses of an event filter

Operator	Number of addresses	Result type	Supported by the OPC UA server of a CPU
Equals_0	2	Boolean	Yes
IsNull_1	1	Boolean	Yes

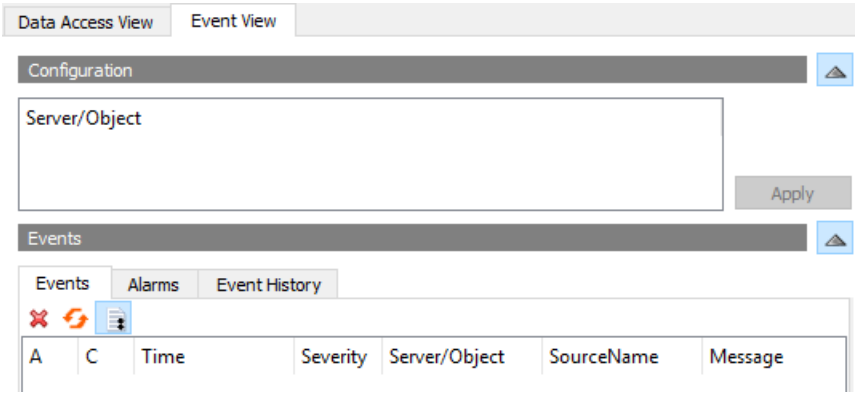
Operator	Number of addresses	Result type	Supported by the OPC UA server of a CPU
GreaterThan_2	2	Boolean	Yes
LessThan_3	2	Boolean	Yes
GreaterThanOrEqual_4	2	Boolean	Yes
LessThanOrEqual_5	2	Boolean	Yes
Like_6	2	Boolean	Yes
Not_7	1	Boolean	Yes
Between_8	3	Boolean	Yes
InList_9	2 ... n	Boolean	Yes
And_10	2	Boolean	Yes
Or_11	2	Boolean	Yes
Cast_12	2	Type from Operand[1]	No
InView_13	1	Boolean	No
OfType_14	1	Boolean	Yes
RelatedTo_15	6	Boolean	No
BitwiseAnd_16	2	Integer	Yes
BitwiseOr_17	2	Integer	Yes

Example client UaExpert

The example of the UaExpert OPC UA client shows how events of an OPC UA server can be received via a subscription. Here is the most important information on the displayed events/alarms:

- Event View is a separate view of events in addition to the Data Access View.
- The "Configuration" area contains the selected event signaling object with the fields for the Select Clause. A configuration of Where clauses is currently not possible in UaExpert.
- In the "Events" area, "Events" tab: Corresponds to the TIA alarm view with activated "Alarm archive" button; events of the "Information only" category and outgoing alarms are also visible there, because UaExpert buffers them in the background for display. These events are not visible in the "Alarms" tab.
- In the "Events" field, "Alarms" tab: Corresponds to the TIA alarm display with activated "Current alarms" button; alarms are visible here with their status, e.g. "active" (corresponds to "incoming") and these alarms can also be acknowledged using the context menu. Outgoing alarms are no longer visible in this view.

In the columns of the Event area, a selection of event fields is offered, for example, the event text (Message) and whether the alarm was acknowledged (A=Acknowledged).



Special features of the display of alarms via the OPC UA server of the CPU

The following once again summarizes the special features of the alarm display via OPC UA Alarms and Conditions for the current status.

Topic	Explanation
Comment	Via OPC UA, you can add a comment to a alarm using the "AddComment" method or the "Acknowledge" method. This comment is no longer available after a server restart.
Pending alarms are not lost after a server restart	The OPC UA server supports the "ConditionRefresh" method with which it makes the current state of the system available to the OPC UA client, for example, after download of a new data block (requires server restart and re-establishment of the connection).

11.3.6.6 Processing associated values of alarms

You can specify placeholders for SIMATIC alarms. With placeholders you can integrate up to 10 associated values (SD_1 to SD_10) into the alarm text. Placeholders can also be specific text list entries.

When you are using alarms with placeholder, you must observe the following rules:

- Placeholders that represent values in the alarm are only inserted automatically for system diagnostic alarms or security event alarms. For other categories of alarms (e.g. program alarms), the placeholders for values are not resolved. The OPC UA clients must resolve these alarms.
- Placeholders that reference text lists are resolved by the CPU (format, e.g.: %t#<name of the text list>).

Example of how values and placeholders are assigned through UaExpert

1. Make sure that you have selected all fields that you need in the UaExpert configuration.
   Note that each field that is not needed causes a communication load. Therefore, you should avoid a complete selection as shown in the example below.

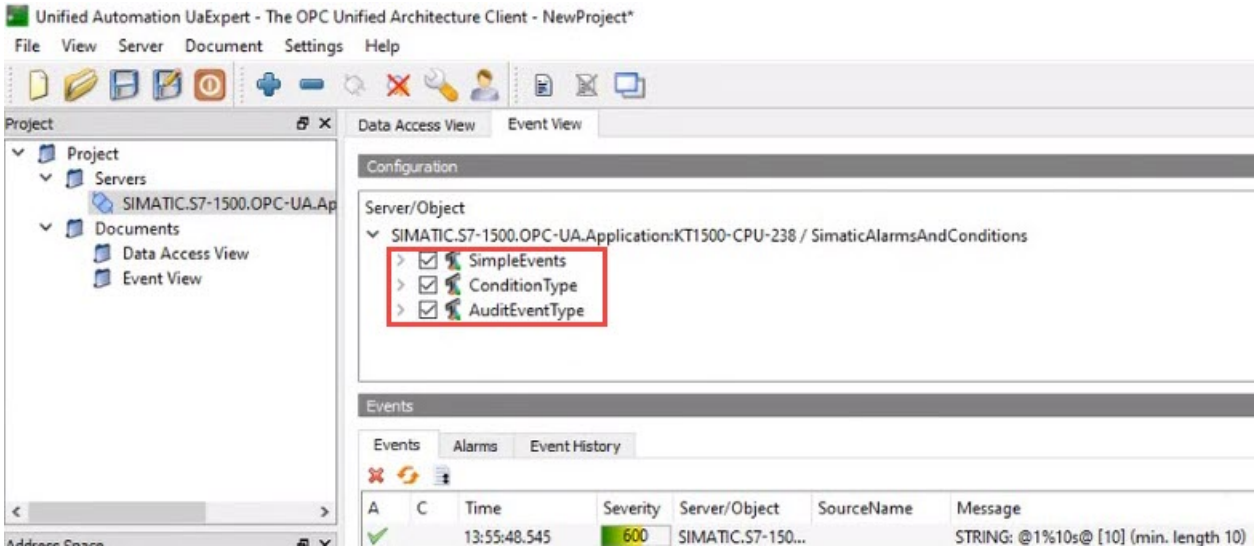


Figure 3-214 ServerObject-Configuration_neutral120

2. In the "Events" tab of UaExpert, you select the alarm with the integrated associated values. In the "Details" area of the alarm, you will find the value that is to be integrated into the alarm.
   Example: "AssociatedValue_01" is assigned to SD_1 (format @1% ...@).
   You will find explanations on the formats for associated values in the TIA Portal information system (e.g. by searching for "Example of associated values").

Support of simple data types as associated values

The field type from "AssociatedValue_01 to ..._10 is of the Union type and is limited to some simple types. The OPC UA data type is SimaticAssociatedAlarmValue. The following simple data types are supported:

3:AssociatedValue_01	SimaticAssociatedAlarmValue
Switch Field	2
Boolean	True
3:AssociatedValue_02	SimaticAssociatedAlarmValue
Switch Field	6
SByte	123
3:AssociatedValue_03	SimaticAssociatedAlarmValue
Switch Field	3
Int16	1234
3:AssociatedValue_04	SimaticAssociatedAlarmValue
Switch Field	4
Int32	12345
3:AssociatedValue_05	SimaticAssociatedAlarmValue
Switch Field	7
Byte	123
3:AssociatedValue_06	SimaticAssociatedAlarmValue
Switch Field	8
UInt16	1234
3:AssociatedValue_07	SimaticAssociatedAlarmValue
Switch Field	11
Float	1
3:AssociatedValue_08	SimaticAssociatedAlarmValue
Switch Field	12
Double	2
3:AssociatedValue_09	SimaticAssociatedAlarmValue
Switch Field	9
UInt32	12345
3:AssociatedValue_10	SimaticAssociatedAlarmValue
Switch Field	13
String	HelloWorld

Figure 3-215 UnionDataTypes_neutral120

Mapping to SIMATIC data types

The following assignment SIMATIC data type => OPC UA data type applies:

Supported data types for SD_1 to SD_10	Mapping to OPC UA
BOOL	Boolean
BBOOL	Boolean
BYTE	Byte
CHAR	Byte
SINT	SByte
USINT	Byte
WORD	UInt16
WChar	UInt16
INT	Int16
UINT	UInt16
DWORD	Uint32
DINT	Int32

Supported data types for SD_1 to SD_10	Mapping to OPC UA
UDINT	Uint32
REAL	Float
LREAL	Double
String	String
WString	String

11.3.6.7 Simultaneous receipt of messages in multiple languages

Alarms are transmitted from the OPC UA server to the OPC UA client in the default or reference language. In the "Multilingual support" area of the CPU parameters, you can set the loaded project languages in which the alarms are to be transmitted.

As of Version 4.0 of the S7-1500 CPUs, you have the option of having the languages of connected OPC UA clients selected:

- When establishing the session, a client can request message texts in one or more active project languages using the parameter "LocaleIds []"; see OPC 10000-4: Services, ActivateSession Service Parameters.

  Only message texts can be requested from the OPC UA server of the CPU in this way; the parameter has no effect on other localized texts in the address space.

  Requirement: The "Provide multilingual message texts corresponding to the active project languages in the device" option has been enabled.
- A client can request the message texts in all three active project languages simultaneously, e.g. to collect the alarms on a central server, so that they can be evaluated by people in different languages.

Requirements

- S7-1500 CPU as of firmware version 4.0
- The OPC UA client supports the LocaleIds "qst" and "mul" for multilingual texts.
- The "Provide multilingual message texts corresponding to the active project languages in the device" option has been enabled ("Alarms and Conditions" area in the CPU properties).

Effect of the LocaleId "qst" and "mul"

OPC UA specification (OPC 10000-3: UA Part 3: Address Space Model) describes the built-in data type "LocalizedText", which is used for texts in different languages.

The elements of the structure for the data type LocalizedText are defined as follows:

Name	Type	Description
LocalizedText	Structure	
Locale	LocaleId	Identifier for the language (language code) <language>-<Country/Region>, e.g. "en-US" Specified by IETF RFC 5646
Text	String	Localized text (language-specific translation)

LocaleId = "qst"

"qst" is not an abbreviation but merely a defined string for a LocaleId, which contains replacement texts in addition to the contents, as in the case of "mul".

When an OPC UA client requests a LocalizedText with the LocaleId "qst", it receives the message texts in all loaded project languages on the CPU. In addition to the Array of LocaleId, the JSON text element has a section with the definition of replacement texts (replacement section). The client must carry out the provided replacements in the message text.

Example texts in two languages; "t" stands for "text", "r" for "replacement":

```
{
 "t": [
 ["de-DE","mein Text @1@ /2/"],
 ["en-US","my text @1@ /2/"]
 ],
 "r": [
   ["@1@", "myCompany"]
   ["/2/", 1.2345]
 ]
}
```

Resulting text:

```
de-DE: "mein Text myCompany 1,2345"
en-US: "my text myCompany 1.2345"
```

Because the decimal number 1.2345 in the replacement section is not formatted as String, it can be written correctly in the different languages (with decimal point in en-US and with decimal comma in de-DE) – provided that this function has been implemented in the client.

LocaleId = "mul"

If an OPC UA client requests a LocalizedText with the "mul" LocaleId, this request is ignored by the OPC UA server. The reason for this is that the OPC UA server does not support the "mul" LocaleId. It is only returned as a response to a request via the "qst" LocaleId if no replacement texts are contained in the response.

Rules

Alarm texts are assembled by the server according to the following rules, and provided to the client:

- To simplify the handling of multilingual message texts, only the LocaleId "qst" is allowed for the server of the S7-1500.

  If you request multilingual message texts with "qst" and there are placeholders (associated values) in the text, the placeholders are provided in the replacement section. If no placeholders are present in the text, the text is returned as LocaleId "mul" without replacement section.

  If only one language is returned (e.g. because there is only one active language or alignment with the requested languages results in a single language) and no placeholder is present in the text, the message text is not returned as JSON but rather is returned directly as localized text in the appropriate language.

- A client can retrieve the alarms in all languages provided by the server or only some of these languages. The client defines the selection through an Array of LocaleIds, which follows the LocaleId "qst". If no other LocaleIds follow the LocaleId "qst", all available languages are provided by the server.
- Multilingual replacement texts are not returned in the replacement section. You implement multilingual replacement tests using text lists.

Reading out supported languages

The OPC UA server publishes the supported languages under the node "Server Capabilities > LocaleIdArray".

11.3.6.8 Methods for OPC UA Alarms and Conditions

The OPC UA specification Part 9 (OPC 10000-9: Alarms & Conditions) defines methods for OPC UA servers to enable OPC UA clients to react to state changes, for example.

In the following, the methods are described that are supported by the OPC UA server of the S7-1500 CPU with their special features.

Requirement

Using the relevant methods for the Alarms and Conditions functionality requires the following:

- Alarms and Conditions is activated
- For the "Acknowledge" method, the acknowledgment of alarms by OPC UA clients must be allowed on the server side.

Methods for OPC UA Alarms and Conditions

In the following, the methods are briefly explained with the special features and restrictions caused by the implementation for the OPC UA server of the S7-1500 CPU.

The methods are visible in the type space.

The OPC UA specification listed above contains the general description.

You can find a detailed description of the individual methods below this overview table.

Method	Description
Acknowledge	Method for acknowledging an alarm object that is uniquely identified by a EventId.
ConditionRefresh	Method for requesting an update of all alarm objects (in SIMATIC language: updating of all pending alarms). All monitored items of the subscription are updated. Synchronization of pending alarm objects from the OPC UA server of the CPU is indicated e.g. in the following situations: • Connecting for the first time or resuming the connection (after interrupting the communication) • Screen change on an operator screen of an HMI device
AddComment	Method for adding comments to alarm objects.

Calling the "Acknowledge" and "AddComment" methods

Method calls in OPC UA use MethodId and ObjectId.

In the case of an alarm object, ObjectId is the node ID for the instance of the alarm object.

Since the address model of Simatic Alarms and Conditions does not provide instances for alarm objects, the OPC UA specification provides in this case that the OPC UA client uses the ConditionId as ObjectId.

You can find information on how to determine the ConditionId using a SimpleAttributeOperands in the SelectClause of the event filter, see also the OPC UA specification Part 9 (OPC 10000-9: Alarms & Conditions):

Name	Type	Description
SimpleAttributeOperand		
typeId	NodeId	*NodeId* of the *ConditionType Node*
browsePath[]	QualifiedName	empty
attributeId	IntegerId	Id of the *NodeId Attribute*

Acknowledge

The Acknowledge method (MethodId: i=9111) has the following parameters:

Parameter	Data type	Description
[in] EventId	ByteString	EventId identifies a specific event notification. Only events whose AckedState.Id field has the value "False", can be acknowledged with the "Acknowledge" method.
[in] comment	LocalizedText	Text for commenting the acknowledgment, e.g. by an operator. See also supplementary description of the "AddComment" method.

Method Result Codes

Result Code	Description
Good	Method was successfully executed.
BadNotSupported	Method cannot be called because the option for acknowledging for Alarms and Conditions by OPC UA clients is deactivated in the CPU properties for OPC UA.
BadConditionBranchAlreadyAcked	Acknowledgment has already been made.
BadNodeIdUnknown	Method was called with the wrong ConditionId (see notes on ObjectId).
BadEventIdUnknown	Method was called with the wrong EventId.

ConditionRefresh

The ConditionRefresh method (MethodId: i=3875) has the following parameters:

Parameter	Data type	Description
[in] SubscriptionId	Uint32	SubscriptionId of the subscription to be updated.

Method Result Codes

Result Code	Description
Bad_SubscriptionIdInvalid	The SubscriptinId is not valid.
Bad_RefreshInProgress	The "ConditionRefresh" is currently running.
Bad_UserAccessDenied	The method "ConditionRefresh" runs in the context of a wrong session. This means that the subscription belongs to a different session.

NOTE

ConditionRefresh2 method

The OPC UA server of the S7-1500 CPU does not support the ConditionRefresh2 method which can specifically synchronize a monitored item (MonitoredItem) in a subscription. In this case, the OPC UA Server returns the result code "Bad_MethodInvalid". Use the method "ConditionRefresh" instead.

AddComment

You have the possibility to add comments to Alarms- objects of the SimaticAlarmConditionType type because the support of comments is mandatory for OPC UA Alarms and Conditions .

A comment was save in the "Comment" event field.

The following time stamp event fields belong to the comment:

- "Comment.SourceTimestamp" for the time when the comment is transferred to the CPU
- "Time" for the time when the Alarms object was modified

When the "AddComment" method is called, "Time" and "Comment.SourceTimestamp" are identical.

Special features of Alarms and Conditions comments for the OPC UA server of the CPU

The AddComment method (MethodId: i=9029) has the following parameters:

Parameter	Data type	Description
[in] EventId	ByteString	EventId identifies the event notification for which a state was reported.
[in] comment	LocalizedText	Text for commenting the specified Alarms object.

Method Result Codes

Result Code	Description
Good	Method was successfully executed.
BadNodeIdUnknown	Method was called with the wrong ConditionId (see notes on calling the methods "Acknowledge" and "AddComment").
BadEventIdUnknown	Method was called with the wrong EventId.

Special features of Alarms and Conditions comments for the OPC UA server of the CPU

You have the possibility to add comments to alarm objects of the "SimaticAlarmConditionType" type with the AddComment method. A comment is also set when the Acknowledge method is called. The "AddComment" method can be called several times.

- A comment was save in the "Comment" event field. The "Comment.SourceTimestamp" indicates the last time at which a **comment** was set.
- The "Time" time stamp marks the **last modification time of the alarm object**.

When the "AddComment" method is called, "Time" and "Comment.SourceTimestamp" are identical.

When the "Acknowledge" method is called, the two time stamps may differ, since the acknowledgment is asynchronous.

The support of comments for OPC UA Alarms and Conditions is mandatory. The SIMATIC alarm system does not know corresponding comments for alarms. Therefore, some special features have to be considered:

- There is only one comment:
  There is only one comment for an alarm object, so that an existing comment is always overwritten when several method calls are made in succession.
- Lifetime and time stamp:
  Comments are only stored at the current alarm object. If the alarm object no longer exists, e.g. after a server restart, the comment no longer exists either. The corresponding "Comment" and "Comment.SourceTimestamp" event fields are then reset (zero).
  The "Time" event field is then set as if the method call "AddComment" did not exist.
  Example: If you comment on an unacknowledged Alarms object, the "Time" event field receives the time of this comment change. After a server restart, the "Time" event field does not show the time when the comment was set, but the time when the corresponding Event arrived.

11.3.6.9 Handling memory limits for OPC UA Alarms and Conditions

The OPC UA server of the S7-1500 CPU has product-specific limited memory capacity for the "Alarms and Conditions" function (see CPU specifications).

Two memory pools for different categories of alarms are available:

- Pool only for ProgramAlarms (corresponds to program-related alarm originators (producers) such as program alarms via Program_Alarm, ProDiag, Graph)
- Pool only for SystemDiagnostics (corresponds to system diagnostic alarms)

Under unfavorable conditions (e.g. alarm burst) the CPU cannot make all pending alarms (ProgramAlarms or SystemDiagnostics) from the SIMATIC alarm area available to the OPC UA Alarms and Conditions system. However, alarms are not lost in this case.

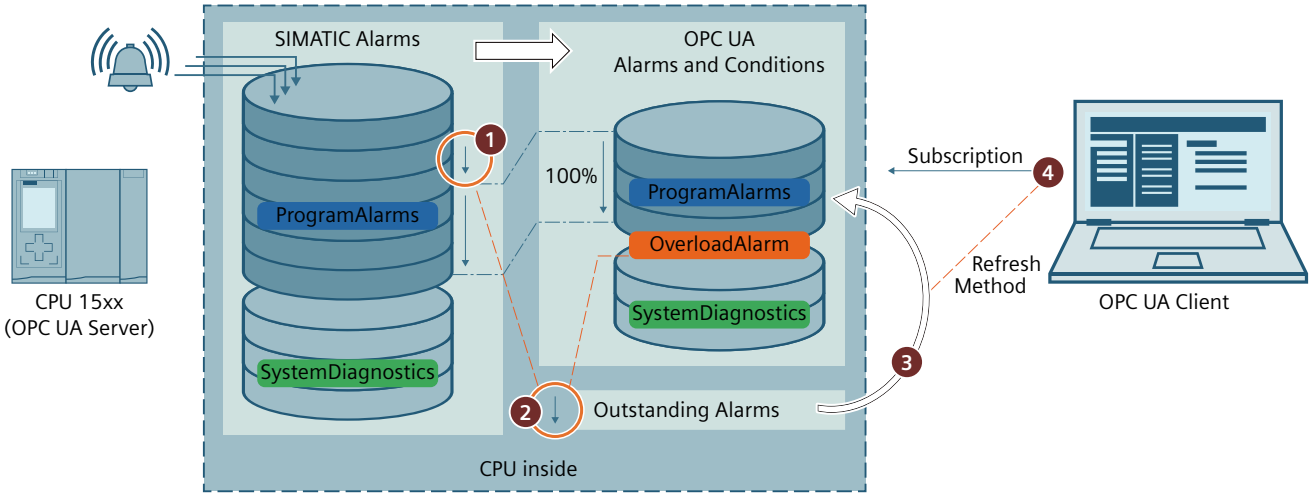
You have the possibility to react to this overload event in the user program. According to your application you can use the "ConditionRefresh" method to make alarms that "did not make it into the OPC UA Alarms and Conditions system" available to the OPC UA Alarms and Conditions system again.

Requirement

- Alarms and Conditions is activated
- Event subscriptions are set up in the OPC UA client

Principle

The following figure shows a simplified process for temporarily storing ProgramAlarms to make them available again at another time for the OPC UA Alarms and Condition System. The nodes mentioned in the caption are visible in the following image of the address model.



① Number of active alarms is too high to make all alarms accessible via OPC UA Alarms and Conditions

② Overloads alarm (overload alarm) is triggered. This overload alarm is active until the following situation occurs:
- No more alarms are pending for the OPC UA Alarms and Conditions system (OutstandingProgramAlarms = 0) and
- Number of alarms in the OPC UA Alarms and Conditions system < Hysteresis-cleaned maximum value for OPC UA alarms (= MaxAlarmsInQueue - OverloadHysteresis)

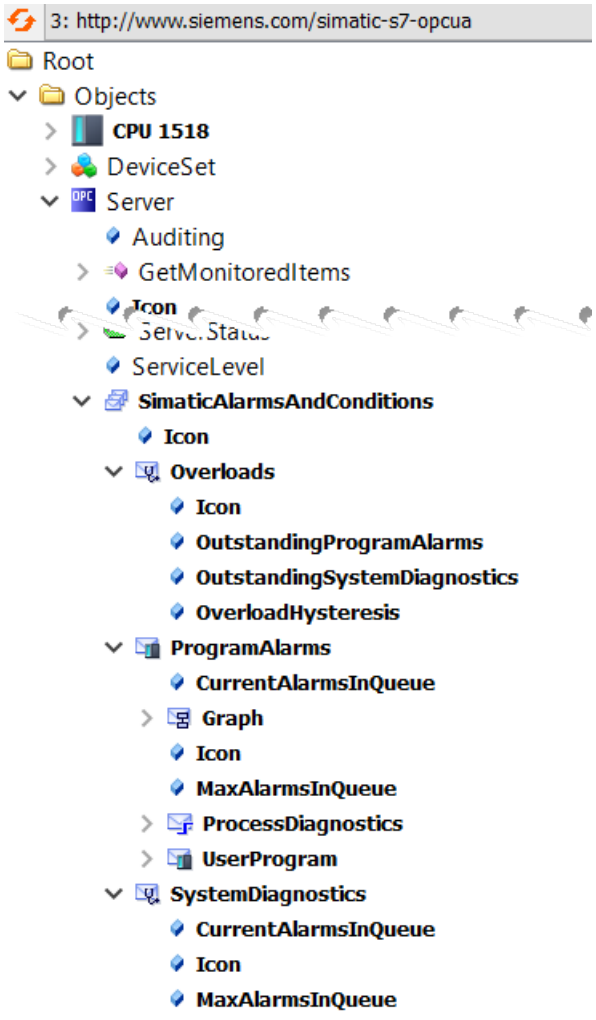
Alarms that are not available in the OPC UA Alarms and Conditions system due to the overload situation are buffered by the CPU as "OutstandingAlarms".

③ When an OPC UA client executes the ConditionRefresh method, not only are all alarm objects of the relevant subscription synchronized, but also the alarms outstanding for OPC UA Alarms and Conditions (OutstandingAlarms) are transferred to the Alarms and Conditions memory area - until the maximum number of alarms is reached. "Oldest" alarms are transferred first. After that every subscription to these alarms receives the transferred alarms - not only the OPC UA client that called the ConditionRefresh method.

④ The OPC UA client controls the handling of pending alarms via the information of the Overloads nodes.

Address model for Alarms and Conditions

The following figure shows the nodes of the OPC UA Alarms and Conditions address model.



Special features

- When pending alarms go out or are acknowledged, they no longer enter the OCP UA Alarms and Conditions system area via the ConditionRefresh method. They are then "invisible" to OPC UA Alarms and Conditions and thus to the connected OPC UA clients. This fact influences e.g. statistical evaluations of alarm progressions.
- To avoid a high alarm frequency for the Overloads Alarm if the number of alarms oscillates around the maximum value, the limit for triggering the alarm is higher than the limit for canceling this alarm: The value for this difference is displayed in the "OverloadHysteresis" node.
  Example: Maximum number of alarms: 200, OverloadHysteresis: 3.
  Overloads alarm is triggered starting with 200 alarms and is only canceled if there are fewer than 197 alarms. If the number of alarms increases again, it will be triggered again when 200 alarms are exceeded.

11.3.7 Using diagnostics options

11.3.7.1 Diagnostics of the OPC UA server

Online diagnostics of the OPC UA server

The S7-1500 CPU OPC UA server can be diagnosed online with standard OPC UA clients, such as UaExpert.

The diagnostic information is subdivided into the following areas:

- Server Diagnostics
- Sessions Diagnostics
- Subscription Diagnostics

In the address space of the server, for example, the following nodes are available with diagnostic information:

- **ServerDiagnosticsSummary**: Server diagnostics summary
  - CurrentSessionCount: Number of active sessions
  - SecurityRejectedSessionCount: Number of sessions rejected due to mismatching end point security settings between client and server
- **SessionsDiagnosticsSummary**: Session diagnostics summary
  - ActualSessionTimeout: Set time that a session lasts, e.g. in the event of disconnection
- **SubscriptionDiagnosticsArray**: ARRAY with one element per subscription for each session

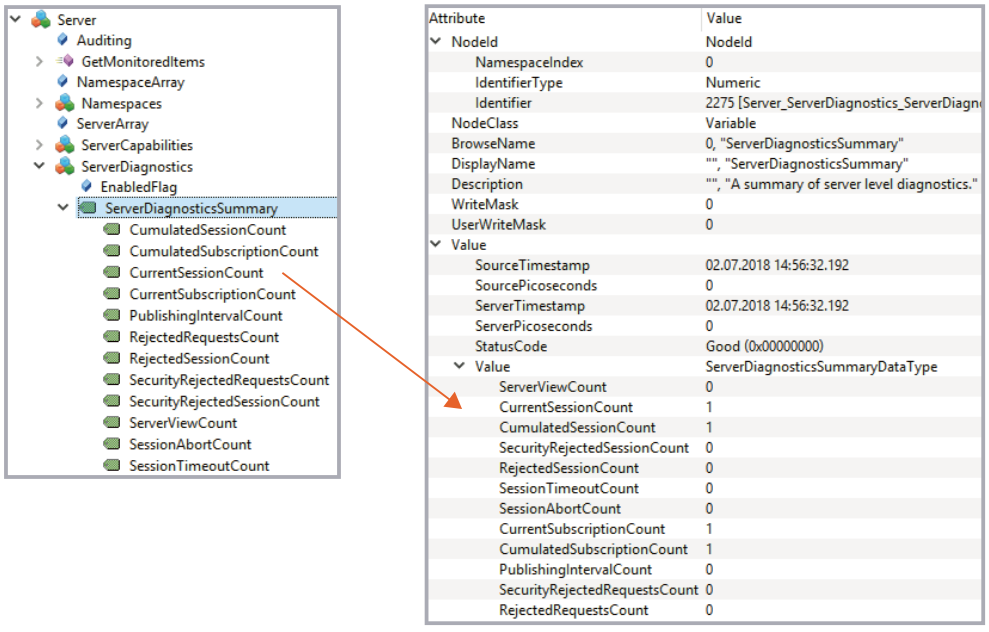


Figure 3-216 Server diagnostics

The SessionsDiagnosticsSummary node also shows the properties of the client application accessing the server within the session.

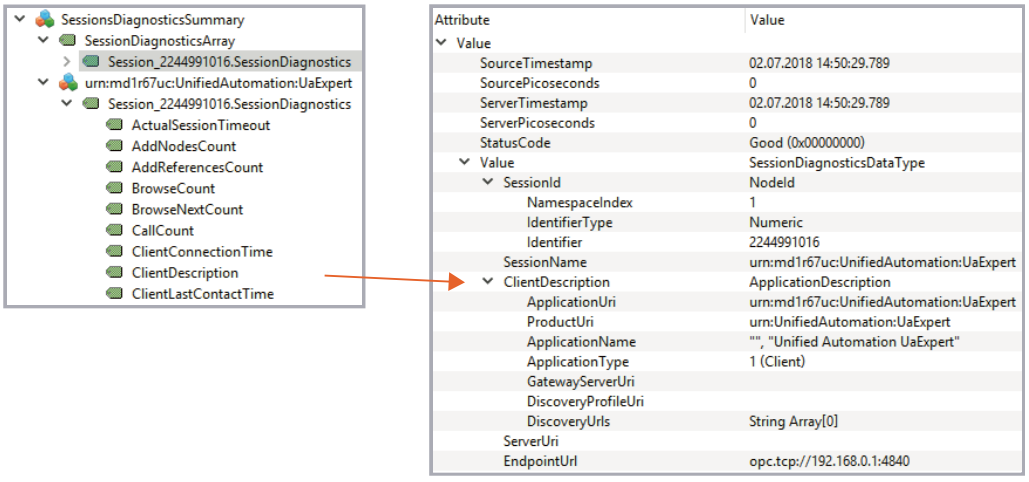


Figure 3-217 Sessions diagnostics with the properties of the client application

Diagnostics of the connection between client and server

To diagnose the status of the connection during program runtime in the client, use the following instruction:

OPC_UA_ConnectionGetStatus: Read connection status.

11.3.7.2 Running diagnostics for OPC UA servers in the program

From STEP 7 (TIA Portal) V18 onwards, you can access nodes in the OPC UA address space of an S7-1500 CPU (firmware version V3.0 onwards) to evaluate the contents for diagnostic purposes in the program.

Functional principle

In the local address space of the CPU, there are numerous nodes where the OPC UA server of the CPU stores data and states. The "OPC_UA_ReadList" instruction enables you to access this information and evaluate it in the user program.

Example: "ServerState" is a node in the address space of the CPU that contains values for the server state or for state transitions (Running, Shutdown, Failed, etc.).

You do not use the instruction as a client instruction, but instead as an instruction for reading nodes of the own local OPC UA address space. In this regard, special rules and requirements apply to this application case.

More information

You can find more information on calling the "OPC_UA_ReadList" instruction for diagnostic purposes in the TIA Portal help, topic "Diagnosing OPC UA servers with OPC_UA_ReadList".

11.3.7.3 Server state transition diagnostics

Information on the server state

S7-1500 CPUs as of firmware version V2.8 are able to create an entry in the diagnostic buffer upon state changes of the OPC UA server.

The diagnostic buffer displays the new state.

The cause of the state change is also displayed, such as download to the CPU, POWER OFF - POWER ON transition, user program instruction or service request from a partner (client).

Requirement

The "Change of OPC UA server status" option is selected (OPC UA > Server > Diagnostics) in the OPC UA properties of the CPU.

NOTE

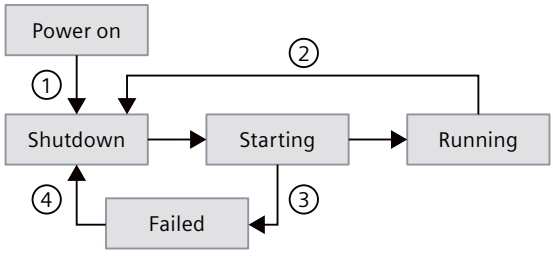
If this option is selected, the CPU also automatically enters the lowest set security policy into the diagnostic buffer after startup.

Examples

If the OPC UA server of the CPU shuts down due to a download process and then starts with a valid new configuration, the diagnostic buffer shows new server state, e.g. Shutdown => Starting => Running.

If the OPC UA server shuts down due to a download process and the server cannot start because the type dictionary is too large, the diagnostic buffer finally shows the state "Failed" (Shutdown => Starting => Failed).

Server states and state transitions



①, ④ POWER ON or Load in RUN, if OPC UA relevant data could be affected.

② Loading the hardware configuration with deactivated OPC UA server. The server remains shut down.
Loading the hardware configuration with activated OPC UA server and faulty OPC UA data (for example, too many structures with the result that the type dictionary becomes too large). In this case, the server cannot start (see ③).

③ OPC UA server cannot start due, for example, to faulty configuration.

Figure 3-218 Server states and state transitions

Description of the server states

The individual states that the OPC UA server can assume are explained below.

Server states	Explanation
Shutdown	Initial status • After POWER ON • After loading the hardware configuration with activated or deactivated OPC UA server. • After loading OPC UA relevant data
Starting	OPC UA address space in server is initialized.
Running	OPC UA server running (normal productive state for OPC UA server).
Failed	Error state. OPC UA server cannot start due, for example, to faulty configuration.

11.3.7.4 Session state transition diagnostics

Information on the session state

S7-1500 CPUs as of firmware version V2.8 are able to create an entry in the diagnostic buffer for state changes of an OPC UA session.

The diagnostic buffer displays the new state. The corresponding session ID is also displayed.

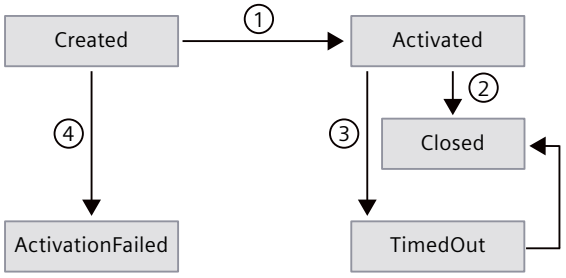
Requirement

The "Change of session states" option (OPC UA > Server > Diagnostics) is selected in the OPC UA properties of the CPU.

Example

A client transmits incorrect authentication data (for example, incorrect password) when a connection is established. The new state of the "ActivationFailed" session is entered with the corresponding session ID in the diagnostic buffer.

Subscription states and state transitions



① Client connects to server, login with correct authentication data (correct credentials).
② Client closes connection correctly.
③ Client no longer sends messages; session ends with timeout.
④ Client connects to server, login with incorrect authentication data.

Figure 3-219 Session states and state transitions

11.3.7.5 Check for security events

If the CPU diagnostics detects a security event during the OPC UA communication, it can enter it in the diagnostic buffer.

Requirements

- S7-1500 CPUs as of firmware version 2.8
- The "Check for security events" option is activated (properties of the CPU > OPC UA > Server > Diagnostics).

Security events detected in diagnostics

S7-1500 CPUs perform diagnostics on the following OPC UA relevant security events:

- Client-certificate is invalid (for example, syntactically or semantically incorrect, incorrect signature, current date is not in the validity period)
- User name/password login failed (deactivated or incorrect data)
- Client wants to use a specific security policy or a specific message security mode; the server does not support the security policy or the requested security mode.
- Client does not establish connection according to specification (OPC UA Spec) (for example, unexpected SecureChannelID/SessionID/client Nonce)

Example

If an attempt is made to compromise communications (for example, by session hijacking, man-in-the-middle attacks etc.), the server detects this via analysis.

11.3.7.6 Request of a remote client failed

S7-1500 CPUs as of firmware version V2.8 are able to create an entry in the diagnostic buffer for the following events:

- Bad client requests (incorrect use)
- Service error occurred
- CPU-specific high limits of the OPC UA server were violated

Example of a faulty client request

For example, there is an incorrect request when a client addresses a node (tag) that does not exist or if a resource is requested that does not exist.

In this case, the corresponding service that caused the fault is entered in the diagnostic buffer and the corresponding session ID is also entered.

Service fault

If a service itself fails, the server returns a ServiceFault. In this case, the status code (Bad...) and the according session ID are entered in the diagnostics buffer.

Example of limit violations

If a service request exceeds a CPU-specific limit, for example, number of sessions, number of monitored items, number of subscriptions, etc., this diagnostics is entered in the diagnostics buffer. Together with the message, it is indicated which limit has been violated.

Exception: If you summarize diagnostics and the message occurs frequently, the limit causing the error is not entered. You receive general information that the supported configuration limit has been violated.

Possible entries for the service that is causing the error

Depending on the client application used, requests to the server can be triggered differently from the user's viewpoint, for example, by an online tool with a graphical user interface or by instructions in a client's program.

With its service-oriented architecture, OPC UA follows a request-response paradigm, therefore the respective client application converts the requests into the service requests defined in OPC UA.

The names of these services are defined and grouped according to their use. You can find more information on the website of the OPC Foundation (https://opcfoundation.org/).

In the case of an incorrect use, you can find precisely these names of the services, together with the corresponding session ID, in the diagnostic buffer as the service that caused the error.

The services available with OPC UA are listed below.

Discovery Service Set
FindServers

GetEndpoints

Session Service Set
CreateSession
ActivateSession
CloseSession
Cancel

View Service Set
Browse
BrowseNext
TranslateBrowsePathsToNodeIds
RegisterNodes
UnregisterNodes

Attribute Service Set
Write
Read

Method Service Set
Call

Monitored Item Service Set
CreateMonitoredItems
ModifyMonitoredItems
DeleteMonitoredItems
SetMonitoringMode
SetTriggering

Subscription Service Set
CreateSubscription
ModifySubscription
DeleteSubscriptions
TransferSubscriptions
Publish
Republish
SetPublishingMode

11.3.7.7 Subscription diagnostics

Information about a subscription

S7-1500 CPUs as of firmware version V2.8 are able to create an entry in the diagnostic buffer at state changes of a subscription.

The diagnostic buffer displays the new state; exception: "KeepAlive".

Requirement

In the OPC UA properties of the CPU, the option "Subscriptions: Change of status" (OPC UA > Server > Diagnostics) is selected.

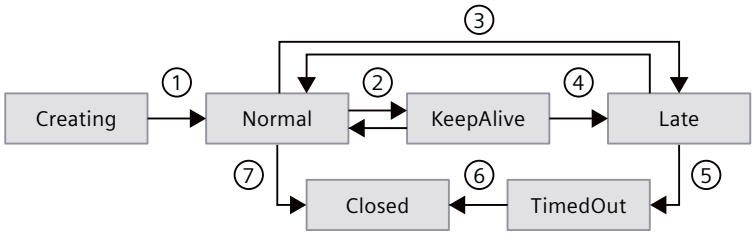
Example

An OPC UA client is connected to an S7-1500 CPU as OPC UA server and generates a subscription in the server.

The diagnostic options for subscriptions are selected in the OPC UA properties of the CPU.

The "Creating" and "Normal" states are entered one after the other with the corresponding subscription ID in the diagnostic buffer.

Subscription states and state transitions



① Subscription is generated and is then active.
② Status change is not entered in the diagnostic buffer because too many entries may be made in the diagnostic buffer depending on the amount of data.
③ See explanation in table for "Late"; for example, no requests to send from client.
④ Maximum KeepAlive value reached.
⑤ See explanation in table for "TimedOut".
⑥ Maximum lifetime of subscription reached.
⑦ Client has deleted subscription.

Figure 3-220 Subscription states and state transitions

Description of the subscription states

A subscription in the OPC UA server can have the following states:

Status	Meaning
Creating	Client has requested a subscription in the server; the server creates the subscription.
Normal	Subscription is created in the server and active.
Closed	Client has deleted the subscription.
KeepAlive	Status if the monitored items do not change over a long period of time. These state transitions are not entered in the diagnostic buffer.
Late	Client has generated a subscription with minimal sampling and publishing intervals. The amount of monitored items is not transmitted to the client during this time. Client no longer transmits requests to send (for example, due to failure).

Status	Meaning
TimedOut	The client has requested a subscription. The server can only honor the subscription (send Publish Response) when there is a sufficient number of send requests (Publish Requests) from the client. When the client stops sending subscription requests, the subscription enters the "TimedOut" state after a certain time.

Subscription: Error in the sampling times

As of firmware V2.5 of the SIMATIC S7-1500 CPU, the OPC UA server can transmit the status code "GoodOverload" when using subscriptions, if an overload of the CPU occurs when sampling the items.

As of firmware V2.8 of the SIMATIC S7-1500 CPU, the OPC UA server can also enter this event into the diagnostic buffer.

Requirement

In the OPC UA properties of the CPU, the option "Subscriptions: Sampling time errors" (OPC UA > Server > Diagnostics) is selected.

Error-free subscription

In the case of an OPC UA subscription to various elements (such as tags), the OPC UA server of the SIMATIC S7-1500 must check the elements for value changes at specified intervals (sampling interval). This check, referred to as "sampling", requires some time, which depends on the number and the data type of the items. After the sampling is completed and a publishing request has been received, the server sends the elements to the client.

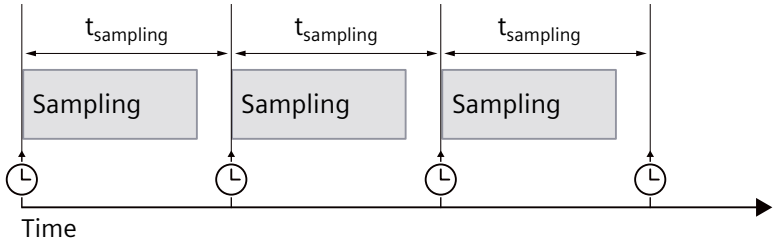
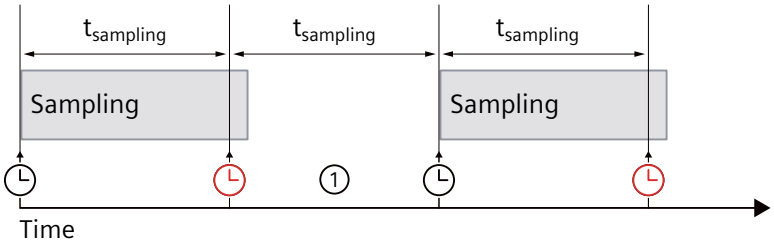


Figure 3-221 Error-free subscription

Subscription with error

If there are too many elements in the queue, there may be an overload of the communication stack. The CPU cannot check all elements in the given sampling interval and must therefore skip the next sampling job.

In this case, the CPU sends the status code "GoodOverload" (0x002F0000) per element, even though the elements were not checked. The meaning of the status code according to IEC 61131-3 is as follows: "Sampling has slowed down due to resource limitations".



① Sampling job is skipped

Figure 3-222 Subscription with error

See also FAQ 109763090 (https://support.industry.siemens.com/cs/ww/en/view/109763090).

More information

You can find information about the server settings for subscriptions in the section Settings of the server for subscriptions (Page 252).

11.3.7.8 Summarizing diagnostics

To prevent the diagnostics buffer being "swamped" by large numbers of identical OPC UA diagnostics, as of STEP 7 V16 service pack 1, you can set parameters so that these diagnostics are entered in the diagnostics buffer as group alarm. Per interval (monitoring time), the CPU then only generates one group alarm per OPC UA diagnostics.

The following sections describe which diagnostics the CPU groups together and how the process runs with a high message volume.

Requirement

The "Summarize diagnostics in case of high message volume" option is activated in the OPC UA properties of the CPU (OPC UA > Server > Diagnostics, "Summarize diagnostics" area).

Example

An OPC UA client repeatedly "overloads" an S7-1500 CPU as OPC UA server with a sampling rate that the server cannot handle (overload).

The "Summarize diagnostics in case of high message volume" setting is activated.

A message appears in the diagnostics buffer for this diagnostic option. It states that the sampling rate cannot be reached; followed by the number of these events within the configured interval.

OPC UA diagnostics that can be summarized

The diagnostics listed below each form their own groups (type). Diagnostic events from the same group are combined using the setting "Summarize diagnostics in case of high message volume":

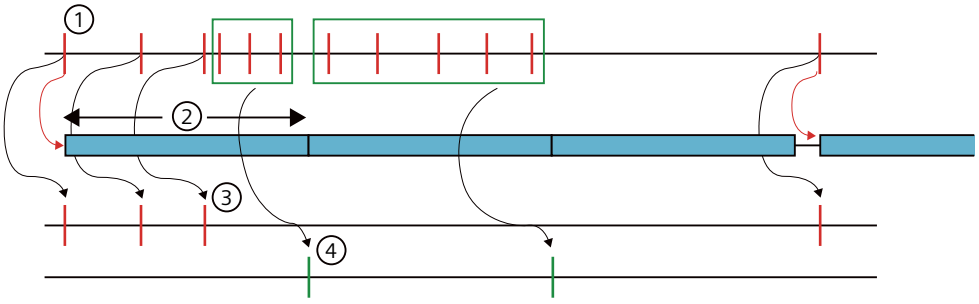
- Incorrect use of an OPC UA service
- OPC UA Service error
- Subscription status has changed
- Sampling rate could not be achieved (subscriptions, overload)
- OPC UA security check failed
- Configuration limit of the OPC UA server violated

Principle of operation

The CPU enters the first three events of an event type in the diagnostics buffer. It then ignores all subsequent diagnostics of this group.

At the end of the monitoring time (interval), the CPU generates a group alarm in which it enters the diagnostics and the frequency of this diagnostics during the elapsed interval. If these diagnostics also occur in the intervals that follow, the CPU only generates one group alarm per subsequent interval.

A diagnostic surge leaves the following pattern in the diagnostics buffer: Three individual messages followed by a series of group alarms. This series can consist of two, three or more group alarms depending on the selected monitoring time and duration of the diagnostic surge.



① Diagnostic results of a group (of a type), for example "Sampling rate could not be reached".

② Interval (monitoring time): When a diagnostic event occurs the first time (or reoccurs), the monitoring time is started (or restarted).

③ Single alarms: The first three diagnostic events from the same group are entered in the diagnostics buffer immediately. Starting with the fourth diagnostic event, the CPU generates only group alarms. If a diagnostic event of this group occurs after a pause of at least one interval, the CPU enters a single alarm in the diagnostics buffer and restarts the monitoring time.

④ Group alarms: After three diagnostic events, the CPU only generates a group alarm as a summary of all additional diagnostic events in this interval. If these diagnostic events also occur in the intervals that follow, the CPU only generates one group alarm per subsequent interval.

Figure 3-223 Summary of diagnostics

11.4 Using the S7-1500 CPU as an OPC UA client

11.4.1 Overview and requirements

With STEP 7 (TIA Portal) Version V15.1 and higher, you can assign parameters and program an OPC UA client that can read PLC tags in an OPC UA server. Furthermore it is possible to transfer new values for PLC tags to an OPC UA server. In addition, you can call methods that an OPC UA server provides in your user program. You use the instructions for OPC UA clients in your user program for this.

The instructions of the OPC UA client are based on the standard "PLCopen OPC UA Client for IEC61131-3".

PLCopen specification

With these standardized instructions, you can develop an OPC UA client functions in your user program that can be executed in an S7-1500 CPU.

In addition, it is possible with just a few adaptations to run this user program in controllers of other manufacturers if these manufacturers have also implemented the OPC UA Specification "PLCopen OPC UA client for IEC61131-3".

Convenient editors in STEP 7

For the parameter assignment of the instructions for OPC UA clients, a convenient editor is available in the TIA Portal – the connection parameter assignment (Page 245).

As of Version 15.1, STEP 7 also features an editor for client interfaces (Page 351).

This section describes how you work with these editors.

First, you will be shown how to create and configure a new interface with the interface editor, because you need this type of interface for the subsequent connection parameter assignment.

The description uses an example for better comprehensibility, see Description of the example (Page 350).

Requirements

- You have the required runtime license for OPC UA and have configured the license in STEP 7 (CPU Properties > Runtime Licenses).
- The client of the S7-1500 CPU is activated.

To use the client of the S7-1500 CPU, you must enable it:

1. Select the area "OPC UA > Client" in the properties of the CPU.
2. Select the "Enable OPC UA client" option.

If you do not enable the client, the connection is not established. You receive a corresponding error message at the instructions, for example "OPC_UA_Connect".

For information about the application name, which also applies to the server and the client, see here (Page 245).

Overview

To use the editor and the connection parameter assignment, follow these steps:

1. First, specify a client interface. Add to this the PLC tags and PLC methods interface that you want to access ("First step (Page 351)").
2. Next, configure the connection to the OPC UA server (Second step (Page 365)).
3. Finally, use the configured connection for the OPC UA client instructions (Third step (Page 375)).

11.4.2 Useful information about the client instructions

With the standardized OPC UA client instructions you are able to control communication for the following tasks with the S7-1500 CPU as an OPC UA client:

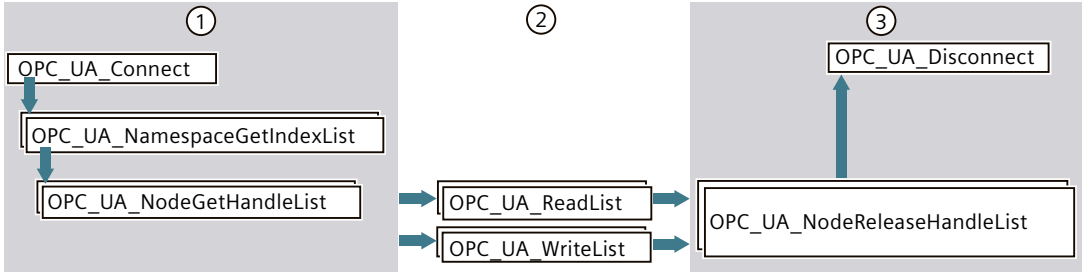
- Read/write tags of the OPC UA server
- Call methods in the OPC UA server

Optional instructions can be used to determine the following information:

- The status of the connection between the OPC UA client and OPC UA server
- Node IDs of nodes with known hierarchy of the address space

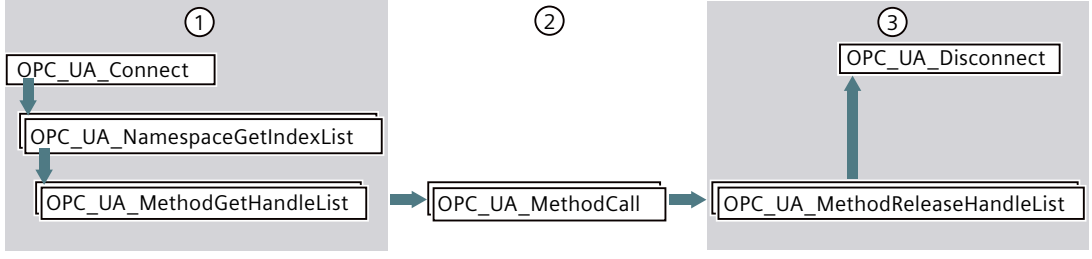
Standardized sequence of OPC UA communication

The sequence of the communication, and thus the order of the instructions, follows a pattern that is illustrated in the following.



① Instructions for preparation of read and write operations
② Read and write instructions
③ Instructions for "clean-up" after a completed read or write operation

Figure 3-224 Run sequence for a read or write operation

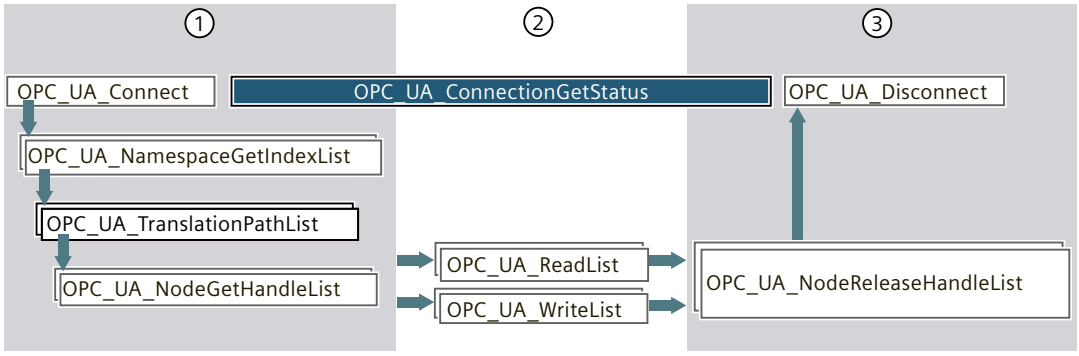


① Instructions for preparation of method calls
② Method calls
③ Instructions for "clean-up" after completed method calls

Figure 3-225 Run sequence for a method call in the OPC UA server

Optional instructions (reading out the status of a connection / reading out node IDs of nodes with known hierarchy of the address space)

- OPC_UA_ConnectionGetStatus
- OPC_UA_TranslatePathList



① Instructions for preparation of read and write operations with inserted instruction for requesting, for example, the NodeIDs of nodes of the OPC UA server.

② You can determine the connection status between the establishment and termination of the connection in parallel with other instructions.

③ Instructions for "clean-up"

Figure 3-226 Run sequence of optional instructions

Convenient editors in STEP 7

The OPC UA client instructions are described in detail in the reference part (STEP 7 information system). For parameter assignment of the instructions, a convenient editor is available in the TIA Portal – the connection parameter assignment (Page 365).

We recommend starting with the connection parameter assignment for the first program draft and using additional instructions and manually optimizing the program as required.

Information about the client instructions

The client instructions are described in detail in the help to the Instructions > Communication > OPC UA > OPC UA client.

Application example in Online Support

This application example (https://support.industry.siemens.com/cs/ww/en/view/109762770) provides you with an S7 user block "OpcUaClient" that summarizes the most important functions of the OPC UA instructions, accelerates the implementation for you and simplifies the programming. The OPC UA server in the example is an S7-1500 controller with a simple simulation program for process values.

The S7 user block performs the following:

- Establishment and termination of the connection to the server
- Diagnostics of the connection and automatic reconnection after connection terminations
- Registered Read
- Registered Write
- Registered Method Call

11.4.3 Number of client instructions that can be used simultaneously

Maximum number of simultaneously running jobs for asynchronous instructions for OPC UA

The maximum number of simultaneously running jobs for asynchronous instructions for OPC UA can be found in the respective equipment manual in the technical specifications section or on the Internet (https://sieportal.siemens.com/su/blVMV).

For the OPC UA instructions for session management or data access, you need the following values from the technical specifications to calculate the maximum number of jobs running at the same time:

- Number of connections, max.
- Number of simultaneous calls of the client instructions for session management, per connection, max.
- Number of simultaneous calls of the client instructions for data access, per connection, max.

In addition to the OPC UA instructions, the following table shows the use and calculation of the maximum number of jobs running at the same time.

OPC UA instruction	Use	Calculation
OPC_UA_Connect	Session management	"Number of connections, max." multiplied by "Number of simultaneous calls of the client instructions for session management, per connection, max."
OPC_UA_NamespaceGetIndexList		
OPC_UA_NodeGetHandleList		
OPC_UA_MethodGetHandleList		
OPC_UA_TranslatePathList		
OPC_UA_NodeReleaseHandleList		
OPC_UA_MethodReleaseHandleL-ist		
OPC_UA_Disconnect		
OPC_UA_ConnectionGetStatus		
OPC_UA_ReadList	Data access	"Number of connections, max." multiplied by "Number of simultaneous calls of the client instructions for data access, per connection, max."
OPC_UA_WriteList		
OPC_UA_MethodCall		The value can be taken directly from the technical specifications.

Maximum number of usable OPC UA client interfaces

If you create OPC UA client interfaces using the connection parameter assignment, the number of client interfaces is limited to 40.

Create the OPC UA client interfaces by double-clicking the "Add new client interface" symbol in the project tree of the "OPC UA communication" area.

The maximum number of OPC UA client interfaces is independent of whether you also use the CPU as OPC UA server.

11.4.4 Example configuration for OPC UA

The following sections describe how you can use the client interfaces editor and the connection parameter assignment.

The description is based on a specific example: Two S7-1500 CPUs operate in the system: One CPU serves as the OPC UA client and the other as the OPC UA server.

You can, of course, also use controllers, sensors and IT systems of other manufacturers as OPC UA clients or servers. In particular, the data exchange between different systems (interoperability) is a major advantage of OPC UA.

Connection parameter assignment using an example:

The plant produces blanks in a production line.

The following controllers are used:

1. An S7-1511 CPU serves as the controller of the production line.
   The controller is named "**Productionline**" in the example.
   The OPC UA server of the controller is enabled.
   The CPU has the IP address 192.168.1.1 in the example.
   This CPU publishes the values of following tags via the OPC UA server:
   - **NewProduct**
     The tag has the data type "BOOL".
     When this PLC tag has the value TRUE, the production line has processed a blank.
     The blank is ready for pick-up.
   - **ProductNumber**
     This tag contains the identification number of the blank.
     The tag has the data type "Int".
   - **Temperature**
     This tag contains temperature values recorded during the production of the blank.
     The tag is an array with elements of the "Real" data type.

   In addition, this CPU provides the following writable tag:
   - **ProductionEnabled**
     The tag is set by the OPC UA client.
     The tag has the data type "BOOL".
     If the value is set to TRUE, the production line is released and may produce blanks.

   In addition, this CPU provides the following method via the OPC UA server:
   - **OpenDoor**
     OPC UA clients can hereby arrange for an access door to be opened to the production line.

2. An S7-1516 CPU controls the interaction with other production lines.
   This CPU is named "**Supervisor**" in the example.
   The OPC UA client of this CPU is enabled.
   Using OPC UA, this CPU can read the NewProduct and ProductNumber tags, set the ProductionEnabled tag and call the OpenDoor method.
   The CPU has the IP address 192.168.1.2 in the example.

The following figure shows the example in the network view of the TIA Portal:

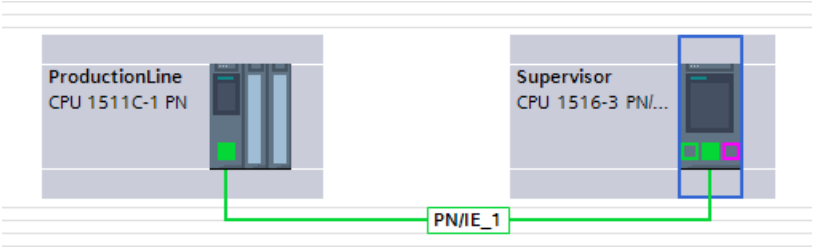


Figure 3-227 Example of assigning connection parameters in the network view

11.4.5 Creating client interfaces

As of Version 15.1, the TIA Portal has an editor for client interfaces.

You group all PLC tags that you want to read or write from an OPC UA server in a client interface.

In addition, the client interface contains all methods that the OPC UA server provides and that you want to call with your user program (that acts as an OPC UA client).

If you create a client interface, STEP 7 also creates data blocks for the parameter assignment of the connection to the OPC UA server from which you want to read data or to which you want to write data.

Maximum number of client interfaces
You can create a maximum of 40 client interfaces.

Editor for client interfaces

To create a client interface, follow these steps:

1. Select the project view in the TIA Portal.
2. In the "Devices" area, select the CPU you want to use as an OPC UA client.
3. Click "OPC UA communication > Client interfaces".

4. Double-click "Add new client interface".
   STEP 7 creates a new client interface and display in the editor.

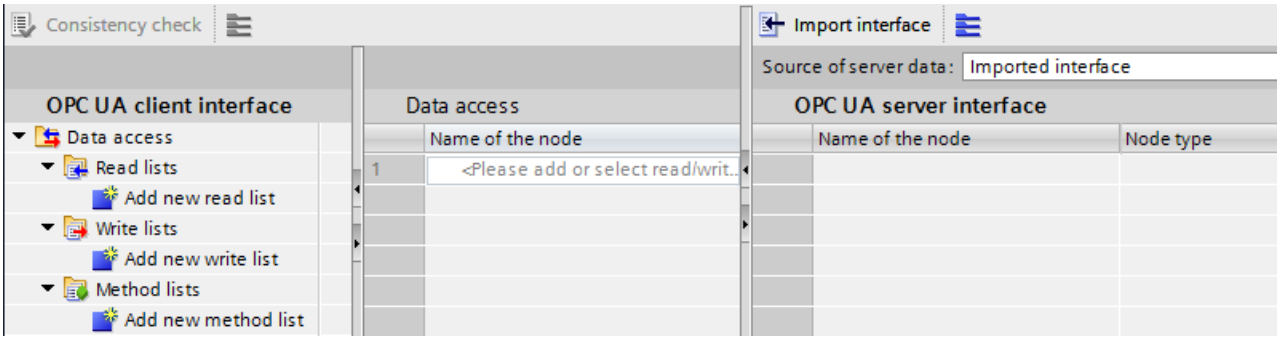


Figure 3-228 Adding OPC UA client interface

   STEP 7 names the new interface "Client interface_1". If a "Client interface_1" already exists, the new interface receives the designation "Client interface_2" etc.
   In addition, STEP 7 creates the following data blocks:
   – Client_Interface_1_Configuration
     The data block already contains all system data types that are needed for the instructions of the OPC UA client.
     This data block is filled when you configure the connection to the OPC UA server.
     You configure a connection in the properties of the client interface, see: Example configuration for OPC UA (Page 350).
   – Client_Interface_1_Data
     A data block for the PLC tags that you want to read or write from an OPC UA server as well as for methods that you want to call in the OPC UA server.
     You use this data block in your user program.
     This data block is currently still empty.
5. Select a descriptive name for the new client interface.
   Select "Productionline" in the example.
   This also changes the names of the associated data blocks to:
   – Productionline_Data
   – Productionline_Configuration
6. To import an OPC UA server interface, click the "Import interface" button in the top right of the editor.
   This allows you to import an XML file which describes the server interface of an OPC UA server.
   Alternative: To determine online the server interface of a connected OPC UA server, see: Determine server interface online (Page 358).
7. STEP 7 displays a dialog with which you can select an XML file.
   This XML file describes a address space of an OPC UA server.
   The address space of an OPC UA server contains all PLC tags and server methods published by an OPC UA server.
   OPC UA clients can access this address space:
   - Read PLC tags
   - Write PLC tags

- Calling Server Methods

The address space of an OPC UA server can be divided into one or more server interfaces.

For creating server interfaces, see: Creating a server interface for companion specification (Page 278).

8. Create a **read list** in this client interface.

   To do this, follow these steps:

   – Click "Add new read list" in the left section of the editor.

     STEP 7 adds a new list named "ReadList_1".

     For the example, change the name to "ReadListProduct"

   – Now add the new read list of the PLC tags that you want to read from the OPC UA server.

     In the example the "NewProduct" and "ProductNumber" tags are added to the "ReadListProduct" read list.

     Select the "NewProduct" tag in the right-hand field of the editor ("OPC UA Server interface"). Drag the "NewProduct" tag to the "ReadProduct" read list in the middle field of the editor. Follow the same procedure with the "ProductNumber" tag.

   The figure below shows the right field of the editor.

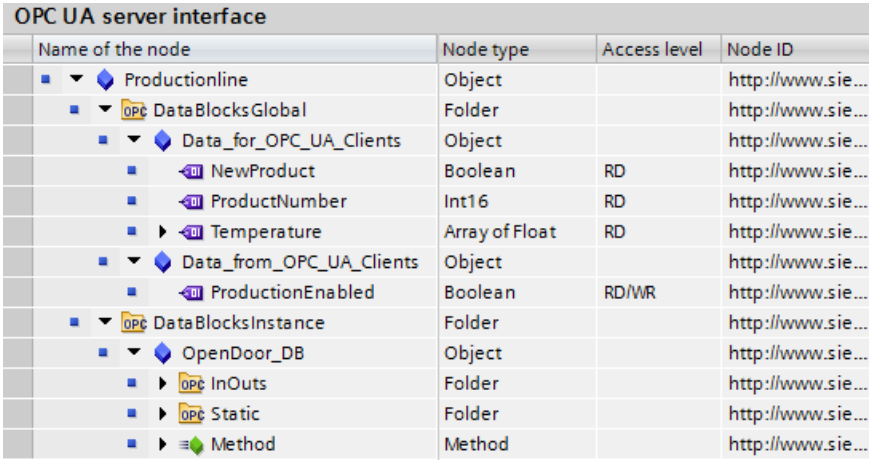


Figure 3-229 Read list in the OPC UA server interface

Alternative:

You can also select a new read list by dragging the right field of the editor ("OPC UA Server interface") to a node of the type Object or Folder and then dragging it to "Add new read list" in the left field of the editor. The new read list then contains all PLC tags of the node that has been moved.

In the example, select the object "Data_for_OPC_UA_Clients", which contains the tags "NewProduct" and "ProductNumber". STEP 7 generates the new read list "Data_for_OPC_UA_Clients". In addition, the object contains the tag "Temperature". Delete the "Temperature" tag from the read list. Since they should not be read in the example.

Change the name of the read list in "ReadListProduct".

The following figure shows the content of the read list:

ReadListProduct

Name of the node	Node type	Access level	Node ID
NewProduct	BOOL	RD	http://www.siemen...
ProductNumber	INT	RD	http://www.siemen...

Figure 3-230 Read list

NOTE

Read and write lists do not support all node types.
The OPC UA client of the S7-1500 CPU does not support all OPC UA data types (node types) that can be made available via an OPC UA server interface. If you place an unsupported node type, for example, in a read list or write list a corresponding error signal appears. In this case, you cannot include the corresponding node in the read or write list.
Which types are supported is described here: Mapping of data types (Page 226)

9. If you want assign new values to PLC tags, create a **write list** in this client interface.
   To do this, follow these steps:
   – Click "Add new write list" in the left section of the editor.
     STEP 7 adds a new list with the name "ReadList_1".
     For the example, change the name to "WriteListStatus".
   – Now add the new write list of all OPC UA server tags to which you want to assign new values.
     In the example, add the "WriteListStatus" tag to the write list "ProductionEnabled".
     Select the Tag of right field of the editor ("OPC UA Server interface"). Drag the tag to the write list in the middle field of the editor.

   Alternative:
   You can also create a new write list by selecting a node of the type Object or Folder in the right field of the editor ("OPC UA server interface") and then dragging to "Add new write list" in the left field of the editor.
   The new write list then contains all tags of the relevant node.
   In the example, select the object "Data_from_OPC_UA_Clients", which contains the tag "ProductionEnabled". STEP 7 generates the new write list "Data_from_OPC_UA_Clients". Change the name in "WriteListStatus".
   The following figure shows the content of the write list:

WriteListStatus

Name of the node	Node type	Access level	Node ID
ProductionEnabled	BOOL	RD/WR	http://www.siemen...

Figure 3-231 Write list

10. If you want to call a method of this OPC UA server, generate a new method list.
    To do this, follow these steps:
    – In the left section of the editor, click "Add new method list".
      STEP 7 adds a new list with the name "Method list_1".
      For the example, change the name to "MethodListOpenDoor".
    – Now add a method of the OPC UA server to the new method list.
      In this example, add the method "OpenDoor" to the method list "MethodListOpenDoor".
      Select the method of right field of the editor ("OPC UA Server interface"). Drag the method to the method list in the middle field of the editor.

    Alternative:

    You can also generate a new method list by selecting a method (node of the type Object) in the right field of the editor (OPC UA Server interface) and then dragging it to "Add new method list" in the left field of the editor. The new method list then contains the method of the relevant node.

    The following figure shows the content of the method list:

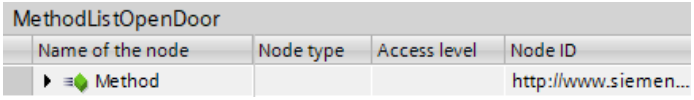


Figure 3-232 Methods list

See also Useful information about server methods (Page 306).

11. Compile the project.
    To do so, select the project and click the following button in the toolbar:



STEP 7 compiles the project and updates the data blocks that belong to the "Productionline" client interface.

NOTE

During compilation, STEP 7 overwrites all data in the data blocks belonging to the client interface. For this reason, you should not add to or modify these data blocks manually.

NOTE

Renaming nod names (DisplayNames)

In read lists, write lists and method lists you can rename the name of a node by means of the shortcut menu. This is the "DisplayName" in the OPC UA language usage.

If you rename the name of a method list node and the node is already used in a programmed block for the method call "OPC_UA_MethodCall", the compilation of the project leads to consistency errors: During the compilation the UDTs of the method are generated with the changed name. The references to the method used in the program are then no longer correct.

To correct the consistency errors, you can either undo the name change of the method in the client interface or navigate to the method call and assign the relevant parameters again there under "Properties > Block parameters" ("Configuration" tab).

Data blocks of client interface

The following data blocks belong to the "Productionline" client interface:

- **Productionline_Configuration**

  A data block for the configuration.

  In the example, this data block is called "Productionline_Configuration".

  The data block already contains all system data types that are needed for the instructions of the OPC UA client.

  In addition, the data block contains general default values for parameter assignment of the connection to an OPC UA server.

  If you are working with connection parameter assignment, this data block will be filled.

- **ProductionLine_Data**

  A data block for the PLC tags that you have entered in the client interface editor.

  In the example, this data block is called "Productionline_Data".

  The figure below shows the data block.

Static	
ReadListProduct	Struct
Variable	"Productionline.ReadListProduct"
NewProduct	Bool
ProductNumber	Int
NodeStatusList	Array[0..1] of DWord
NodeStatusList[0]	DWord
NodeStatusList[1]	DWord
TimeStamps	Array[0..1] of LDT
TimeStamps[0]	LDT
TimeStamps[1]	LDT
WriteListStatus	Struct
Variable	"Productionline.WriteListStatus"
ProductionEnabled	Bool
NodeStatusList	Array[0..0] of DWord
NodeStatusList[0]	DWord
MethodListOpenDoor	Struct
MethodStatusList	Array[0..0] of DWord
MethodStatusList[0]	DWord
MethodResultList	Array[0..0] of DWord
MethodResultList[0]	DWord
Method	Struct
Inputs	"Productionline.MethodListOpendoor.Method.Inputs"
Number	Int
Outputs	"Productionline.MethodListOpendoor.Method.Outputs"
Result	Int

Figure 3-233 "Productionline_Data" data block

Use the "Productionline_Data" data block in your user program and access the read values of the "NewProduct" and "ProductNumber" PLC tags. This is explained in the following section using an example.

Reading and writing PLC tags of the client interface

Example: Reading the "ProductNumber" value

For example, you write in an SCL program:

```
#MyLocalVariable :=
"Productionline_Data".ReadListProduct.Variable.ProductNumber;
```

You use this, for example, to assign the number of the blank that was just produced in the production line to the local tag "#MyLocalVariable".

Requirements:

- A connection exists to the OPC UA server of the CPU, which controls the production line.
- The OPC UA client has read the current values.

For this reason you check whether a read value is valid:

- Check whether the value in "Productionline_Data".ReadListProduct.NodeStatusList[1] is equal to 0.
- Optional: Check when this value was sent from the OPC UA server. This value is in "Productionline_Data".Product.TimeStamps[1]. If no time stamp is requested, the communication load is reduced.

Example: Writing the "ProductEnabled" value

Transfer the new values for PLC tags, in the example for the "ProductionEnabled" tag, to the OPC UA server using the data block.

With the following assignment, you enable the production line in the example plant:

```
"Productionline_Data".WriteListStatus.Variable.ProductionEnabled :=
TRUE;
```

This is only successful, however, if the following requirements are met:

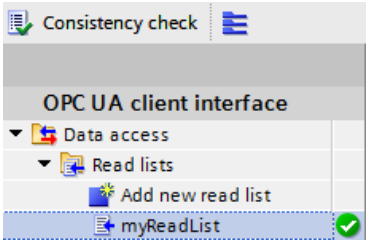
- A connection exists to the OPC UA server of the CPU, which controls the production line.
- Current values are being written via the OPC UA client

Consistency check

Finally, check the consistency of the read/write list or method list.

1. Select the list that you want to check.
2. Click the "Consistency check" button above the "OPC UA client interface" area.

A green check mark indicates an error-free assignment of the tags or methods to the corresponding elements of the server interface.



You can assume that the data exchange between client and server and method calls operate without problem in runtime.

In the event of an error a list appears in the Inspector window. From this list you can jump to the respective error.

During the consistency check, STEP 7 checks:

- Whether all elements that you use in the respective list are also present in the server.
- Do the data types used match?
- For methods: Do the number, name, order, and data types of method arguments match?

11.4.6 Determine server interface online

With STEP 7 (TIA Portal) you can determine the interface of an OPC UA server online. This provides information on which tags of a connected OPC UA server you can read or set (write) with OPC UA clients. It also provides information on which server methods of the OPC UA server are available for OPC UA clients.

If you are work offline you can create the interface of the OPC UA server by means of an OPC UA XML file. The address space of the server is described in the OPC UA XML file, see: Export OPC UA XML file (Page 244).

Determine online server interfaces

To determine a server interface online, follow these steps:

1. In the STEP 7 project tree, select the CPU which is configured as OPC UA client (Supervisor in the example).
2. Select the client interface (in the example, OPC UA Communication > Client interfaces > Productionline).
   If no client interface has been created, double-click "Add new client interface".
3. Double-click the selected client interface.
   The editor for client interfaces is displayed.

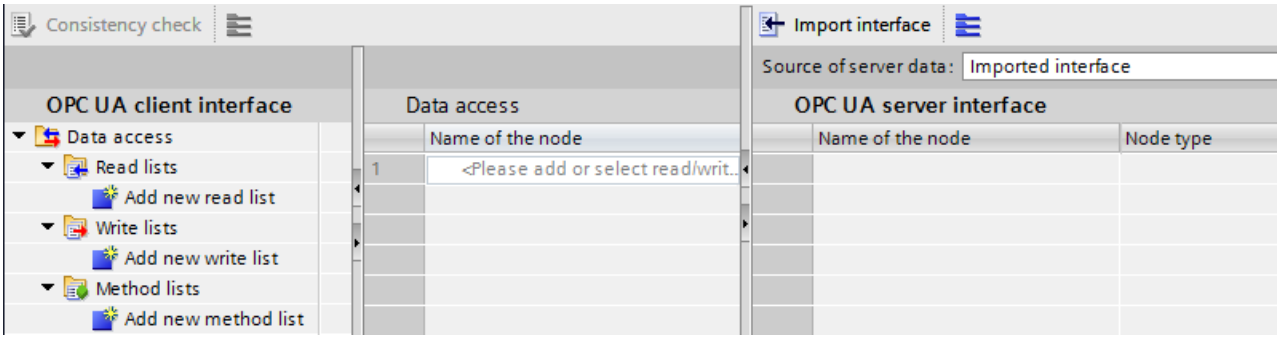


Figure 3-234 Editor for client interface

4. In the left section of the editor, click "Add new read list", "Add new write list", or "Add new method list".
5. In the right field of the editor, select "Online[]" as data source for "Source of server data":



6. Click the "Online Access" button.
   STEP 7 displays the "Connect to OPC UA server" dialog.

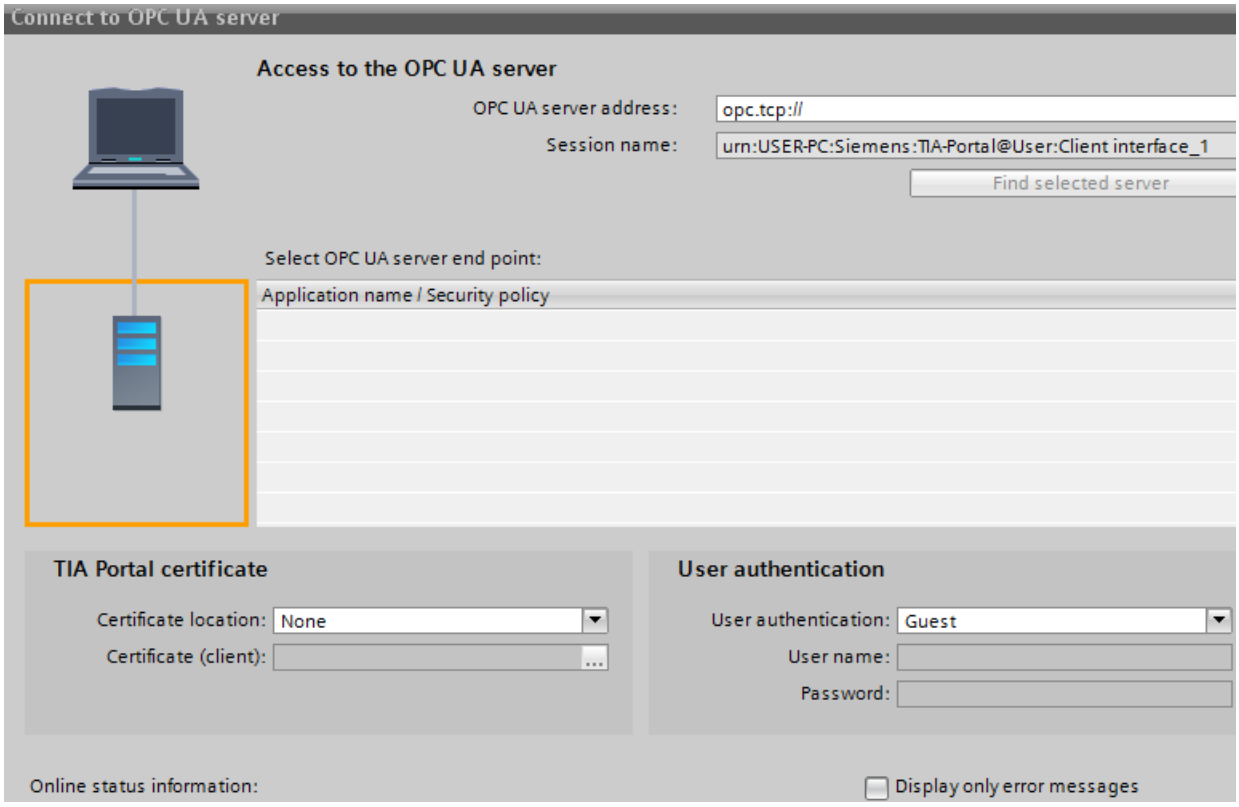


Figure 3-235 "Connect to OPC UA server" dialog

Tip: When establishing an online connection to an OPC UA server for the first time, use the "Online access" button. When reconnecting after a disconnection, select the "Connect to Online Server" button next to the "Online" selection field.

In the top right, enter the IP address of the OPC UA server whose server interface you want to determine online.

7. Click "Find selected server".
   STEP 7 establishes a connection to the OPC UA server and determines all security settings (server endpoints) that the server holds in readiness.
   STEP 7 displays the end points as list:



Figure 3-236 Found OPC UA server with all server endpoints

8. Click on the end point you want to use for a connection of STEP 7 to the OPC UA server.

9. Do you want to use a secure connection?
   - If you have selected a secure end point, then select the entry "TIA Portal" for the "Certificate location".

     And under "Certificate (Client)", select a client certificate for your PC on which STEP 7 (TIA Portal) is currently running.

     If a client certificate does not yet exist for your PC, you can generate a client certificate here in the TIA Portal.

     Proceed as follows to generate a certificate for your PC:

     - Click on the button in the "Certificate (Client)" input field.

     - Click "Add".

     - For "Certificate owners" enter "STEP 7 (TIA Portal)".

     - Select the "OPC UA client" entry at "Usage".

     - For "Subject Alternative Name (SAN)", enter the IP address of your PC, on which you are currently running STEP 7 (TIA Portal), under "Value". Overwrite the already entered IP address.

     - If your PC uses a second IP address, enter this address as well. If your PC does not use a second IP address, delete the second IP address already entered.

     - Click "OK".
   - If you have not selected a secure end point, then keep the default ("None").
10. How do you want log on?
    - If you want to log onto the OPC UA server as guest, then apply the default with "User authentication".
    - If you want to log on with user name and password, select "User name and password".

      Use the user name and password which was stored during the configuration of the OPC UA server in the properties of the CPU under "General > OPC UA > Server > Security > User authentication > User management".
11. Click on the "Go online" button.

    When a secure connection is established, a message appears that you must accept the server certificate for the secure connection to be established. In the message window, you can display further details about the server certificate via a link.

    This standard Windows window only provides information about the server certificate. If you click on the button to install the server certificate, the server certificate is not saved to the certificate memory of the TIA Portal, i.e. at the next connection attempt you will be prompted again to accept the server certificate.

    STEP 7 then establishes a connection to the OPC UA server and again displays the editor for client interfaces.

    In the right field of the editor, STEP 7 displays the uppermost level of the address space of the OPC UA server:

12. Click on the small black triangle next to "Objects".

    STEP 7 now also displays the level below Objects.
13. Click on the small black triangle next to "Productionline".

    STEP 7 now also displays the level below Productionline.

14. Now open additional lower-level folders:

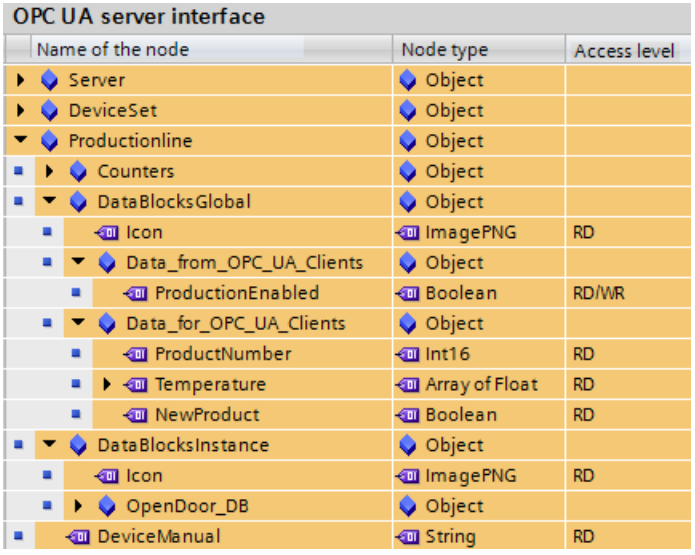


Figure 3-237 Online view of OPC UA server interface

More information

You can find information about mapping of data types in the section Mapping of data types (Page 226).

For information on how to create a client interface, refer to the section Creating client interfaces (Page 351).

11.4.7 Using multilingual texts

In the client interface editor, you are also importing texts that can be displayed in different languages with the OPC UA XML files (information models). Multilingualism is optional, and each node can be defined differently regarding the languages it offers.

In the XML file, these are the following fields that can be prepared for different languages:

- Display name
- Description

Example for multilingual texts in an OPC UA XML file

In the XML file below, the display name and the description, for example, are entered with a "default" text and multiple localizable texts.

- Default text is the first entry without localization information.
- Localized text is the text after "Locale=" followed by a language code, e.g. "it-IT" for Italian

```
<UAVariable NodeId="ns=3;i=6070" BrowseName="3:EngineeringRevision" ParentNodeId="ns=3;i=1002"
DataType="String">
    <DisplayName>EngineeringRevision</DisplayName>
    <DisplayName Locale="en-US">EngineeringRevision</DisplayName>
    <DisplayName Locale="de-DE">Revisionsstand</DisplayName>
    <Description>Revision Level of the engineering environment.</Description>
    <Description Locale="en-US">Revision Level of the engineering environment.</Description>
    <Description Locale="de-DE">Revisionsstand der Engineeringumgebung.</Description>
    <Description Locale="fr-FR">Niveau de révision de l'environnement d'ingénierie.</Description>
    <Description Locale="it-IT">Livello di revisione dell'ambiente di ingegneria.</Description>
<References>
    <Reference ReferenceType="HasTypeDefinition">i=68</Reference>
    <Reference ReferenceType="HasModellingRule">i=78</Reference>
</References>
</UAVariable>
```

Figure 3-238 Example of multilingual texts in an OPC UA XML file

Display of multilingual texts

When importing a server interface, the available multilingual texts are saved internally and downloaded to a CPU together with the project.

The client editor displays the text from the OPC UA XML file in the columns "Name of the node" (corresponds to "DisplayName") and "Description" (corresponds to "Description").

The following cascading rules determine which language is shown for a node:

- When the node contains text in the currently used editing language, the text is also displayed in the editing language.

  (Setting the editing language: In the project tree, select the area "Languages & resources > Project languages")
- When the node does not contain text in the editing language but a default text is defined there (without language code), the default text is displayed.
- "Name of the node" column: If no default text is defined either but a text in any other language exists, the DisplayName text is displayed in the first available language. This rule does not apply to description texts.
- If none of the conditions listed above is met, no text is displayed.

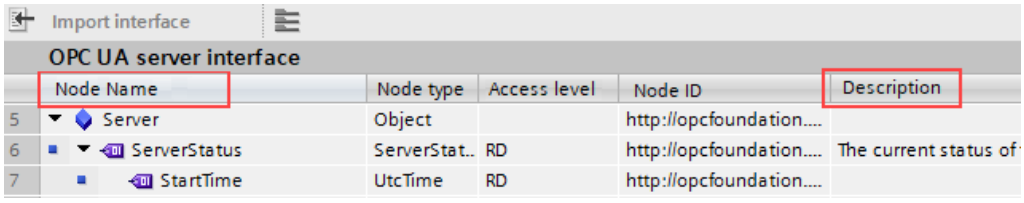


Figure 3-239 Display for multilingual texts

When you change the editing language, the multilingual text in the imported interface will also change according to the rules explained above.

You can then apply the nodes in the corresponding lists (read list, write list, method list) with drag and drop.

You cannot change the language in the lists (read list, write list, method list).

Applying the displayed description texts as comment in PLC data types

When you compile the program, STEP 7 automatically creates PLC data types (UDTs) for each read list, for each write list and for inputs or outputs of each method. These UDTs each have one element for each node.

The UDTs apply the description text as comment according to the rules stated above. STEP 7 creates the comment in only one language, just like the texts in the OPC UA server interface can only be displayed in one language.

11.4.8 Rules for the access to structures

The rules for the access to structures are explained below. Note these rules when reading and writing values of complete structures provided by an OPC UA server.

How the client of the S7-1500 CPU accesses structures

The OPC UA client of the S7-1500 CPU uses neither TypeDictionaries nor DataTypeDefinition attributes, which a server offers for the resolution of these structures.

These options of the OPC UA client for checking structural elements in runtime are limited in the client.

Rules for the access to structures

If you use the client interfaces to configure the read and write lists (connection parameterization) and assign the PLC data types to the imported or online determined address model of the server, the read and write accesses to structures operate trouble-free in runtime.

The configuration by means of client interface automatically ensures that the sequence and the data type of the structural elements are coordinated on client and server side.

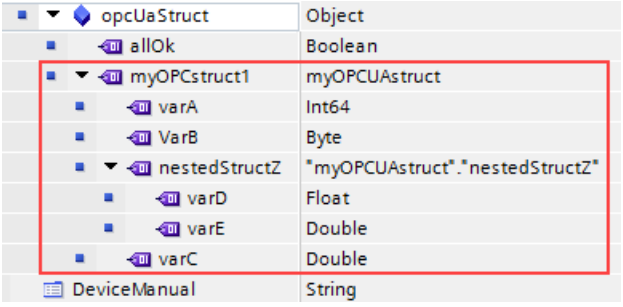
Recommendation: Update an S7-1500 CPU (as server) to the current firmware version (e.g. V2.0 > V2.5.2 or higher).

In runtime the OPC UA client only checks the total length of the transmitted value; more detailed checks are not possible.

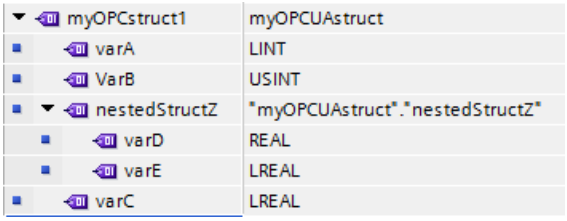
Strings (WSTRING, STRING and OPC UA ByteString) are also permitted in structures. Strings do have a variable length, but OPC UA surmounts this variability: At the time of transfer, a length field in which the length of the string is encoded is prefixed to each string. Therefore, a S7-1500 CPU as a OPC UA client can check the length of a string and determine whether the string "fits into" the assigned CPU tag. In this manner, the CPU can also check the total length of the structure.

Mapping rules apply to the assignment of OPC UA structures to PLC tags or DB tags (see Mapping of data types (Page 226)).

Example of an error-free assignment of the structure elements
In the imported node set file (XML export), the structure is defined as follows:



The structure mapped in the read list matches, both in the order and in the assigned data types, the corresponding nodes of the node set file.



If the structure now changes on the server, for example tagA and tagB are swapped, and the read list remains the same in the client, the assignment is no longer correct:

- The total length of the data remains the same (only the order has changed)
- The configuration of the structure is different for client and server!

⚠ WARNING

No error message in the case of different structure configuration between client and server
If the structures of client and server do not match, this rule violation will possibly not generate any error during compilation and also not in runtime.
Make sure not to change the configured assignments for structures in runtime. If required, reconfigure the assignment in the read and write lists!

11.4.9 Using connection parameter assignment

11.4.9.1 Creating and configuring connections

With the instructions for OPC UA clients, you create a user program that exchanges data with an OPC UA server. A series of system data types are required for this.

To simplify your work with these system data types, a connection parameter assignment for OPC UA clients is available starting in STEP 7 (TIA Portal) Version 15.1.

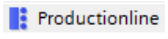
Use of the connection parameter assignment is optional and not mandatory. You can also manually create the required system data types.

We use an example to make the description easier to follow, see description of the example (Page 350).

Opening the connection parameter assignment

To configure the connection to an OPC UA server, follow these steps:

1. In the "OPC UA communication" area, double-click the client interface whose parameters you want to assign in the project tree.
   For the example configuration: Double-click the "ProductionLine" client interface.

   The section "Create client interface (Page 351)" describes how to create a client interface.
2. Click the "Properties" tab (Inspector window) if the tab is not already displayed.
   STEP 7 now displays the connection parameter assignment for the instructions of the OPC UA client.
   The "General" tab is open.
3. Click on the "Configuration" tab and set the connection to the OPC UA server.

Setting the connection parameters

1. Select a descriptive name for the session. For the example, select the name "OPC UA Connection to ProductionLine".
2. In the "Address" field, enter the IP address of the OPC UA server to which your user program (that operates as an OPC UA client) is to establish a connection. In the example configuration, the CPU that controls the production line has the IP address "192.168.1.1". A connection to the OPC UA server of this CPU is to be established. For this reason, you enter this IP address in the "Address" field. In this case, the OPC UA server uses the default port 4840.
   Alternatively, you can enter a valid DNS name in the "Address" field. The length of the DNS name is limited to 242 characters.
   If the address is not valid, the error message is shown: "Enter a valid address".
   If the string of the "Address", "Port" and "Path" fields contains more than 254 characters, an error message is also displayed.

3. Enter a path within the OPC UA server to restrict access to this path. The information is optional. However, some servers only establish a connection if a server path is specified.

   When you specify a path, it is automatically entered at the "ServerEndpointUrl" entry in the configuration DB for the client interface. The entry then consists of the components "OPC Schematic Prefix", "IP address", "Port number" and "Server path", for example: "opc.tcp://192.168.0.10:4840/example/path".

   The following figure shows the entry of the IP address for the OPC UA server:

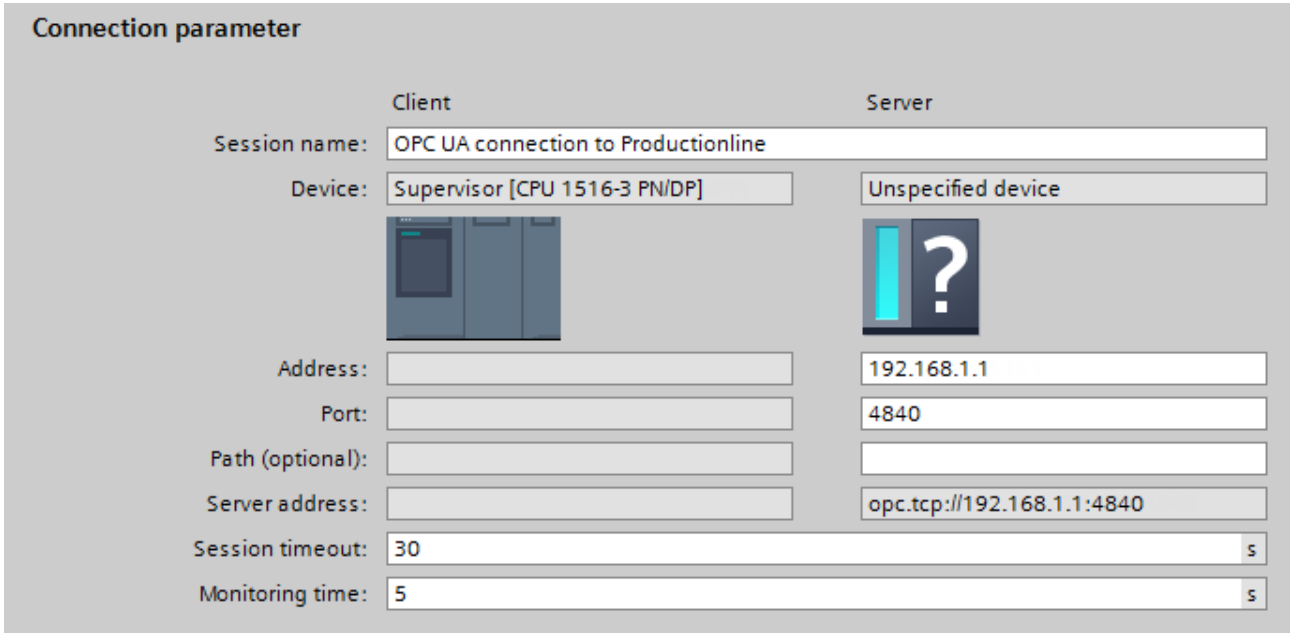


Figure 3-240 Connection parameters

4. If the OPC UA server is not using the standard port 4840, you must insert the port number here.

   For example, enter the number 65535 in the field, if the OPC UA server to which you want to establish a connection uses this port number.

5. In addition, you accept the default settings for session timeout (30 seconds) and monitoring time (5 seconds).

Setting the security parameters

1. Click the "Security" area in the "Configuration" tab.

   This area contains all security settings for the connection to the OPC UA server.

The following settings are possible, for example:

"General" area

Security mode:
In the drop-down menu, select the security mode that the connection to the OPC UA server must fulfill.

If the server does not meet the selected mode, a session is not established.

The following settings are available:

- No security: No secure connection!
- Sign: OPC UA server and OPC UA client sign the data transmission (all messages): Manipulations can thus be detected.
- Sign & Encrypt: OPC UA server and OPC UA client sign and encrypt the data transmission (all messages):

Security policy:
Set the encryption techniques for the signing and encryption of messages.
The following settings are possible:

- No security
- Basic128Rsa15
- Basic256
- Basic256Sha256

To configure a secure connection, you must observe the following items:

- A certificate is required for the client for a secure connection.
- You have to make the client certificate known to the server.

To find out how to proceed, see the section "Handling client and server certificates (Page 255)" under "Certificate of the OPC UA client".

"Certificates" area

Client certificate/client certificate folder:
Depending on the selected certificate handling (via TIA Portal or via GDS), select either a client certificate or the desired client certificate folder. Both options confirm the authenticity of the OPC UA client.
Click the following icon to select:



STEP 7 displays a list of certificates and services.
Select the certificate that you have made known to the server.
For client certificate management via GDS, select the corresponding client certificate folder.
Click the symbol with the green check mark:



Or create a new certificate or a new certificate folder. To do this, click the "Create" symbol.
If you create a new certificate, you must make this certificate known to the server.

"User authentication" area
The following settings are possible for user authentication:

- Guest
- User name and password
- Users (TIA Portal - Security Settings)

For more information, see Users and roles with OPC UA function rights (Page 266).

Setting languages

UA tags of the String type can be localized with OPC UA, that is, texts (values for the UA tag) can be available in different languages for the server. For example, localized texts can be available for DisplayName (Name of the node) and Description (Description).

In the "Languages" area of the "Configuration" tab you can, for example, influence the language of the texts returned by the server as follows:

In the "Languages" area, enter a number of languages that the server transfers to the client during connection setup.

The language or the local ID ("language code") associated with it that you enter in the first line is the language preferred by the client.

- If the server can provide the UA tag in the requested language, it is transferred to the client.
- If the server cannot provide the UA tag in the requested language, it checks whether it can provide the UA tag in the language you have entered in the second line (first substitute language).
- The server works its way down the list, and when it can provide neither the requested language nor a substitute language, it will provide the default language.

More information

What causes the connection to an OPC UA server to fail? FAQ.
(https://support.industry.siemens.com/cs/ww/en/view/109766709)

11.4.9.2 Handling of the client certificates of the S7-1500 CPU

Where does the client certificate come from?

If you are using the OPC UA client of an S7-1500 CPU (OPC UA client enabled), you can create certificates for these clients with STEP 7 V15.1 and higher as described in the following sections.

When you use UA clients from manufacturers or the OPC Foundation, a client certificate is generated automatically during installation or upon the first program call. You have to import these certificates with the global certificate manager in STEP 7 and use them for the respective CPU.

If you program an OPC UA client yourself, you can generate certificates through the program. Alternatively, you can generate certificates with tools, for example with OpenSSL or the certificate generator of the OPC Foundation:

- The procedure for OpenSSL is described here: "Generating PKI key pairs and certificates yourself (Page 187)".
- Working with the certificate generator of the OPC Foundation is described here: "Creating self-signed certificates (Page 186)".

Certificate of the OPC UA client of the S7-1500 CPU

A secure connection between the OPC UA server and an OPC UA client is only established if the server classifies the certificate of the client as trusted.

Therefore you have to make the client certificate known to the server.

The following sections describe how you can initially generate a certificate for the OPC UA client of the S7-1500 CPU and then make it available to the server.

1. Generate and export a certificate for the client

For a secure connection you have to generate a client certificate and - if the server and client are located in different projects - export the certificate.

If client and server are in the same project, exporting the client certificate and subsequent import are not necessary.

Requirements

The IP interface of the CPU is configured, an IP address is available.

Background: The IP address under which the CPU can be accessed in your system is entered under "Subject Alternative Name (SAN)".

Creating an OPC UA Client certificate

The easiest way to generate a client certificate for an S7-1500 CPU is to configure a client interface.

The configuration of the client interface provides for the selection or generation of a client certificate, see Creating and configuring connections (Page 365).

Alternatively, you can generate the client certificate as follows:

1. In the project tree, select the CPU you want to use as a client.
2. Double-click "Device configuration".
3. In the properties of the CPU, click "Protection & Security > Certificate manager".
4. Double-click "<Add new>" in the "Device certificates" table.
   STEP 7 opens a dialog.
5. Click the "Add" button.
6. Select the "OPC UA client" entry from the "Usage" list.
7. Click "OK".
   STEP 7 now shows the client certificate in the "Device certificates" table.
8. If the server is in another project: Right-click this line and select "Export certificate" from the shortcut menu.
9. Select a directory where you will store the client certificate.

2. Announcing the client certificate to the server

You have to make the client certificate available to the server to allow a secure connection to be established.

To do this, follow these steps:

1. If the client was configured in another project and you created and exported the client certificate there:
   - Select the "Use global security settings for certificate manager" option in the local certificate manager of the server. This makes the global certificate manager available.
     You will find this option under "Protection & Security > Certificate manager" in the properties of the CPU that is acting as server.
   - If the project is not yet protected, select "Security settings > Settings" in the STEP 7 project tree, click the "Protect this project" button and log on.
     The "Global security settings" item is now displayed under "Security settings" in the STEP 7 project tree.
   - Double click "Global security settings".
   - Double click "Certificate manager".
     STEP 7 opens the global certificate manager.
   - Click the "Device certificates" tab.
   - Right-click in the tab on a free area (not on a certificate).
   - Select the "Import" shortcut menu.
     The dialog for importing certificates is displayed.
   - Select the client certificate that the server is to trust.
   - Click "Open" to import the certificate.
     The certificate of the client is now contained in the global certificate manager. Note the ID of the client certificate just imported.
2. Click the "General" tab in the properties of the CPU that is acting as server.
3. Click "OPC UA > Server > Security > Secure Channel".
4. Scroll down in the "Secure Channel" dialog to the section "Trusted clients".
5. Double-click in the table on the empty row with "<add new>". A browse button is displayed in the row.
6. Click this button.
7. Select the prepared client certificate.
8. Click the button with the green check mark.
9. Compile the project.
10. Load the configuration onto the S7-1500 CPU (server).

Result

The server now trusts the client. If the server certificate is also considered trusted, the server and client can establish a secure connection.

11.4.9.3 Handling client certificates during runtime

For CPUs with FW version V4.0, the OPC UA server and the web server already support certificate management during runtime via GDS (Global Discovery Server). If you are using a CPU as of FW version V4.1, the certificate manager informs you in the CPU properties that additional services (OPC UA client) support certificate management during runtime. This also applies if you change an already configured CPU to FW version V4.1.

Effects of the update

CPUs with FW version V4.1 offer the option of integrating additional services into the certificate management during runtime in the CPU properties (Protection & Security > Certificate manager). To be able to update the certificate management for the OPC UA client during runtime, the OPC UA server and GDS Push of the CPU must be enabled. If these requirements are met, you can update the certificate management in runtime. Updating the certificate management in runtime has the following effects:

- Certificate management in runtime is enabled for the OPC UA client of the CPU.
- Existing certificates are still stored on the CPU or in STEP 7 and must be deleted manually.
- When updating the certificate management during runtime, existing certificates and the associated IDs are not transferred. Consequently, the user must adapt the user program in the appropriate places, e.g. in the program blocks for OPC UA.
- The "ManagedApplications" node is created in the namespace of the OPC UA server. After the update, this node contains all certificates that do not belong to the OPC UA server, e.g. the certificates of OPC UA clients or the web server.

NOTE

Previous settings can only be restored by performing a complete reset

The updated certificate management during runtime cannot be undone.

To restore the previous settings, you must replace the CPU with a CPU with FW version V4.0 in STEP 7. In addition, STEP 7 V21 must be reset to STEP 7 V20.

Procedure for updating the certificate management in runtime

The "Update certificate management at runtime" button can only be selected if you replace a configured CPU with FW version lower than V4.1 with a CPU with FW version V4.1.

To activate the certificate management at runtime, proceed as follows:

1. Select the required CPU in the device or network view of STEP 7.
2. In the Inspector window, navigate to "Properties > General > Protection & Security > Certificate manager".
3. In the "Configuration of certificate manager" area, select the option "Use certificates provided by certificate manager during runtime".
4. Click the "Update certificate management during runtime" button.
   STEP 7 displays a warning with the additional services and possible cases in which you need to adapt the user program.
5. Click Yes if you want to perform the update.

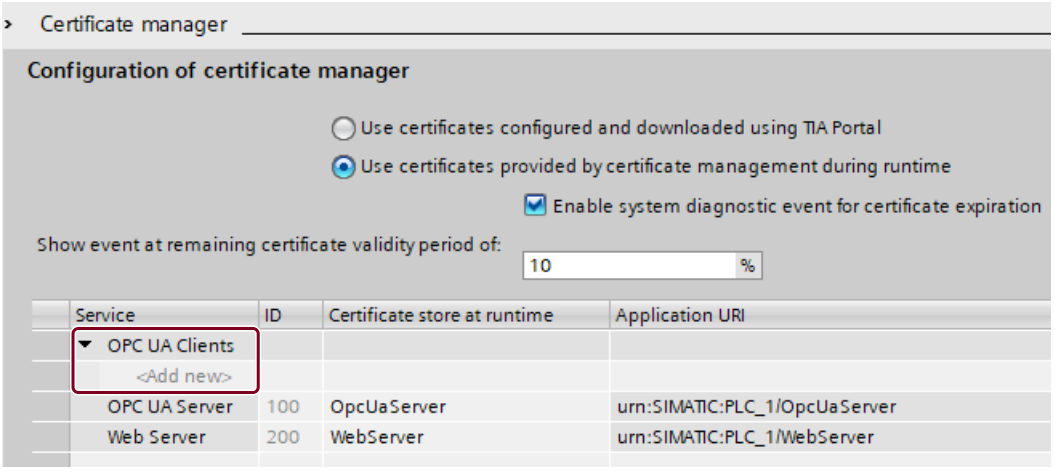


Figure 3-241 Certificate manager after activated certificate management during runtime

Result: You have activated certificate management during runtime. The note and the button for updating the certificate management in runtime are no longer displayed. The table shows the "OPC UA clients" service.

You can find out how to create, edit or delete the certificate stores for the "OPC UA clients" service during runtime in the next sections.

Creating and deleting OPC UA client certificate stores at runtime

For the "OPC UA Clients" service, you can create different certificate stores at runtime and use them for different connections or applications. The generated certificate stores are displayed under the "OPC UA clients" service.

To generate a certificate store for the OPC UA client at runtime, proceed as follows:

1. Under the "OPC UA clients" service, double-click <Add new>.
   STEP 7 creates a new entry, in this case "OPC UA client".
2. Optional: Assign the desired ID for the certificate store in the "ID" column.
   STEP 7 uses consecutive numbering by default. Each ID can only be assigned once in the project. STEP 7 shows duplicate IDs as incorrect.
3. Optional: Change the name of the client certificate folder in runtime.
   By default, STEP 7 generates the name from the service and a consecutive numbering. If you change the name, STEP 7 automatically applies the changes to the associated application URI.

NOTE

Possible consequence of name changes to the client certificate folder

The name of the client certificate store at runtime is also used in the BrowseName and the NodeId for the nodes in the address space of the OPC UA server. If you change the name of the client certificate store, you may need to re-register your applications with your certificate management software.

4. Repeat steps 1 to 3 to generate further certificate stores.
5. Use the IDs from step 2 in the OPC_UA_Connect instructions in the user program to be able to use the certificate from the certificate store to establish the connection.
   If you are already using the OPC UA client with certificates, you can reuse the existing IDs in the certificate store in the "ID" column. In this case, you do not need to change the user program.

Result: You have created and edited various certificate stores for the OPC UA client at runtime. The following figure shows an example of two generated certificate stores for the OPC UA client. The certificate store with ID 1 was generated by STEP 7 by default. The name of the certificate store with ID 2 has been changed.

Service	ID	Certificate store at runtime	Application URI
OPC UA Clients			
OPC UA Client	1	OpcUaClient1	urn:SIMATIC:PLC_1/OpcUaClient1
OPC UA Client	2	MyOpcUaClient	urn:SIMATIC:PLC_1/MyOpcUaClient
<Add new>			
OPC UA Server	100	OpcUaServer	urn:SIMATIC:PLC_1/OpcUaServer
Web Server	200	WebServer	urn:SIMATIC:PLC_1/WebServer

Figure 3-242 Generate client certificate store for certificate management at runtime

To delete a created client certificate store, right-click on the desired certificate store and select "Delete" from the context menu. Deleted certificate stores are no longer available once they have been loaded into the CPU and can no longer be used.

Use the generated certificate stores as already described in the section Creating and configuring connections (Page 365).

Deleting existing certificates on the CPU

When you load your configuration into the CPU, the load preview dialog shows the existing certificate store on the CPU. You can select the certificates you wish to delete. If you select the "OPC UA clients" service, all existing certificates in all OPC UA client certificate stores will be deleted.

11.4.9.4 User authentication

In the OPC UA client interface of the S7-1500, you can set what authentication is required for a user of the OPC UA client wishing to access the server. To do so, you must select the corresponding client interface in the project tree of the requested S7-1500 CPU under "OPC UA communication > Client interfaces" and select the type of user authentication in the Inspector window under "Properties > Configuration > Security".

Types of user authentication

The following options are available for user authentication:

- **Guest**

  The user does not need to verify authorization (anonymous access). The CPU creates an anonymous session for the user, and the OPC UA server does not check the authorization of the client user.
- **User name and password**

  The user must prove authorization (no anonymous access). The OPC UA server checks whether the client user is authorized to access the server. Authorization is given by the user name and the correct password. These inputs cannot be checked by the client interface, which means all values are accepted as being valid.

  NOTE

  STEP 7 stores user name and password unencrypted in the data block/instance data block. Recommendation: Use the user authentication for the "User (TIA Portal - Security Settings)" TIA project.
- **Users (TIA Portal - Security Settings)**

  You can enter a user name from the list of users entered in the project for authentication. The names of the registered users for the current project are available in the user administration in the project tree under "Security Settings > Users and roles". There you can also enter additional users.

  You can also enter a name that is not listed in the user administration of the project or leave the field blank. This is necessary when the corresponding user name is only provided by a different source during runtime, for example, via HMI or from a different OPC UA client.

"No Security" security policy and authentication via user name and password

You can set the following combination:

Security policy = "No Security" and authentication via user name and password.

- The OPC UA server of the S7-1500 supports this combination. OPC UA clients can connect and encrypt the authentication data or not.
- OPC UA client of the S7-1500 CPU also supports this combination: However, in runtime it only connects if it can send the authentication data encrypted via cable!

Result: With the following configuration, no connection can be established at runtime:

- S7-1500 as OPC UA client
- OPC UA server which supports no encryption of authentication data when "No Security" (="none") is set as security policy.

More information

You can find information about the users and roles with OPC UA function rights in the section Users and roles with OPC UA function rights (Page 266).

11.4.9.5 Using a configured connection

Introduction

This section shows you how to use a configured connection for OPC UA instructions (third step).

Requirements

- You have created a client interface and added PLC tags and PLC methods to this interface, see ("First step (Page 351)").
- You have configured a connection to an OPC UA server (Second step (Page 365)).

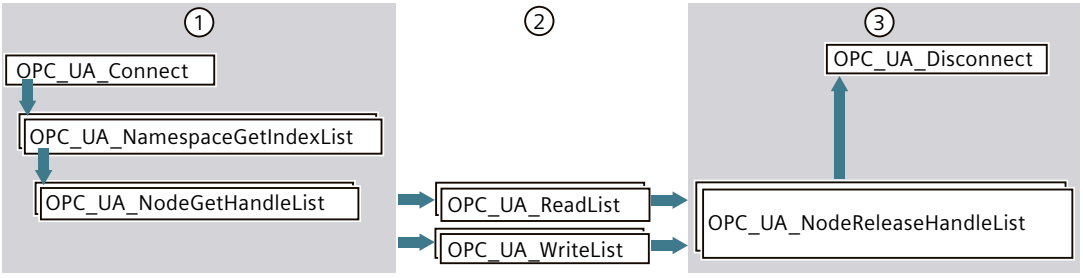
Overview

To read data from an OPC UA server or write data to an OPC UA server, use the following instructions:

- OPC_UA_Connect
- OPC_UA_NamespaceGetIndexList
- OPC_UA_NodeGetHandleList
- OPC_UA_ReadList or OPC_UA_WriteList
- OPC_UA_NodeReleaseHandleList
- OPC_UA_Disconnect

Order of the OPC UA instructions

The following figure shows the order in which the OPC UA instructions are called in a user program in order to use these instructions to read or write PLC tags:



① Instructions for preparation of read and write operations

② Read and write instructions

③ Instructions for "clean-up" after a completed read or write operation
The "OPC_UA_NodeReleaseHandleList" instruction can be omitted if "OPC_UA_Disconnect" is called immediately afterwards.

Figure 3-243 Call sequence for write and read operations

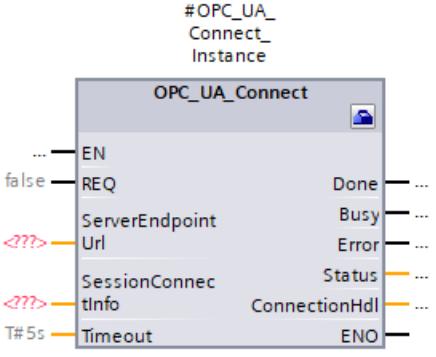
STEP 7 (TIA Portal) automatically supplies the parameters of these instructions if you are using a client interface and a configured connection to an OPC UA server.

The procedure is shown in the following section.

Using a client interface and configured connection

To use a configured OPC UA connection, follow these steps:

1. Open your user program in the TIA Portal.
2. Using drag-and-drop, move the "**OPC_UA_Connect**" instruction into the program editor.
   You will find the instruction under "Instructions > Communication > OPC UA" in the TIA Portal.
3. Select a call option for the instruction
   The example uses a multi-instance.
   STEP 7 displays the instruction in the program editor.
   The editor for the Function Block Diagram (FBD) programming language uses the following display:

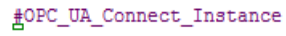


The editor for the Ladder Logic (LAD) programming language displays the instruction similarly.

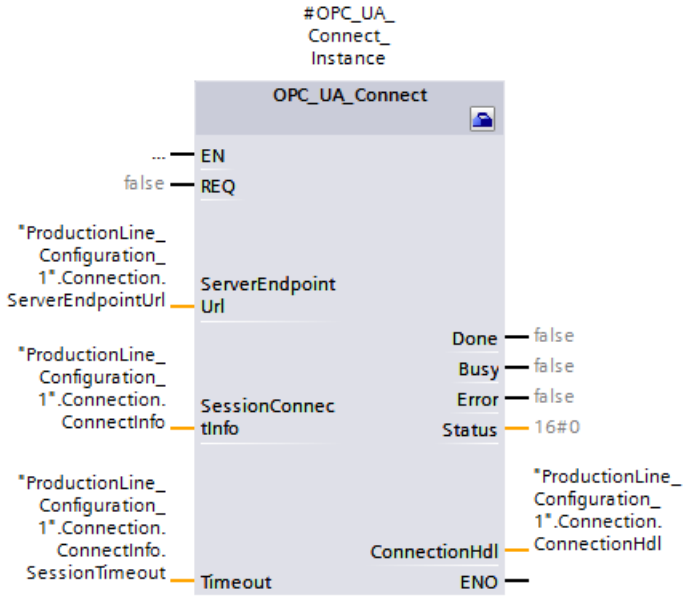
4. Click the toolbox symbol in the editor for FBD or LAD.
   The symbol is located in the heading of the instruction:

   If you are using the editor for STL or SCL: Click the small green rectangle below the first character of the instance name:

   The example (Page 350) uses "#OPC_UA_Connect_Instance" as the instance name.
   STEP 7 displays the properties of the instruction in a separate dialog.
5. For "Client interface" select the client interface that you want to use for the instruction.
   In the example, we select the "ProductionLine" client interface.
   STEP 7 now interconnects the "ProductionLine" client interface with the parameters of the OPC_UA_Connect instruction:

   "ProductionLine" is the interface that the OPC UA client of the example (Page 350) uses for data exchange with the OPC UA server "ProductionLine".
6. Using drag-and-drop, move the "**OPC_UA_NamespaceGetIndexList**" instruction into the program editor.
   You will find the instruction under "Instructions > Communication > OPC UA" in the TIA Portal.
   Select the "Multi-instance" call option.
   Click the toolbox symbol (LAD and FBD) or the small green box below the instance name (STL and SCL) if the editor is not already open.
   Select the client interface that you want to use (in the example "ProductionLine").
   STEP 7 now automatically interconnects all parameters of the "OPC_UA_NamespaceGetIndexList" instruction:

7. Using drag-and-drop, move the "**OPC_UA_NodeGetHandleList**" instruction into the program editor.

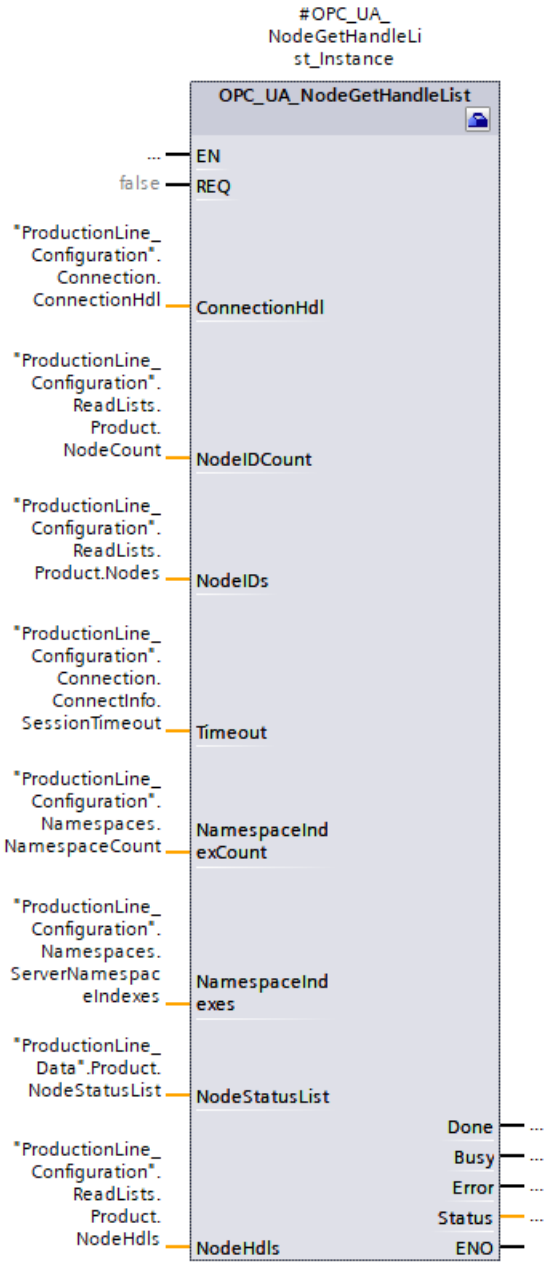
   Select the "Multi-instance" call option.

   Click the toolbox symbol (LAD and FBD) or the small green box below the instance name (STL and SCL) if the editor is not already open.

   Select the client interface that you want to use. The example uses the "ProductionLine" client interface.

   Under "Data access > Read/Write list" select the read or write list that you want to use (in the example the read list "Product").

   STEP 7 now automatically interconnects all parameters of the "OPC_UA_NodeGetHandleList" instruction:



If you want to write data to an OPC UA server, select the write list you want to use under "Data access > Write list" (the "ProductionStatus" write list in the example).

8. Using drag-and-drop, move the "**OPC_UA_ReadList**" instruction into the program editor.

   Select the "Multi-instance" call option.

   Click the toolbox symbol (LAD and FBD) or the small green box below the instance name (STL and SCL) if the editor is not already open.

   Select the client interface that you want to use. The example uses the "ProductionLine" client interface.

   Under "Data access > Read list" select the read list that you want to use (in the example the "Product" read list).

   STEP 7 now automatically interconnects all parameters of the "OPC_UA_ReadList" instruction.

   If you want to write data to an OPC UA server, use the "**OPC_UA_WriteList**" instruction and select the list of tags you want to send to the server under "Data access > Write list" ("ProductionStatus" write list in the example).

9. If you use different read lists or write lists as program-controlled lists in your user program, move the "**OPC_UA_NodeReleaseHandleList**" instruction to the program editor using drag-and-drop operation.

   Select the client interface that you want to use.

   Now select a read list or write list that you want to release: Only release read or write lists that you rarely use, since re-registering is time-consuming.

   Then, repeat the steps starting with step 7 with the "OPC_UA_NodeGetHandleList" instruction.

10. Using drag-and-drop, move the "**OPC_UA_Disconnect**" instruction into the program editor.

    Select the "Multi-instance" call option.

    Click the toolbox symbol (LAD and FBD) or the small green box below the instance name (STL and SCL) if the editor is not already open.

    Select the client interface that you want to use. The example uses the "ProductionLine" client interface.

    STEP 7 now automatically interconnects all parameters of the "OPC_UA_Disconnect" instruction.

Supported instructions

For the following instructions, STEP 7 automatically supplies the parameters if you are using a client interface and a configured connection to an OPC UA server:

- OPC_UA_Connect
- OPC_UA_NamespaceGetIndexList
- OPC_UA_NodeGetHandleList
- OPC_UA_MethodGetHandleList
- OPC_UA_MethodReleaseHandleList
- OPC_UA_ReadList
- OPC_UA_WriteList
- OPC_UA_MethodCall

- OPC_UA_NodeReleaseHandleList
- OPC_UA_Disconnect

Compact instructions

As of TIA Portal V17, compact instructions are available for OPC UA which summarize the write job/read job/method call and the connection establishment:

- OPC_UA_ReadList_C for generating a connection and reading tags
- OPC_UA_WriteList_C for generating a connection and writing tags
- OPC_UA_MethodCall_C for generating a connection and calling methods

You will find information about the compact instructions services in the TIA Portal Help.

11.5 Tips and recommendations

11.5.1 Rules for subscriptions

The following rules apply to subscriptions:

- Group subscriptions in the client according to different sampling and publishing intervals and distribute the monitored elements (variables) to these groups.

  Example: Create a subscription for longer publishing intervals (e.g. 5 seconds) and a subscription for shorter publishing intervals (e.g. 0.1 second).
- Disable unneeded subscriptions.

  Reason: The "Deactivated" subscription mode reduces resource consumption.
- To further optimize resource consumption, reduce the subscription timeout for the client. The subscription timeout cannot be specified directly, this time results from the subscription settings "PublishingInterval" and "LifetimeCount" confirmed by the server. Background: When a client has created subscriptions and the session is terminated, the subscriptions initially remain in the server and occupy memory resources. The OPC UA server only releases the resources needed for this when the subscription timeout ends the lifetime of the subscriptions.
- Consider the maximum number of monitored items of subscriptions for the corresponding S7-1500 CPU.

  The information can be found in the technical specification of the respective CPU. The information is based on a sampling / publishing interval of 1 second.

  You can find more information in the FAQ 109755846 (https://support.industry.siemens.com/cs/us/en/view/109755846).
- Select the same sampling and publishing intervals for the OPC UA client and for the OPC UA server.

- Avoid arrays and structures as elements of subscriptions – if the process allows.
  Reason: If even one value of an array/structure changes, the entire structure is transferred, creating an unnecessary communication load.
- Occasional non-compliance with the required sampling rate is acknowledged by the OPC UA server of the S7-1500 CPU according to OPC UA specification with a "GoodOverload" error code, see also TIA Portal Help. Different OPC UA clients handle "Good" error codes unequal to "0" differently. Consider this behavior and, if needed, reduce the communication load according to the measures described above.

More information

For information on how to set the server for subscriptions, refer to the section Settings of the server for subscriptions (Page 252).

11.5.2 Rules for the user program

User programs for OPC UA

The following rules apply to user programs:

- If your application allows it and the communication load is high, you should set a minimum time for cycle OBs.
  Advantages:
  - The cycle time remains constant for the most part
  - The CPU has more time for communication tasks throughout

  Tip: Use the instruction "Runtime_Info"; mode 21 or mode 25 (see TIA Portal Help) to analyze the CPU utilization (e.g. communication).
- Reduce the number of variables or data blocks that can be reached from OPC UA/HMI. By default, all variables from OPC UA/HMI are accessible when creating variables/DBs/IDBs. This measure leads to improved performance when loading in RUN.
  Tip: Using the detailed object display in the TIA Portal, you can easily mark the non-OPC-UA-relevant data blocks as "not accessible from OPC UA".
- Consistent transfer of data beyond the limits of simple data types is only possible with OPC UA methods. If you use other OPC UA functions (Subscriptions, Read/Write), you must ensure data consistency in the application.
- OPC UA offers the "RegisterNodes" service for repeated read and write accesses to the same variables. Servers can use this service to prepare for optimized access to variables. The instruction "OPC_UA_NodeGetHandleList" of the S7-1500 as OPC UA client implicitly calls this service to prepare the server for optimized accesses (in OPC UA usage "Registered Read/Write").

Calling detailed object display in the TIA Portal

To call up the detailed object display, proceed as follows:

1. Switch to the "PLC Programming" portal in the portal view.
2. Select "Show all objects".
3. Switch to the "Details" tab in the selection window.

4. In the "DB accessible from OPC UA" column, disable the accessibility from OPC UA for individual objects.

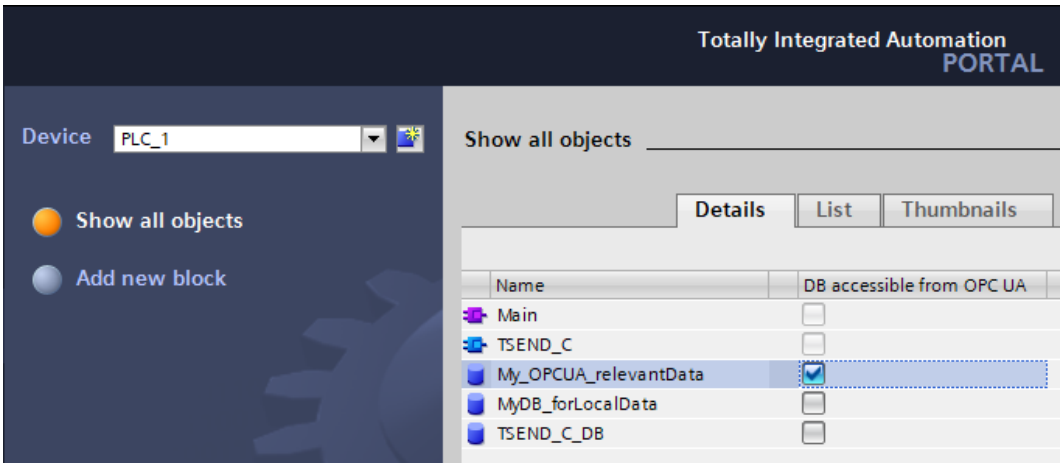


Figure 3-244 Calling detailed object display in the TIA Portal

11.5.3 Master copies for OPC UA communication

Master copies for the OPC UA interfaces

Interfaces of OPC UA servers and OPC UA clients that you want to use multiple times can be stored either in the project library or in a global library. Master copies in the project library can only be used within the project. When you create the master copy in a global library, it can be used in different projects.

The OPC UA capable CPUs differentiate between 3 interface types of the OPC UA server:

- Standard OPC UA server interface
- Companion specification interface
- Namespace reference

When adding the OPC UA interface in the project tree under "OPC UA Communication" each interface type gets its own symbol. The same symbol is used by the master copy.

Create either single master copies or a master copy with multiple interfaces.

Creating multiple master copies from selection

You select one or more elements and create individual master copies from them

1. Open the library in the "Libraries" task card.
2. Select the desired elements.
3. Using a drag-and-drop operation, move the elements to the "Master copies" folder or any subfolder of "Master copies".

Creating a master copy from selection

You select multiple elements and create a single master copy from them that contains all selected elements.

1. Copy to the clipboard the elements that you want to create as master copies.
2. Right-click on the "Master copies" folder or any of its subfolders in the library.
3. In the shortcut menu, select "Paste as a single master copy" command.

If multiple interfaces are added to a master copy from the OPC UA server or OPC UA client, the label and the symbol in the library are changed accordingly.

A symbol with "+" is displayed instead of the simple symbol.

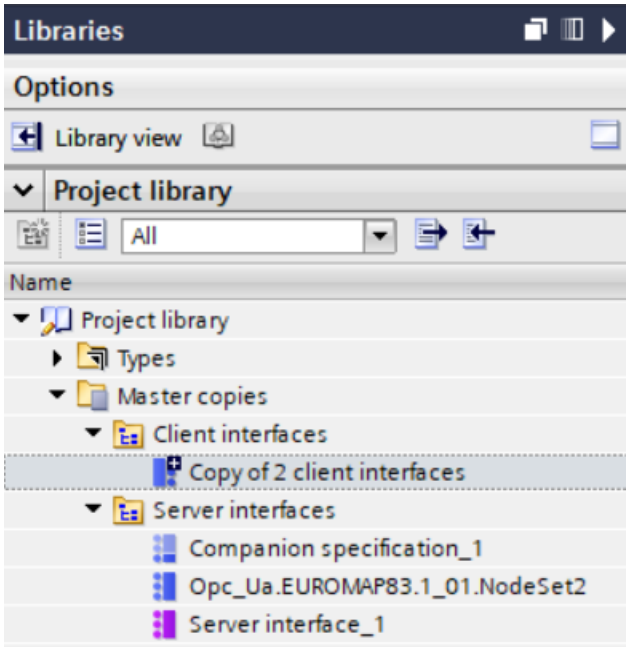


Figure 3-245 Create copy template in STEP 7

More information

For information on how to create a user-defined server interface, refer to the section Creating a user-defined server interface (Page 283).

Addressing via DHCP

12

In order to provide future-proof, efficient and flexible automation, more and more components from the production area support IT standards. Worldwide Ethernet standards, integrated communication and versatility make IT-supported automation an economical solution for your requirements. Functional expansions of the communication options of the S7-1500 CPUs in this direction give you more freedom for the possible uses of your system or machine. You use IT technology to automate efficiently. With the introduction of DHCP and the expansions of DNS for S7-1500 CPU as of firmware version V2.9, you gain more flexibility for the design of your automation solution.

For the interfaces of an S7-1500 CPU you can set that address parameters such as the IP address with subnet mask, can be got from a DHCPv4 server (hereinafter DHCP server).

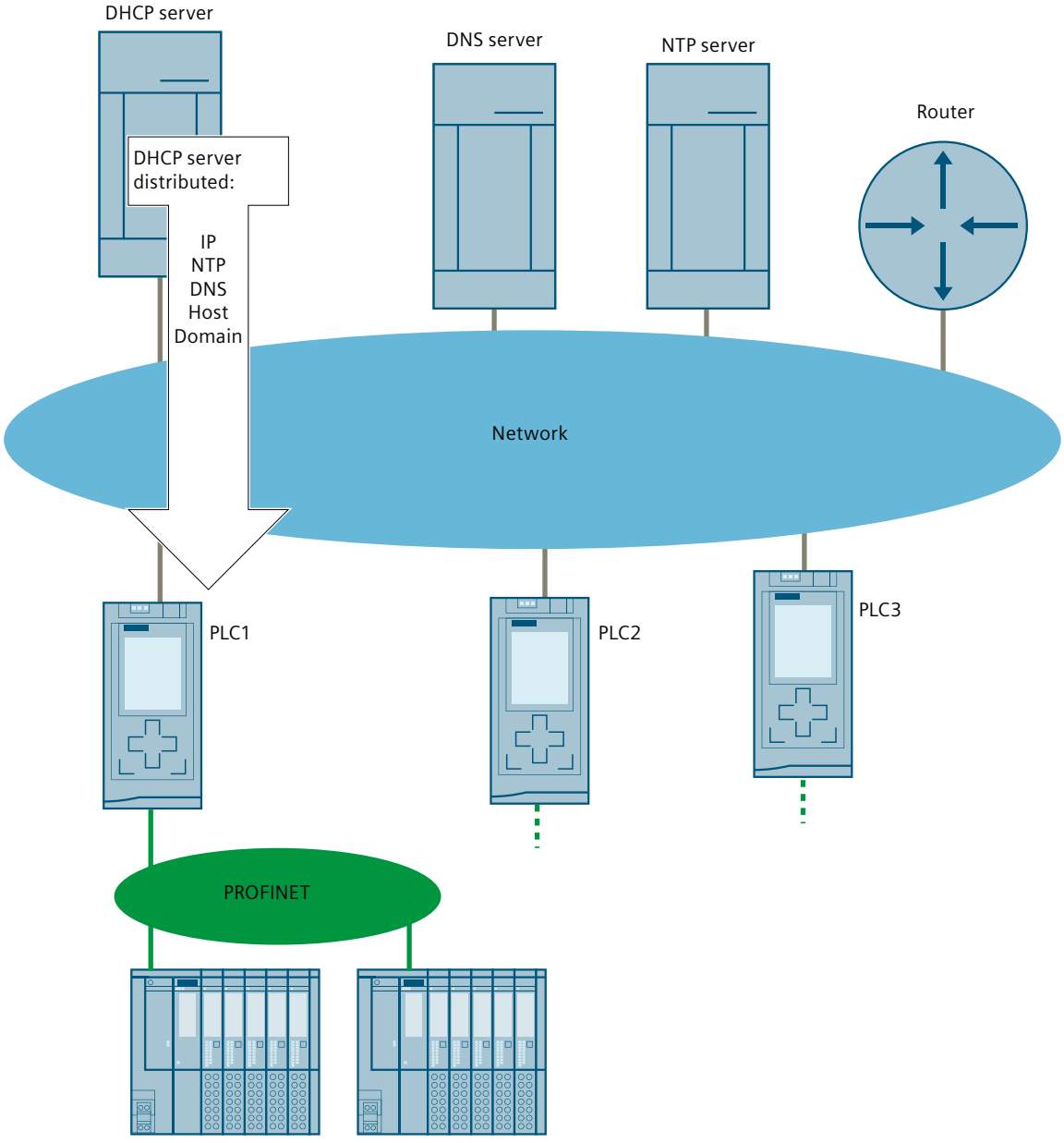


Figure 3-246 Overview of DHCP

Areas of application

- Use of the S7-1500 CPU in a managed IT environment
- Adding new devices in a modular manufacturing structure

12.1 Principle of address assignment via DHCP

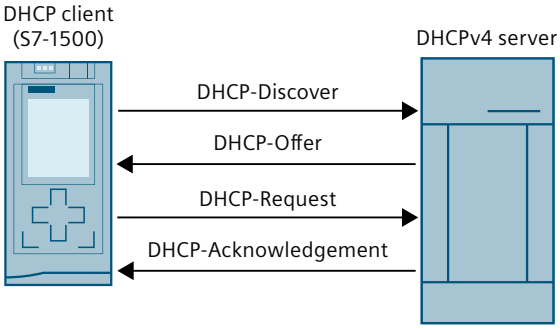
Requirement configuration

The following requirements must be met so that a PROFINET interface of the S7-1500 CPU can obtain IP address parameters via a DHCP server:

- The address assignment via a DHCP server is configured.
  Activate DHCP (Page 392)
- No PROFINET IO communication may be configured for the interface.

Principle of DHCP address assignment

The process begins as soon as the project is loaded into the CPU or the CPU is switched on with configured DHCP address assignment and started up, the process of DHCP assignment begins:



DHCP Discover	The DHCP client searches for a suitable DHCP server via broadcast. The DHCP client identifies itself to the DHCP server with the configured client ID or with its MAC address.
DHCP Offer	The DHCP server offers the DHCP-client IP address parameters (IPv4 address, subnet mask, optional default router) and if necessary further data (options).
DHCP Request	The DHCPclient requests the IP address parameters and options offered in the DHCP offer. The DHCP client of the S7-1500 CPU always accepts the first DHCP offer of a DHCP server that meets the requirements (IP address with subnet mask).
DHCP Acknowledgment	The DHCP server confirms and transmits the IP address parameters and options offered in the DHCP offer. The DHCP server also notifies the DHCP client how long the DHCP client can use the address parameters (lease time).

Figure 3-247 Principle of address assignment with DHCP

The IP address parameters and options are stored in the load memory of the CPU. After a general reset or restart of the CPU, the IP address parameters and options are obtained again via DHCP.

DHCP address assignment options

For the S7-1500 CPU you can configure that the following options are obtained via a DHCP server:

- Addresses of up to four DNS servers
  Get addresses of the DNS servers via DHCP (Page 394)
- Address of up to four NTP servers
  Get addresses of the NTP servers via DHCP (Page 395)
- Host and domain name
  Obtain host and domain name via DHCP (Page 395)

If necessary, the DHCP server also supplies the address of a router (default gateway) as option.

How long can the S7-1500 CPU use the DHCP address parameters?

In addition to the address parameters, the DHCP server also notifies the S7-1500 CPU (DHCP client)of the lease time. The lease time defines how long the CPU can use the address parameters.

When the lease time has fully expired, the CPU returns the assigned address parameters. The CPU has an internal time monitoring for the lease time.

At certain times when the lease time expires, the CPU has the option of extending the lease time:

- Renewal: Half of the lease time has expired: The CPU contacts the original DHCP server and asks for an extension of the lease time. The original DHCP server can either confirm the existing lease time or assign a new lease time. With a new lease time, the time monitoring in the CPU is reset.
- Rebinding: 7/8 of the lease term has expired: The CPU contacts all available DHCP servers via broadcast and asks for an extension of the lease time. A DHCP server can either confirm the existing lease time or assign a new lease time. With a new lease time, the time monitoring in the CPU is reset.

  In the event of a negative response from DHCP server during rebinding or if no DHCP server replies, the CPU returns the address parameters after 8/8 of the lease time.

If the CPU has returned the address parameters after the lease time has expired, the CPU starts a new cycle for DHCP addressing with a new DHCP discover.

More information

For information on how to configure client ID, refer to the section Configuring the client ID (Page 393).

12.2 DHCP with DNS

As of STEP 7 V17, the S7-1500 CPU supports the host name and domain address parameters used in name-based communication (DNS).

For specific communication services, name-based addressing via the complete name consisting of host name and domain, is useful:

- The CPU is addressable under the complete name, for example at OPC UA, Open User Communication. In the case of dynamic IP address assignment by the DHCP server, unique addressing is always possible through the DNS name.
- Certificates of the S7-1500 CPU may contain the complete name, for example, for OPC UA communication, web server, secure communication.
  - Only if you configure host name and domain for the S7-1500 CPU in STEP 7, then the complete name is entered in the device certificates in the project as subject alternate name (SAN).
  - As soon as you obtain the host name and/or domain via DHCP or assign it via the user program, the complete name is not stored in the device certificates in the project.

How you set the DNS configuration for your CPU depends on how you assign the host name and domain in your network .

- Central assignment of host name and domain

  You assign the host name and domain centrally in your network, for example via a configured DNS server. In STEP 7 you configure that the CPU obtains the host name and domain via DHCP.

  In the following configuration, only the client ID is configured in the S7-1500 CPU. At the DHCP address assignment the DHCP-server returns the host name and domain options to the CPU.

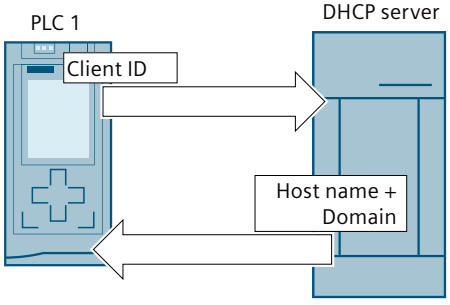


Figure 3-248 Obtain host and domain name via DHCP

For this configuration, you must first activate the host name and domain configuration in STEP 7. You then configure that the host and domain name are obtained via DHCP.

Obtain host and domain name via DHCP (Page 395)

- Local assignment of host name and domain
  You can configure the host name and domain in STEP 7 or assign them in the user program.

NOTE

Validity of the data obtained from DHCP
If you change the host name and/or domain in the user program, then all data obtained via DHCP (IP suite, host name, domain, NTP server, DNS server) becomes invalid and is retrieved again from DHCP server. Therefore, you should only change the Hostname and/or Domain in urgent cases and not during operation.
All connections can be dropped if the IP address of the interface changes.

In the following configuration, the host name and its domain are configured in the S7-1500 CPU in addition to its client ID. During DHCP address assignment, the CPU supplies the host name and the domain to the DHCP server in addition to the client ID. The DHCP server receives the information to update, for example a DNS server with the address data of the CPU.

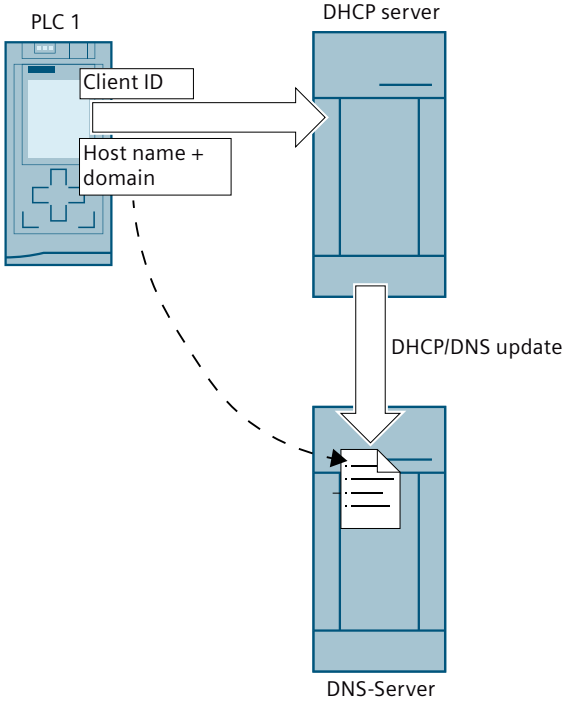


Figure 3-249 Configure host and domain name

For this configuration, you must first activate the host name and domain configuration in STEP 7. You then configure the host name and domain in STEP 7.

- Central assignment of the domain and local assignment of host name.
  - You configure in STEP 7 that the CPU gets the domain via DHCP.
  - You can configure the host name in STEP 7 or assign it via the user program.

  In the following configuration, the host name is also configured in the S7-1500 CPU in addition to its client ID. When assigning DHCP addresses, the CPU supplies the client ID as well as the host name to the DHCPv4 server. The DHCP server supplies the domain option to the CPU.

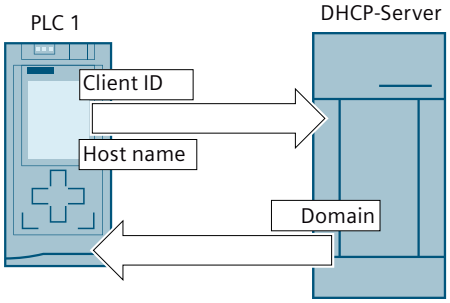


Figure 3-250 Configure host name, obtain domain name via DHCP

For this configuration, you must first activate the host name and domain configuration in STEP 7. Then configure the host name in STEP 7 and configure that the domain is obtained via DHCP.

Requirements

- You have activated the address assignment via DHCP for at least one interface of the S7-1500 CPU.

Configuration of host and domain name

To activate the host name and domain configuration in STEP 7, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name" > "Host and domain name configuration".
3. Select the "Enable host name and domain" check box.

Configuring the host name in STEP 7

To configure the host name in STEP 7, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name" > "Host and domain name configuration"> "Host name".

3. For "Host name configuration:" select "Set host name in the project" from the drop-down list.
4. Enter the host name for "Host name:".
   – Enter your desired host name.
   – If you select the "Host name identical to device name" check box, STEP 7 automatically assigns the device name as the host name.

Only if you have configured the host and domain name in STEP 7, the full name is displayed for "Full name:".

Assign host name in the user program

To assign the host name in the user program, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name" > "Host and domain name configuration" > "Host name".
3. Under "Host name configuration:" select "Set hostname directly on the device (e.g. PLC program, display)" in the drop-down list.
4. Call the instruction "CommConfig" in the user program. The DATA parameter must point to a UDT "Conf_Hostname" where the host name is defined.

You can find more information on the "CommConfig" instruction and on the UDT "Conf-Hostname" in the STEP 7 online help.

Configuring a domain in STEP 7

To configure the domain in STEP 7, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name" > "Host and domain name configuration" > "Domain".
3. For "Domain configuration:" select "Set domain in the project" from the drop-down list.
4. Enter your desired domain under "Domain:".

Only if you have configured the host and domain name in STEP 7, the full name is displayed for "Full name:".

Assigning a domain in the user program

To assign the domain in the user program, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name" > "Host and domain name configuration" > "Domain".
3. Under "Hostname configuration:" select "Set domain directly on the device (for example PLC program, display)" in the drop-down list.
4. Call the instruction "CommConfig" in the user program. The DATA parameter must point to a UDT "Conf_Domainname" where the domain name is specified.

You can find more information on the "CommConfig" instruction and on the UDT "Conf-Domainname" in the STEP 7 online help.

Rules for maximum lengths of host name, domain and client ID

Note the following maximum lengths in bytes. One byte corresponds to one character:

- Host name: Maximum 63 bytes
- Domain: Maximum 252 bytes
- Client ID: Maximum 254 bytes
- Host + Domain name: Maximum 254 bytes
- Host + Domain name + Client ID: Maximum 260 bytes
  Applies only when host and domain name must be sent to the DHCP server.

12.3 Activate DHCP

Requirements

- S7-1500 CPU firmware V2.9 or higher

Procedure

To activate DHCP for the PROFINET interface of an S7-1500 CPU, follow these steps:

1. Select the PROFINET interface of the S7-1500 CPU in STEP 7.
2. In the properties of the interface, navigate to "Ethernet addresses" > "Internet Protocol Version 4 (IPv4)".
3. Select the option "IP address of DHCP server".

Result

You have set the interface so that it obtains your IP address via a DHCP server.

"Use MAC address as client ID" is set as the operating mode for DHCP on the S7-1500 CPU. How to adjust the client ID is described under Configuring the client ID (Page 393).

12.4 Configuring the client ID

The client ID

The S7-1500 CPU always identifies itself to a DHCP server with the client ID (DHCP option 61). The client ID is interface specific.

The S7-1500 CPU supports the following two operating modes with regard to the client ID:

- Use the MAC address as the client ID: The MAC address of the CPU is used as the client ID for the DHCP client. Note, if you execute a device exchange of the CPU in this operating mode, the MAC address and therefore also the client ID changes.
- User-defined client ID: With this option you specify the client ID in the configuration in STEP 7. You also have the option of adapting the client ID during runtime, for example, in the user program using the "CommConfig" instruction.
  If you perform a device exchange of the CPU in this operating mode, the new CPU is assigned the configured client ID.

Requirement

- You have activated address assignment via DHCP for the interface.

Configuring the client ID

To configure the client ID in STEP 7, follow these steps:

1. Select the PROFINET interface of the S7-1500 CPU in STEP 7.
2. In the properties of the interface, navigate to "Ethernet addresses" > "Internet Protocol Version 4 (IPv4)"> "IP address of DHCP server".
3. For "Operating mode:" select the required operating mode from the drop-down list:
   – Use MAC address as client ID (default setting)
   – User-defined client ID

   If you have selected the option "Use MAC address as client ID", then you are already finished here. For "User-defined client ID", continue with step 4.
4. Enter a valid client ID for "Client ID".
   – A character string with 7-bit ASCII characters is allowed in the area from 0x21 to 0x7e.
   – Some DHCP servers expect a leading "0" (e.g. some SCALANCE devices). In this case, enter "\ 0" followed by your client ID.
   – You can also leave the field blank. In this case, you must select the "Client ID can be changed at runtime" check box.
5. In order to make the user-defined client ID adaptable during runtime, select the "Client ID can be changed during runtime" check box.

Adapting the client ID during runtime

You can use the "CommConfig" instruction to adapt the client ID via the user program. Call the instruction. The DATA parameter must point to a UDT "Conf_ClientId" or a UDT "Conf_ClientId_Opaque". The client ID must be specified in the UDT.

If you have left the user-defined client ID free in the configuration in STEP 7, then the CPU uses the MAC address as the client ID until the client ID is adapted for the first time.

NOTE

Validity of data obtained via DHCP

If you change ClientId with "CommConfig", all data obtained via DHCP will be invalid: IP Suite, domain name, NTP server, DNS server. Therefore, you should only change ClientId in urgent cases and not during operation.

You can find more information on the instruction "CommConfig" and the UDTs "Conf_ClientId" and "Conf_ClientId_Opaque" in the STEP 7 online help.

12.5 Get addresses of the DNS servers via DHCP

Requirements

- You have activated the address assignment via DHCP for at least one interface of the S7-1500 CPU.

Get addresses from DNS servers via DHCP

To obtain the addresses of up to 4 DNS servers via DHCP, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "DNS configuration" > "Server list".
3. For "Name resolution via DNS:" select "Set DNS server remotely (e.g. DHCP)" in the drop-down list.

Result: If the DHCP server supplies addresses from DNS servers as option, the CPU uses up to 4 addresses.

12.6 Get addresses of the NTP servers via DHCP

Requirements

- You have activated the address assignment via DHCP for at least one interface of the S7-1500 CPU.

Obtaining addresses from NTP servers via DHCP

To obtain the addresses of up to four NTP servers via DHCP, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Time of day" > "Time synchronization"> "NTP mode".
3. For "Time synchronization:" select "Set NTP server remotely (e.g. DHCP)" in the drop-down list.

Result: If the DHCP server supplies addresses from NTP servers as option , the CPU uses up to 4 addresses.

12.7 Obtain host and domain name via DHCP

Requirement

- You have activated the address assignment via DHCP for at least one interface of the S7-1500 CPU.
- You have activated the host name and domain configuration in STEP 7.

Obtain host name via DHCP

To obtain the host name via DHCP, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name"> "Host and domain name configuration"> "Host name".
3. For "Host name configuration:" select "Set host name remotely (e.g. DHCP)" in the drop-down list.

Result: If the DHCP server supplies a host name as option, the CPU uses this host name.

Obtaining a domain via DHCP

To obtain the domain via DHCP, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. In the properties of the CPU, navigate to "Advanced configuration" > "Host and domain name" > "Host and domain name configuration" > "Domain".
3. For "Domain configuration:" select "Set domain remotely (e.g. DHCP)" in the drop-down list.

Result: If the DHCP server delivers a domain as option, the CPU uses this domain.

Routing

13

13.1 Overview of the routing mechanisms of S7-1500 CPUs

The following table gives an overview of the routing mechanisms of the S7-1500 CPU.

Routing mechanism	Description	Applications	Section
S7 routing	S7 routing is the transfer of data beyond S7 subnet boundaries. You can send information from a transmitter to a receiver across several s7 subnets.	Download user programs Load hardware configuration Execute testing and diagnostics functions	S7 routing (Page 397)
IP forwarding	IP forwarding is a function of devices to forward IP packets between two connected IP subnets.	Simple access from the control level to the field level for configuration and parameter assignment of devices, e.g. via PDM or Web browser. Simplified integration of devices for remote access, e.g. for diagnostics during remote maintenance or firmware update.	IP forwarding (Page 402)
Data record routing	Data can be sent over PROFINET from an engineering station to field devices via multiple networks. Since the engineering station addresses the field devices using standardized records and these records are routed via S7 devices, the term "data record routing" is used to refer to this type of routing.	Data record routing is used, for example, when field devices of different manufacturers are used. The field devices are addressed using standardized data records (PROFINET) for configuration and diagnostics.	Data record routing (Page 415)

13.2 S7 routing

Definition of S7 routing

S7 routing is the transfer of data beyond S7 subnet boundaries. You can send information from a transmitter to a receiver across several s7 subnets. The gateway from one S7 subnet to one or more other subnets is provided by the S7 router The S7 router is a device which has interfaces to the respective S7 subnets. S7 routing is possible via various S7 subnets (PROFINET/Industrial Ethernet and/or PROFIBUS).

Requirements for S7 routing

- All devices that can be reached in a network have been configured in a project in STEP 7 and downloaded.
- All devices involved in the S7 routing must receive routing information about the S7 subnets that can be reached through specific S7 routers. The devices obtain the routing information by downloading the hardware configuration to the CPUs, since the CPUs play the role of an S7 router.

  In a topology with several consecutive S7 subnets, the following order must be kept to when downloading: First download the hardware configuration to the CPU(s) directly connected to the same S7 subnet as the PG/PC, then download one by one the CPUs of the S7 subnets beyond this starting with the nearest S7 subnet through to the S7 subnet furthest away.
- The PG/PC you want to use to establish a connection via a S7 router must be assigned to the S7 subnet it is physically connected to. You can assign the PG/PC to a PG/PC in STEP 7 under Online & Diagnostics > Online accesses > Connection to interface/subnet.
- For S7 subnets of the type PROFIBUS: Either the CPU must be configured as DP master or, if it is configured as a DP slave, the "Test, commissioning, routing" check box must be selected in the properties of the DP interface of the DP slave.
- S7 routing for HMI connections is possible as of STEP 7 V13 SP1.

NOTE

Firewall and S7 routing

A firewall does not recognize the IP address of the sender during S7 routing when the sender is located outside the S7 subnet adjacent to the firewall.

An overview of the devices that support the "S7 routing" function is provided in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/584459).

S7 routing for online connections

With the PG/PC, you can reach devices beyond S7 subnets, for example to do the following:

- Download user programs
- Download a hardware configuration
- Execute test and diagnostics functions

In the following figure, CPU 1 is the S7 router between S7 subnet 1 and S7 subnet 2.

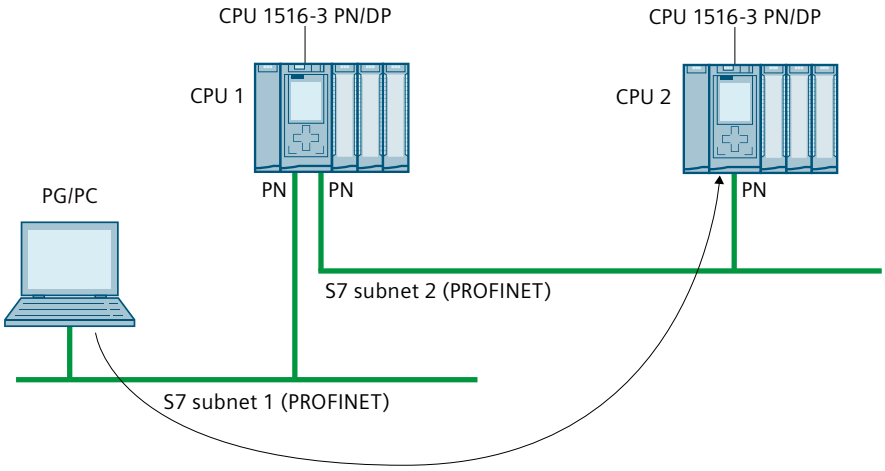


Figure 3-251 S7 routing: PROFINET - PROFINET

The following figure shows the access from a PG via PROFINET to PROFIBUS. CPU 1 is the S7 router between S7 subnet 1 and S7 subnet 2; CPU 2 is the S7 router between S7 subnet 2 and S7 subnet 3.

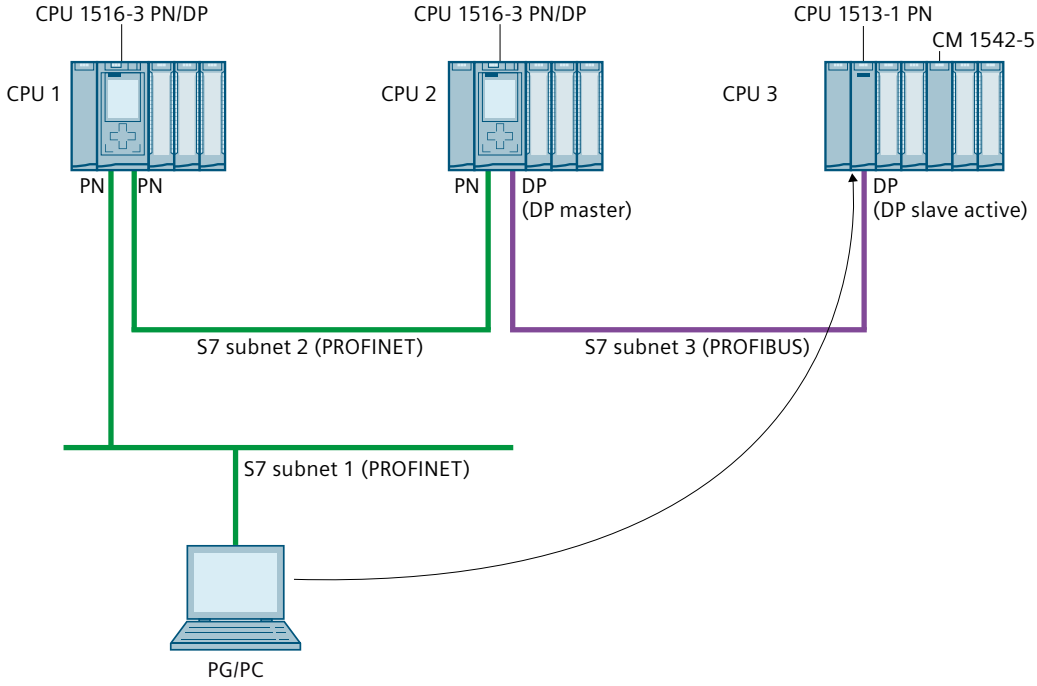


Figure 3-252 S7 routing: PROFINET - PROFIBUS

S7 routing for HMI connections

You have the option of setting up an S7 connection from an HMI to a CPU via different subnets (PROFIBUS and PROFINET or Industrial Ethernet). In the following figure, CPU 1 is the S7 router between S7 subnet 1 and S7 subnet 2.

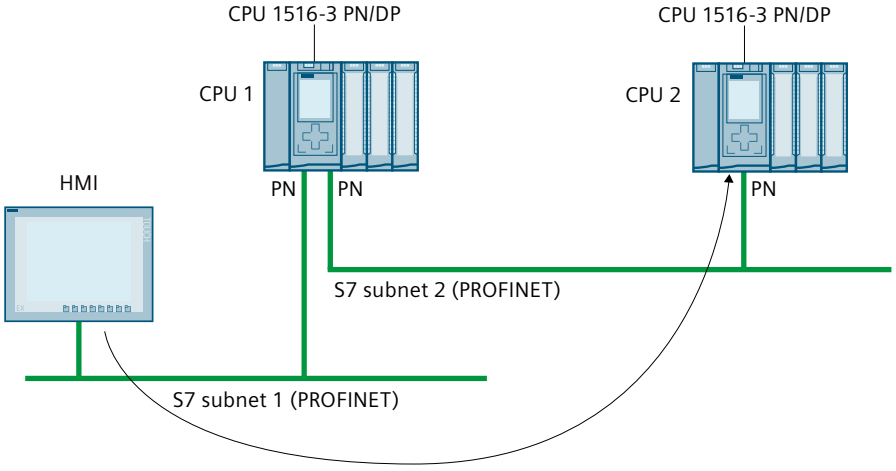


Figure 3-253 S7 routing via HMI connections

S7 routing for CPU-CPU communication

You have the option of setting up an S7 connection from a CPU to another CPU via different subnets (PROFIBUS and PROFINET or Industrial Ethernet). The procedure is described based on examples in the section S7 communication (Page 152).

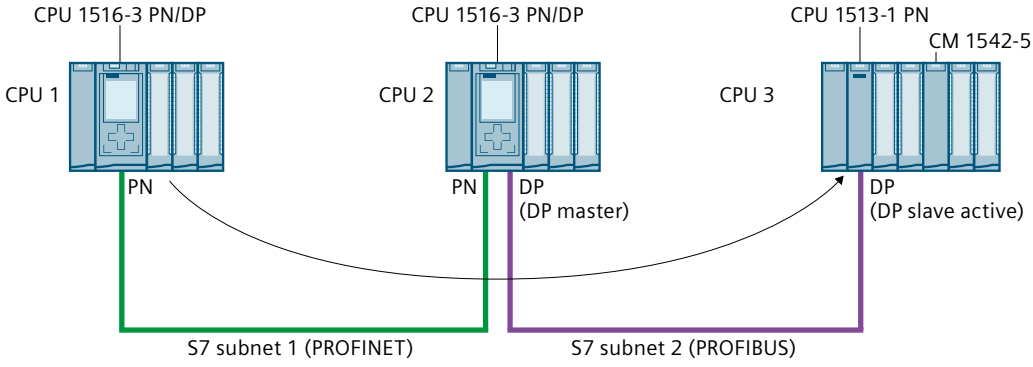


Figure 3-254 S7 routing via CPU-CPU communication

Using S7 routing

For the CPU, select the PG/PC interface and the S7 subnet in the "Go online" dialog of STEP 7. S7 routing is performed automatically.

Number of connections for S7 routing

The number of connections available for S7 routing in the S7 routers (CPUs, CMs or CPs) can be found in the technical specifications in the manuals of the relevant CPU/CM/CP.

S7 routing: Example of an application

The figure below shows the example of an application for remote maintenance of a system using a PG. The connection is made here beyond two S7 subnets via a modem connection.

You configure a remote connection via TeleService in STEP 7 using "Online access" or "Go online".

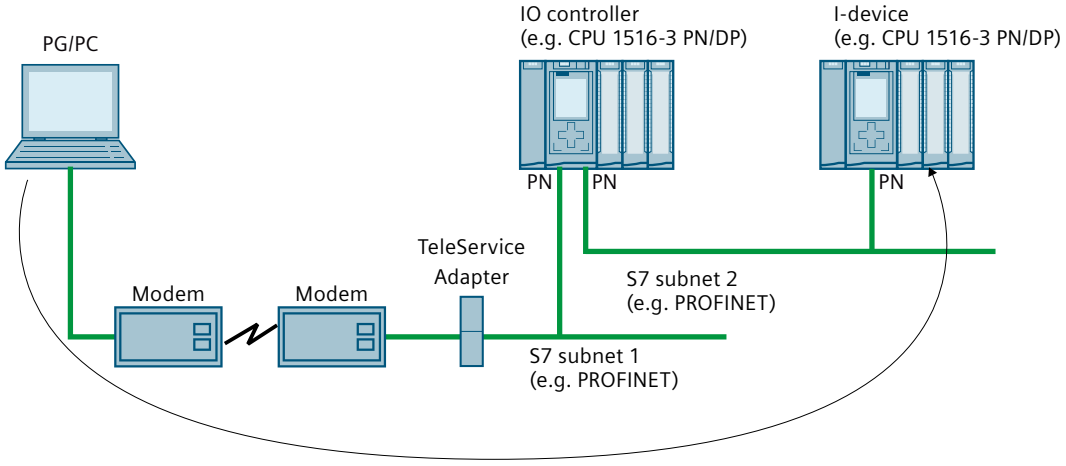


Figure 3-255 Remote maintenance of a plant using TeleService

More information

- The allocation of connection resources with S7 routing is described in the section Allocation of connection resources (Page 424).
- You can find more information on setting up TeleService in the STEP 7 online help.
- For information on HMI communication, refer to the section HMI communication (Page 127).
- You can find more information on S7 routing and TeleService adapters when you search the Internet using the following links:
  - Device manual Industrial Software Engineering Tools TS Adapter IE Basic (https://support.industry.siemens.com/cs/us/en/view/51311100)
  - Downloads for the TS Adapter (https://support.industry.siemens.com/cs/us/en/ps/16006/dl)

13.3 IP forwarding

Forwarding of IP packets with IP forwarding

IP forwarding is a device function to pass along IP packets between connected IP subnets.

Enable/disable the IP forwarding function in STEP 7. For CPUs as of FW version V4.1, you can also enable/disable the IP forwarding function in the user program by transferring a data record.

When IP forwarding is enabled, the S7-1500 CPU forwards received IP packets not addressed to the CPU to locally connected IP subnets or to a configured router.

The following figure shows how a programming device accesses data on an HMI device. Programming device and HMI device are located in different IP subnets. The IP subnets are connected to the two interfaces X1 and X2 of the CPU.

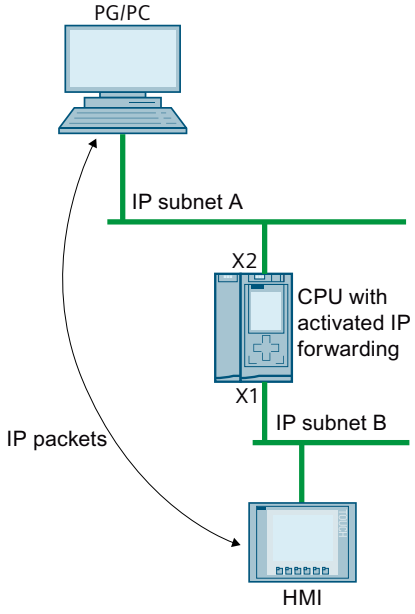


Figure 3-256 Access of a programming device to an HMI via IP forwarding

Areas of application

- Easy access from the control level to the field level for configuration and parameter assignment of field devices, e.g. via PDM or web browser
- Simplified integration of devices for remote access, e.g. for diagnostics during remote maintenance or firmware update

Requirements for using IP forwarding

- S7-1500 CPU as of firmware version V2.8
- Number of Ethernet interfaces:
  - The CPU has at least two Ethernet interfaces.
  - Or the CPU has one Ethernet interface, and a CP 1543-1 as of firmware version V2.2 provides the other Ethernet interface. In this case, the "Access to PLC via communication module" function must be enabled for the CP in the CPU.
- IP forwarding is enabled.
- Suitable standard gateways/routes are configured in each participating device along the outgoing and return paths of the IP packets.

IP route table

When IP forwarding is enabled, the CPU forwards received IP packets that are not addressed to itself. How the CPU forwards the IP packets is defined in its internal IP route table.

The CPU automatically creates the IP route table from the following information of the loaded hardware configuration:

- IP configuration of the Ethernet interfaces
- Configured router

Example of a configuration with IP forwarding

The following figure shows a sample configuration along with the required IP address settings and router settings.

- A PC on the IP subnet 192.168.4.0 communicates with an HMI device on the IP subnet 192.168.2.0.
- The IP address of a router ("Standard gateway") is configured at the CPU, Ethernet interface X3; in the figure below, it is the device that is designated as "IP router".
  In STEP 7, you configure a router in the interface properties under "Ethernet addresses" > "IP protocol".

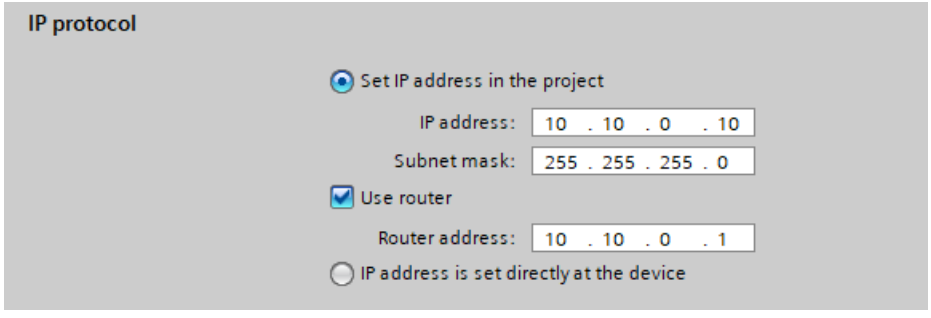


Figure 3-257 Configuring the router

- For the PC, the IP router, the IO device and the HMI device, the IP addresses of a standard gateway or the corresponding routes are also entered.

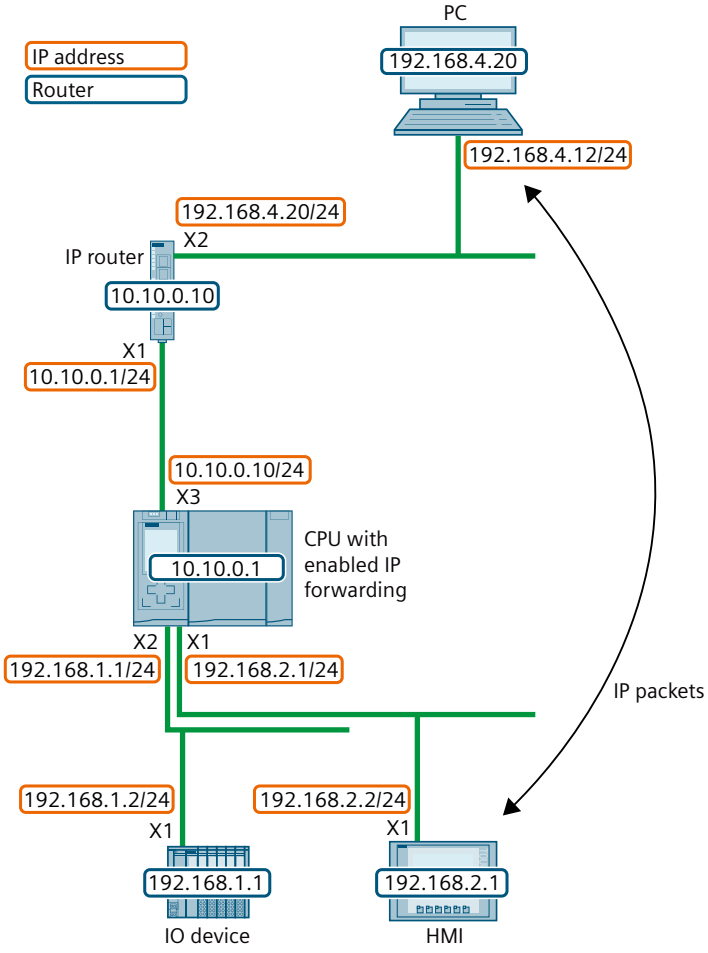


Figure 3-258 Sample configuration

This example configuration results in the following IP routing table for the CPU.

Table 3-30 IP route table of the CPU

Network destination	Interface	Gateway
0.0.0.0/0	10.10.0.10	10.10.0.1
192.168.1.0/24	192.168.1.1	-
192.168.2.0/24	192.168.2.1	-
10.10.0.0/24	10.10.0.10	-

For IP communication between the PG/PC and the HMI device, you need to set up additional IP routes to the IP subnet of the HMI device both in the PC and in the IP router. In the HMI device, you configure the IP address of the CPU interface X1 as the standard gateway.

In a Windows computer, for example, you set up an additional IP route from the command prompt using the command "route add <destination IP subnet> mask <subnet mask> <gateway>". However, you need administrative access rights to do this. For this example, enter the following prompt:

- "route add 192.168.2.0 mask 255.255.255.0 192.168.4.20"

In an IP router, you set up additional routes, e.g. via a web interface. Set up the following route for this example:

- Destination IP subnet: 192.168.2.0
- Subnet mask: 255.255.255.0
- Gateway: 10.10.0.10

Restrictions

You cannot configure any additional IP routes other than the router ("Standard Gateway") for an S7-1500 CPU. The network destination is either a connected IP subnet, or the network destination can be reached via exactly one configurable router. Because the S7-1500 CPU does not support additional IP routes, you cannot build bi-directional IP router cascades.

In the following configuration, you can configure either "Router 1" or "Router 2" in the CPU. "Router 1" is configured as an example. In this case, you cannot configure "Router 2". IP communication between the PC and the HMI device is not possible because the route is not continuous in both directions.

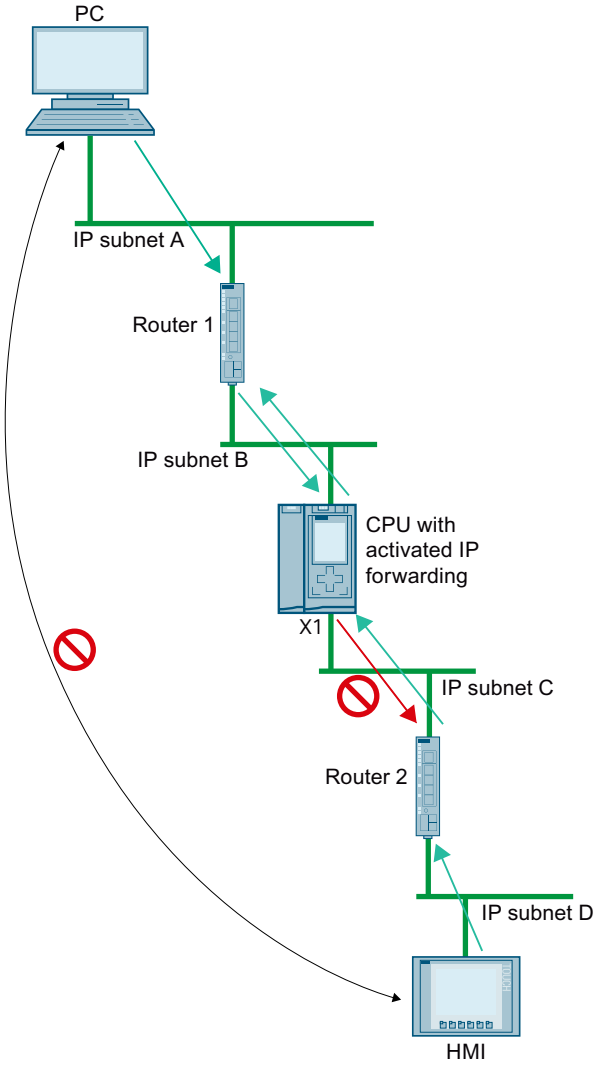


Figure 3-259 Unsupported IP router cascade

IP forwarding via the interface of a CP

IP forwarding also works via the interface of a CP. For this you have to activate the "Access to PLC via communication module" function for this CP in the CPU.

How you enable the "Access to PLC via communication module" function is described in the online help of STEP 7.

IP forwarding via the interface of a CP is **not** supported by the CPs (IE) for the ET 200SP CPUs.

Reaching C/C++ Runtime of the CPU 1518 4 PN/DP MFP via interfaces X1 or X2

If you activate PN/DP MFP IP forwarding for the CPU 1518 4 PN/DP, you will not only reach devices in the IP subnet of interface X3 via interfaces X1 and X2, but also C/C++ Runtime. From the C/C++ Runtime of the CPU 1518 4 PN/DP MFP, you reach all devices in the IP subnets of the interfaces X1, X2 and X3.

Conditions:

- IP forwarding is enabled for the CPU 1518 4 PN/DP MFP.
- The IP address of C/C++ Runtime and the IP address of interface X3 are located in the same IP subnet.
- The routes to the IP subnets at X1 and X2 are entered in C/C++ Runtime.
  In C/C++ Runtime, enter a route with the following command: "Route add-net <destination IP subnet> mask <subnet mask> gw <gateway>

The following figure shows a configuration in which a PC accesses the C/C++ Runtime of CPU 1518-4 PN/DP MFP via interface X2.

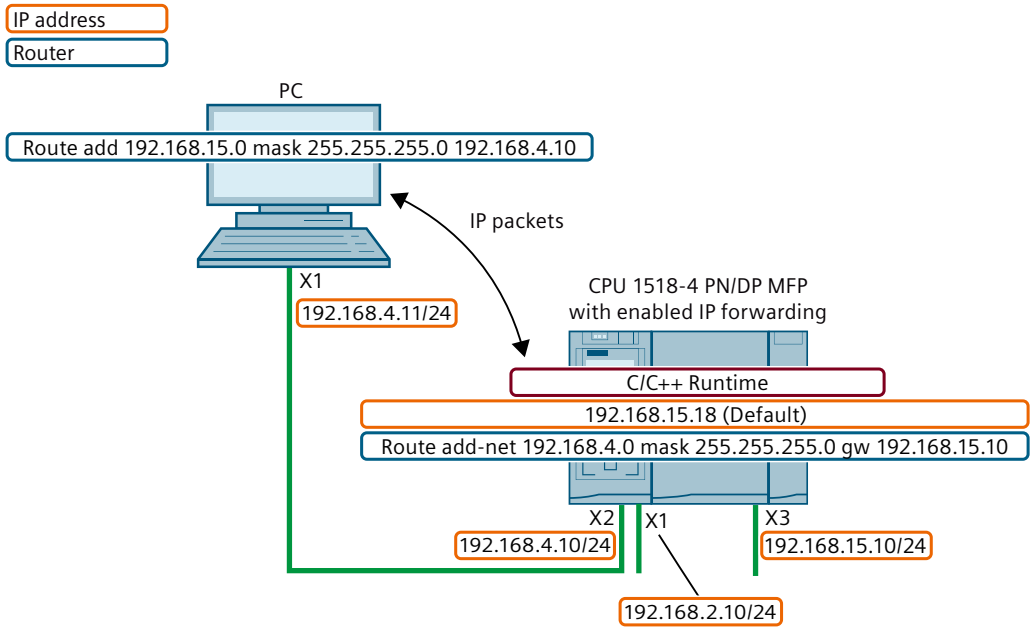


Figure 3-260 Access to C/C++ Runtime via interface X2

Take network security into account for IP forwarding

If you activate IP forwarding for a CPU, you enable "external" access to devices that are actually only accessible and controlled by the CPU. These devices are therefore usually not protected against attacks.

The following figure shows how to protect your automation system against unauthorized access.

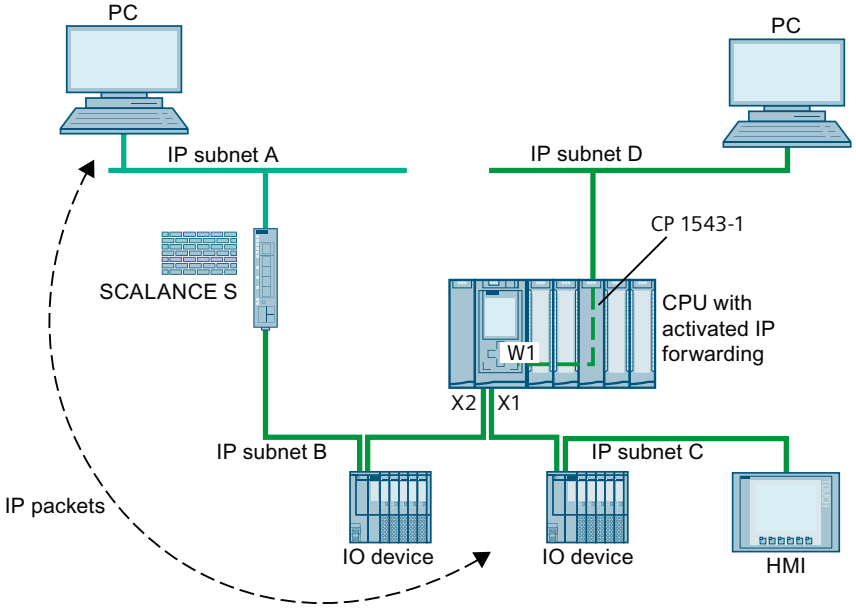


Figure 3-261 Network security for IP forwarding

- The CPU accesses all devices within the dark green IP subnets B and C close to the CPU via the interfaces X1 and X2.
- A SCALANCE S router is configured in the CPU. The CPU accesses the devices in the remote, light green IP subnet A via the router.
- The "Access to PLC via communication module" function is enabled for the CP 1543 in the CPU. The CPU reaches all devices within the IP subnet D via W1 interface.

If IP forwarding is activated in the CPU, a device from IP subnet A can access any device within IP subnets B, C and D close to the CPU.

Protect your automation system and connected devices against unauthorized access from outside.

Separate the CPU-related IP subnets from the remote IP subnets with a firewall. For example, use the SCALANCE S security modules with integrated firewall.
This application example (https://support.industry.siemens.com/cs/ww/en/view/22376747) describes how to protect an automation cell with a firewall using the SCALANCE S602 V3 and SCALANCE S623 security modules.

13.3.1 Enabling and disabling IP forwarding

You can set IP forwarding both in the CPU properties and via the CPU user program. To be able to set IP forwarding via the user program, use a CPU with FW version V4.1 or higher.

⚠ WARNING

Activated IP forwarding reduces security
When IP forwarding is enabled, the device forwards the IPv4 data traffic between the IP subnets that can be reached via its PROFINET interfaces. Forwarding reduces the protection of devices located in the IP subnets against unauthorized access via the network.
You should only enable IP forwarding in a protected environment (commissioning phase) or separate the CPU-related IP subnets from the remote IP subnets with a firewall. For example, you can use the SCALANCE S Security Modules with integrated firewall.

Enabling/disabling IP forwarding in the CPU properties

To enable IP forwarding, proceed as follows:

1. Select the CPU in the network view of STEP 7 (TIA Portal).
2. In the properties of the CPU of the Inspector window, navigate to "General > Advanced Configuration > IP forwarding".
3. In the "Configuration IPv4 forwarding" area, select the "Enable IPv4 forwarding for interfaces of this PLC" check box.

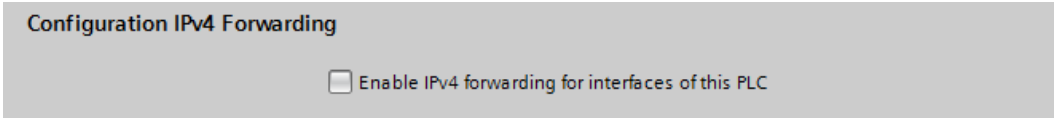


Figure 3-262 Enabling IP forwarding

Result: IP forwarding is enabled for all interfaces of the S7-1500 CPU.

You disable IP forwarding by clearing the check box "Enable IPv4 forwarding for interfaces of this PLC".

Enabling/disabling IP forwarding via the user program

To enable or disable IP forwarding via the user program, proceed as follows:

1. Create a data block in STEP 7 that contains the following data record.

Byte	Element	Code	Explanation
0-1	BlockID	0x3021	Header The data record length is counted starting at byte 4 "Version".
2-3	BlockLength	8	
4	Version	0x01	
5	Subversion	0x00	
6-7	Reserved	0x0000	-
8-9	IP forwarding control	0, 1	0: Disabling IP forwarding. 1: Enabling IP forwarding.
10-11	Reserved	0x0000	-

2. Transfer the data record in an organization block (OB) with the "WRREC" (write data record) instruction to the CPU.
   - Use an integrated PROFINET interface of the CPU as the hardware component in the "ID" parameter of the "WRREC" instruction.
     Recommendation: Use PROFINET interface X1; this interface is available with every CPU.
     Address the interface using its system constant (e.g. ID := "Local~PROFINET_interface_1").
   - The index is 0x3021 (INDEX := 16#3021)

You can also use the data record to determine which IP forwarding status is active in the CPU. To do this, use the instruction "RDREC" (read data record) with the index 0x3021 to an integrated PROFINET interface, e.g. X1 of the CPU.

Interplay of IP forwarding configuration and user program

The CPU does not retentively save the activation status of IP forwarding set by record transfer. After each POWER OFF > POWER ON transition, memory reset or loading of the hardware configuration, the CPU applies the activation status of IP forwarding stored in the hardware configuration.
A transition from RUN > STOP or STOP > RUN has no effect on the current activation status of IP forwarding of the CPU.

13.3.2 Enabling/disabling IP forwarding via data record transfer: Example for a CPU 1516-3 PN/DP

Introduction

In the commissioning phase, you want to control the "IP forwarding" function via the user program. To enable the function, data record 0x3021 is transferred to a PROFINET interface of the CPU in the following example.

Requirement

- CPU 1516-3 PN/DP as of FW version V4.1
- STEP 7 as of version V21

Solution

Transfer the data record 0x3021, with the "Enable IP forwarding" option set, to a PROFINET interface of the CPU. This enables IP forwarding for all interfaces of the CPU.

The following example shows how you can create the data record in a global data block and transfer it in a program cycle OB (for example, OB 1) to the PROFINET interface (Local~PROFINET_interface_1).

To activate IP forwarding for the addressed PROFINET interface of the CPU 1516-3 PN/DP, follow these steps:

1. Create a global data block.
2. Assign a name, for example "ActivateIP_Fwd".
3. Under "Static", create the structure of the 0x3021 data record (in the figure: "IP_FwdRecord") and other tags for transferring the data record. The following figure shows the structure of the data block "ActivateIP_Fwd".

ActivateIP_Fwd

	Name	Data type	Start value	Re..	Ac...	Wr...	Vi..	Comment
1	Static							
2	IP_FwdStartWrite	Bool	false					Start writing Data record 16#3021
3	IP_FwdRecord	Struct						Data record 16#3021
4	blockID	UInt	16#3021					Data record ID
5	blockLength	UInt	8					Length of block
6	version	USInt	1					Byte 1/2 of blockversion
7	subversion	USInt	0					Byte 2/2 of blockversion
8	reserved_1	UInt	0					Reserved for future usage
9	IP_FwdControl	UInt	1					0: deactivate IP_Fwd, 1: activate IP_Fwd
10	reserved_2	UInt	0					Reserved for future usage
11	IP_FwdWritingDone	Bool	false					Writing done
12	IP_FwdWritingError	Bool	false					Error while writing
13	IP_FwdWritingStatus	DWord	16#0					Status of writing

Figure 3-263 Structure of the global data block "ActivateIP_Fwd"

4. Transfer the 0x3021 data record in a program cycle OB (for example, OB 1), with the "WRREC" (write data record) instruction to the CPU 1516-3 PN/DP. You can find an example program in the next section.

Programming example for the data record transfer in OB 1

Data record 0x3021 is transferred in the following program code:

```
//----------------------------------------
// Start writing IP Forwarding settings
//----------------------------------------
IF "ActivateIP_Fwd".IP_FwdStartWrite THEN
 IF (NOT "ActivateIP_Fwd".IP_FwdWritingDone)
 AND (NOT "ActivateIP_Fwd".IP_FwdWritingError) THEN
 "instWrrec_1"(REQ := "ActivateIP_Fwd".IP_FwdStartWrite,
 ID := "Local~PROFINET_interface_1",
 INDEX := 16#3021,
 DONE => "ActivateIP_Fwd".IP_FwdWritingDone,
 ERROR => "ActivateIP_Fwd".IP_FwdWritingError,
 STATUS => "ActivateIP_Fwd".IP_FwdWritingStatus,
 RECORD := "ActivateIP_Fwd".IP_FwdRecord);
 END_IF;
 IF "ActivateIP_Fwd".IP_FwdWritingError THEN
 ; // add error handling
 END_IF;
 IF "ActivateIP_Fwd".IP_FwdWritingDone THEN
 "ActivateIP_Fwd".IP_FwdStartWrite := FALSE;
 "ActivateIP_Fwd".IP_FwdWritingDone := FALSE;
 END_IF;
 END_IF;
```

Disable IP forwarding again

With a small change, you can use the program code used above to disable IP forwarding. Assign the value "0" to the tag "ActivateIP_Fwd".IP_FwdRecord.IP_FwdControl in the user program:

```
"ActivateIP_Fwd".IP_FwdRecord.IP_FwdControl := 0;
```

The next time the "WRREC" instruction is called, IP forwarding is disabled.

13.3.3 Enabling/disabling IP forwarding via data record transfer with S7-1500R/H CPUs

The S7-1500R/H system does not synchronize the IP forwarding status (enabled/disabled) for both CPUs. IP forwarding enabled by the "WRREC" instruction only affects the CPU whose PROFINET interface addresses the "WRREC" instruction. This allows you to enable IP forwarding on the S7-1500R/H system specifically on only one R/H CPU by data record transfer.

If you want to enable IP forwarding on both R/H CPUs of the S7-1500R/H system, you must call the "WRREC" instruction twice. Use the hardware component of a PROFINET interface, e.g. X1 of the left and right R/H CPU.

Example:

The S7-1500R/H system is in the "RUN-Redundant" system state.

If a PROFINET interface of the left CPU is addressed with the "WRREC" instruction, for example, the IP forwarding setting of the left CPU is changed. The IP forwarding status of the CPU on the right remains unchanged.

If the left CPU fails or is replaced, the loaded setting from the configuration in the CPU properties takes effect again after the SYNCUP. Only after the "WRREC" is executed for a PROFINET interface of the left CPU, the IP forwarding setting of the left CPU is changed again.

Solution:

Call the "WRREC" instruction twice. In the first call of "WRREC", address the hardware component of a PROFINET interface of the left-hand CPU. Call the "WRREC" instruction again. This time, address the hardware component of a PROFINET interface of the CPU on the right.

Hardware component for PROFINET interface X1:

- The hardware component of the PROFINET X1 interface of the left-hand CPU is Local1~PROFINET_interface_1.
- The hardware component of the PROFINET X1 interface of the right-hand CPU is Local2~PROFINET_interface_1.

Result: IP forwarding is enabled on both R/H CPUs of the S7-1500R/H system.

NOTE

Transferring the data record to the backup CPU

Call the "WRREC" instruction for the addressed PROFINET interface of the backup CPU only when the S7-1500R/H system has reached the "RUN REDUNDANT" system state. Otherwise, the data record cannot be transferred to the addressed PROFINET interface of the backup CPU and the "WRREC" will output an error.

The S7-1500R/H system signals changes to its system state, e.g. the change to "Run REDUNDANT", by calling the CPU redundancy error OB (OB 72) with the corresponding "Fault_ID".

Example: WRREC calls for both R/H CPUs

To enable/disable IP forwarding for the addressed PROFINET interface of both the CPUs by transferring data records, proceed as follows:

1. Create a global data block.
2. Assign a name, for example, "ActivateIP_Fwd".
3. Under "Static", create the structure of the 0x3021 data record (in the figure: "IP_FwdRecord") and other tags for transferring the data record. The following figure shows the structure of the data block "ActivateIP_Fwd".

ActivateIP_Fwd

	Name	Data ty..	Start val..	Re...	Ac...	Wr..	Vi...	Comment
1	Static							
2	IP_FwdStartWrite	Bool	false		☑	☑	☑	Start writing Data record 16#3021
3	IP_FwdRecord	Struct			☑	☑	☑	Data record 16#3021
4	blockID	UInt	16#3021		☑	☑	☑	Data record ID
5	blockLength	UInt	8		☑	☑	☑	Length of block
6	version	USInt	1		☑	☑	☑	Byte 1/2 of blockversion
7	subversion	USInt	0		☑	☑	☑	Byte 2/2 of blockversion
8	reserved_1	UInt	0		☑	☑	☑	Reserved for future usage
9	IP_FwdControl	UInt	1		☑	☑	☑	0: deactivate IP_Fwd, 1: activate IP_Fwd
10	reserved_2	UInt	0		☑	☑	☑	Reserved for future usage
11	plcLeft	Struct			☑	☑	☑	Writing status of left plc
12	IP_FwdWritingDone	Bool	false		☑	☑	☑	Writing done
13	IP_FwdWritingError	Bool	false		☑	☑	☑	Error while writing
14	IP_FwdWritingStatus	DWord	16#0		☑	☑	☑	Status of writing
15	plcRight	Struct			☑	☑	☑	Writing status of right plc
16	IP_FwdWritingDone	Bool	false		☑	☑	☑	Writing done
17	IP_FwdWritingError	Bool	false		☑	☑	☑	Error while writing
18	IP_FwdWritingStatus	DWord	16#0		☑	☑	☑	Status of writing

Figure 3-264 Structure of the global data block "ActivateIP_Fwd"

4. Add the organization block "CPU redundancy error" (OB 72) to your user program. You can find a program example for OB 72 in the next paragraph.
5. Open the program cycle OB (OB 1).
6. In OB 1, execute two "WRREC" instructions for transferring the data record to the respective addressed PROFINET interface of both CPUs. You can find a program example for OB 1 in the next paragraph.

   Result: The 0x3021 data record was transferred to the PROFINET interface of both the CPUs addressed in each case.

Programming example for the organizational blocks OB 72 and OB 1

Open the added OB 72. Use the following program code to determine whether the R/H system has assumed the "RUN-REDUNDANT" system state and set the starting command for the "WRREC" instructions:

```
//-----------------------------------------
// Check redundancy state and set "IP_FwdWrite"
//-----------------------------------------
IF #Fault_ID = B#16#03 OR #Fault_ID = B#16#06 THEN
 "ActivateIP_Fwd".IP_FwdStartWrite := TRUE;
END_IF;
```

Open the program cycle OB (OB 1). With the following program code, you can run two "WRREC" instructions for transferring the data record to the respective addressed PROFINET interface of both the CPUs:

```
//----------------------------------------
// Start writing IP Forwarding settings
//----------------------------------------
IF "ActivateIP_Fwd".IP_FwdStartWrite THEN
 IF (NOT "ActivateIP_Fwd".plcLeft.IP_FwdWritingDone)
 AND (NOT "ActivateIP_Fwd".plcLeft.IP_FwdWritingError) THEN
 // write IP Forwarding settings for the left PLC
 "instWrrec_1"(REQ := "ActivateIP_Fwd".IP_FwdStartWrite,
 ID := "Local1~PROFINET_interface_1",
 INDEX := 16#3021,
 DONE => "ActivateIP_Fwd".plcLeft.IP_FwdWritingDone,
 ERROR => "ActivateIP_Fwd".plcLeft.IP_FwdWritingError,
 STATUS => "ActivateIP_Fwd".plcLeft.IP_FwdWritingStatus,
 RECORD := "ActivateIP_Fwd".IP_FwdRecord);
 END_IF;
 IF "ActivateIP_Fwd".plcLeft.IP_FwdWritingError THEN
 ; // add error handling for left plc
 END_IF;
 IF (NOT "ActivateIP_Fwd".plcRight.IP_FwdWritingDone)
 AND (NOT "ActivateIP_Fwd".plcRight.IP_FwdWritingError) THEN
 // write IP Forwarding settings for the right PLC
 "instWrrec_2"(REQ := "ActivateIP_Fwd".IP_FwdStartWrite,
 ID := "Local2~PROFINET_interface_1",
 INDEX := 16#3021,
 DONE => "ActivateIP_Fwd".plcRight.IP_FwdWritingDone,
 ERROR => "ActivateIP_Fwd".plcRight.IP_FwdWritingError,
 STATUS => "ActivateIP_Fwd".plcRight.IP_FwdWritingStatus,
 RECORD := "ActivateIP_Fwd".IP_FwdRecord);
 END_IF;
 IF "ActivateIP_Fwd".plcRight.IP_FwdWritingError THEN
 ; // add error handling for right plc
 END_IF;
 IF ("ActivateIP_Fwd".plcLeft.IP_FwdWritingDone)
 AND ("ActivateIP_Fwd".plcRight.IP_FwdWritingDone) THEN
 "ActivateIP_Fwd".IP_FwdStartWrite := FALSE;
 "ActivateIP_Fwd".plcLeft.IP_FwdWritingDone := FALSE;
 "ActivateIP_Fwd".plcRight.IP_FwdWritingDone := FALSE;
 END_IF;
 END_IF;
```

Disabling IP forwarding

With a small change, you can use the program code used above to disable IP forwarding. Assign the value "0" to the tag "ActivateIP_Fwd".IP_FwdRecord.IP_FwdControl in the user program:

```
"ActivateIP_Fwd".IP_FwdRecord.IP_FwdControl := 0;
```

The next time the "WRREC" instruction is called, IP forwarding is disabled.

13.4 Data record routing

Definition of data record routing

Data can be sent over PROFINET from an engineering station to field devices via multiple networks. Since the engineering station addresses the field devices using standardized records and these records are routed via S7 devices, the term "data record routing" is used to refer to this type of routing.

The data sent using data record routing include the parameter assignments for the participating field devices (slaves) and device-specific information (e.g. setpoint values, limit values).

Data record routing is used, for example, when field devices of different manufacturers are used. The field devices are addressed using standardized data records (PROFINET) for configuration and diagnostics.

Data record routing with STEP 7

You can perform data routing with STEP 7 by calling a device tool (for example, PCT) via the TCI interface (Tool Calling Interface) and passing call parameters. The device tool uses the communication paths that STEP 7 also uses for communication with the field device.

No configuration is required for this type of routing except the installation of the TCI tools on the STEP 7 computer.

Example: Data record routing with the Port Configuration Tool (PCT)

You can use the Port Configuration Tool (PCT) to configure the IO link master of the ET200 and assign parameters to connected IO link devices. The subnets are connected via data record routers. Data record routers are, for example, CPUs, CPs, IMs, IO link master.

You can learn about the constellations of data record routers supported by the PCT in this FAQ (https://support.industry.siemens.com/cs/us/en/view/87611392).

The figure below shows an example configuration with the data record routing with PCT.

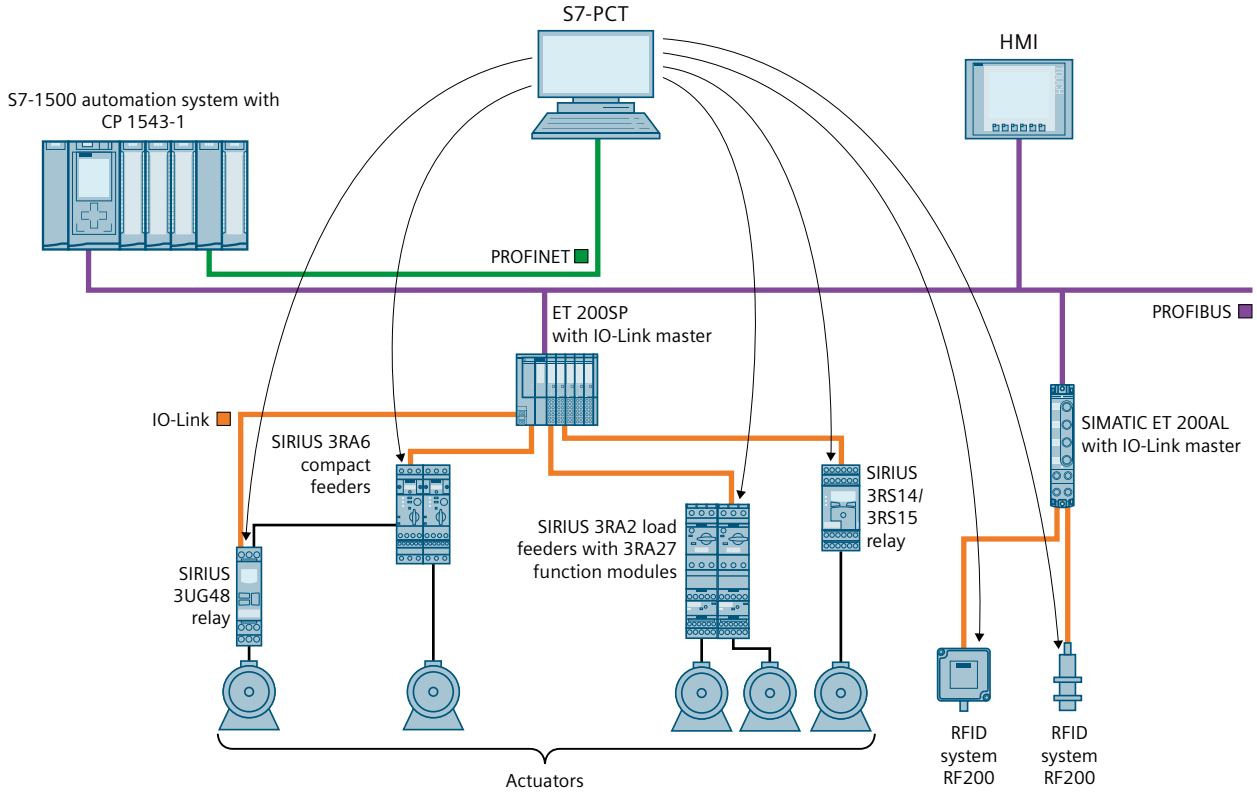


Figure 3-265 Example configuration for data record routing with PCT

Additional information

- The differences that exist between "normal" routing and data record routing are described in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/7000978).
- Whether or not the CPU, CP or CM you are using supports data record routing can be found in the relevant manuals.
- The allocation of connection resources with data record routing is described in the section Allocation of connection resources (Page 424).
- You can find additional information on configuration with STEP 7 in the STEP 7 online help.

13.5 Virtual interface for IP-based applications

As of firmware version 2.8, the S7-1500 CPU offers the option of reaching its IP-based applications, such as OPC UA, not only via its local (PN) interfaces, but also via the interfaces of communications processors in the same station. The supported communications processors can be found in the requirements. A communication partner can access these IP-based applications via a virtual interface that can be configured in the TIA Portal as of version V16. The virtual interface is called W1 (according to IEC 81346-2).

Features of the virtual interface

The virtual interface is not a fully diagnosable interface with the familiar properties of conventional interfaces. The virtual interface is not displayed in the graphical views, because the internal connection via the backplane bus does not represent an S7 subnet and does not have any ports. Therefore, a physical connection by means of a network cable cannot be established.

The IP address of the virtual interface is displayed (in the CPU display in the TIA Portal) and can be configured.

The following communication options can be used via the virtual interface W1:

- OPC UA (client and server)
- Programmed OUC connections
- Programming device/HMI communication
- Partner access from S7 CPUs via PUT/GET instructions

The activated interface can be used in dialogs where IP-based connections are configured.

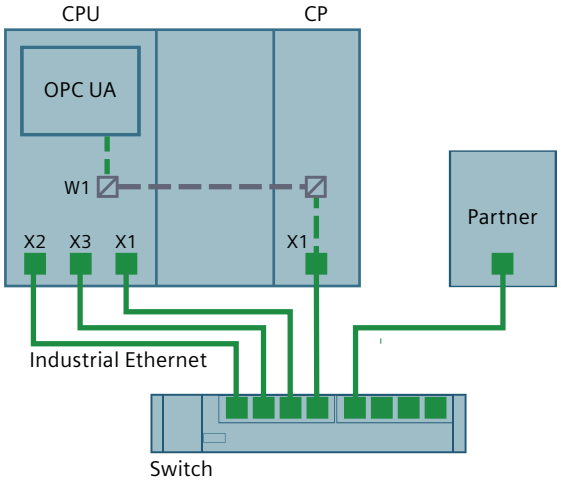


Figure 3-266 Principle of the virtual interface

Compared to conventional interfaces, the virtual interface has the following restrictions:

- No access to the web server over the virtual interface.
- Online backup is not possible via a connected programming device with the TIA Portal.
- If the CPU and communication partners are connected via the virtual interface, they cannot exchange data via LLDP (Link Layer Discovery Protocol).
- The S7 routing service does not use the virtual interface W1.

Requirement

For a CPU service to be accessible via the Ethernet interface of a CP, the following requirements must be fulfilled:

- S7-1500 CPU as of firmware version V2.8
- CP 1543-1 as of firmware version V2.2

Recommendation: Use a CP 1543-1 as of firmware version V3.0. As of this version, the security functions (firewall) are also available for the virtual interface and no additional firewall needs to be installed between the station and an insecure network.

Configuration of the virtual interface W1

In the properties of an S7-1500 CPU as of firmware version V2.8, you can assign a plugged communications module to the W1 virtual interface under "Advanced configuration > Access to PLC via communication module". You can then use this for external access to the CPU. If no CPs are plugged in or the plugged CPs do not support access to the CPU, the selection is empty.

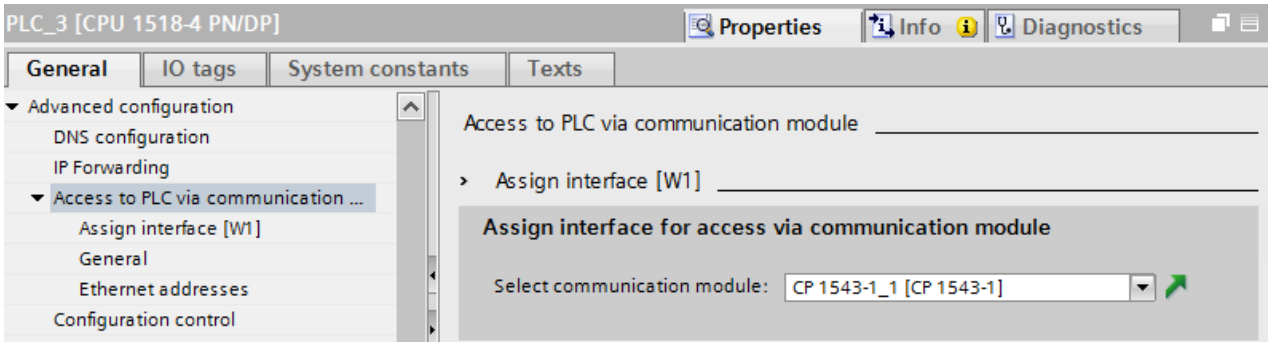


Figure 3-267 Selecting the CP in the CPU properties

After selecting the CP, the specifications and parameters for the virtual interface are displayed. You can edit the settings for the IP protocol and the PROFINET parameters here.

- The IP subnet is freely selectable, just like with the CP. The IP subnet is entered via the subnet mask and IP address of the virtual interface.
- When entering the IP subnet for the virtual interface, note that you are not using the same IP subnet as for the local interfaces of the CPU.

Once the IP address is entered, it is shown in the properties dialog of the OPC UA server in the list of server addresses. These settings provide the CPU with the new W1 virtual interface, via which the CPU services described above, such as the OPC UA server, can be accessed via a communications module. The corresponding connections and S7 communication (e.g. HMI and BSEND, BRCV) are made via this interface. The OPC UA server does not allow selection of a specific interface (selection via an IP address), it is only possible to select either all or none.

NOTE

The IP address of the virtual interface is not listed as W1 in the device display under the currently displayed local interfaces (Xn) but is available under "Addresses" in the "Settings" section. The virtual interface is also visible when no CP is plugged or when the virtual interface is not activated. If no IP suite is available, the IP address and the subnet mask are 0.0.0.0.

If you change the configured and loaded IP address parameters of the virtual interface via display, T_CONFIG instruction, or online, the loaded configuration is active again after the CPU restarts.

Configuration changes on the CP

A change in the assigned communications module may have an effect on the configuration of the virtual interface:

- In the properties of the CPU:
  - Assignment of a different CP: The configuration is used for the new CP.
  - Deselect the assigned CP: The virtual interface W1 is deactivated and the configuration is lost.
    When a CP is assigned again, the configuration must be performed again.
- On the device:
  - Moving the CP: If the CP is only moved to another slot of the device, the configuration continues to be valid.
  - Removing the CP: If the CP is deleted or moved to another device, the configuration is retained. In the drop-down list of the CPU, the CP is displayed as missing and compiling the configuration indicates an error. The missing CP can be deselected or assigned to another CP.

Display in the diagnostics and the system constants

The virtual interface W1 is displayed in the diagnostics view under "Online & Diagnostics". The hardware ID of the virtual interface is displayed in the system constants of the CPU properties.

Settings in the communications module (CP 1543-1 as of FW version V3.0)

Starting with firmware version V3.0 you can use the CP internal firewall to secure the data traffic via the virtual interface. To activate the firewall in the communications module, follow these steps in the protected project:

1. Select the communications module in the STEP 7 work area.
2. In the Inspector window, go to "Properties > Security".
3. Activate the "Enable security functions" option.
   The configurable security functions now appear in the Inspector window.
4. Activate the options "Enable firewall".
   In the Inspector window you can now allow the use of the virtual interface W1.

You can only secure data traffic via the W1 virtual interface of the CPU for the OPC UA service.

NOTE

Checking the manual configuration

If the firewall is enabled, you need to manually check whether the desired services are allowed by the firewall. Only enable those services for the IP and MAC filters that you also want to access via the CP interface. See the notes on security settings and firewall rules of the S7-1500 CPs in the information system of the TIA Portal.

Settings in the communications module (CP 1543-1, FW version V2.2, < V3.0)

The security functions of the CP 1543-1 with a firmware version lower than V3.0 cannot secure data traffic via the virtual interface. Although you can activate the security functions in the TIA Portal, it is not possible to compile such a configuration.

NOTICE
Connecting to non-secure networks If you connect the CP to a non-secure network, it is imperative that you place an additional firewall between the CP and the non-secure network. You can use the SCALANCE S602 V3 and SCALANCE S623 Security Modules with integrated firewall, for example.

Connection resources 14

14.1 Connection resources of a station

Introduction

Some communications services require connections. Connections occupy resources in the automation system (station). The connection resources are made available to the station by the CPUs, communications processors (CPs) and communications modules (CMs).

Connection resources of a station

The connection resources available depend on the CPUs, CPs and CMs being used and must not exceed a maximum number per station.

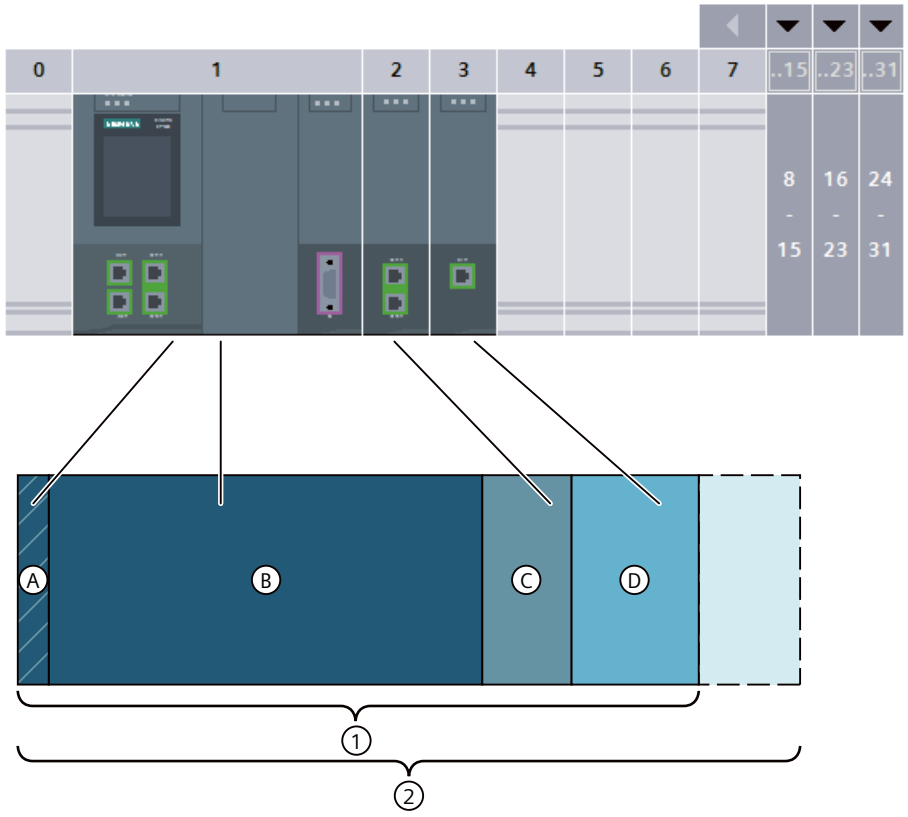
The maximum number of resources of a station is determined by the CPU.

Reserved connection resources
Each CPU has reserved connection resources for PG, HMI and Web server communication. This ensures, for example, that a PG can always establish at least one online connection with the CPU regardless of how many other communications services are already using connection resources.

Dynamic connection resources
In addition, dynamic resources exist. The difference between the maximum number of connection resources and the number of reserved connection resources is the maximum number of dynamic connection resources.

The communications services PG Communication, HMI Communication, S7 Communication, Open User Communication, Web Communication, OPC UA Client/Server Communication and other communication from the pool of dynamic connection resources are used.

The figure below shows an example of how individual components make connection resources available to an S7-1500 station.



① Available connection resources of the station, of which

- A: Reserved connection resources of the station
- A + B: Connection resources of CPU 1518
- C: Connection resources of communications module CM 1542-1
- D: Connection resources of communications processor CP 1543-1

② Maximum communications resources of the station using the example of a configuration from CPU 1518, CM 1542-1 and CP 1543-1

Figure 3-268 Connection resources of a station

Number of connection resources of a station

Table 3-31 Maximum number of connection resources supported for some CPU types

Connection resources of a station	**1511 1511C 1512C 1513**	**1515 1516**	**1517**	**1518**
Maximum connection resources of the station	128	256	320	384
of which reserved	10			
of which dynamic	118	246	310	374
Connection resources of the CPU	88	128	288	320

Connection resources of a station	1511 1511C 1512C 1513	1515 1516	1517	1518
Max. additionally usable connection resources by plugging in CMs/CPs	40	128	32	64
Additional connection resources CM 1542-1	64			
Additional connection resources CP 1543-1	118			
Additional connection resources CM 1542-5	48			
Additional connection resources CP 1542-5	16			

The number of connection resources supported by a CPU or a communications module is described in the technical specifications section of the Equipment Manuals.

Example

You have configured a CPU 1516-3 PN/DP with a CM 1542-1 communications module and a CP 1542-5 communications processor.

- Maximum connection resources of the station: **256**
- Available connection resources:
  - CPU 1516-3 PN/DP: 128
  - CM 1542-1: 64
  - CP 1542-5: 16
  - Total: **208**

The setup provides 208 connection resources. By adding further communications modules, the station can support a maximum of 48 additional connection resources.

Reserved connection resources

10 connection resources are reserved for stations with S7-1500 CPU, ET 200SP CPU and ET 200pro CPU based on S7-1500:

- 4 for PG communication required by STEP 7, for example, for test and diagnostics functions or downloading to the CPU
- 4 for HMI communication which are occupied by the first HMI connections configured in STEP 7
- 2 for communication with the Web server

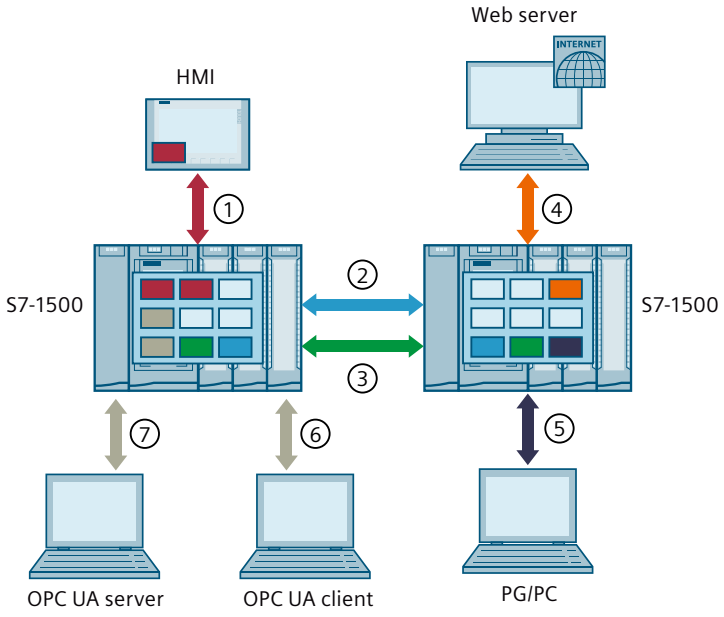
More information

Information on the connection resources of the S7-1500R/H redundant system is available in the section Connection resources of the redundant system S7-1500R/H (Page 448).

14.2 Allocation of connection resources

Overview - occupation of connection resources

The following figure shows how different connections occupy the resources of the S7-1500.



① HMI communication: See below.
② Open User Communication: Connections of Open User Communication occupy a connection resource in every end point.
③ S7 communication: Connections of S7 communication occupy a connection resource in every end point.
④ Web communication: The Web server connection occupies at least one connection resource in the station. The number of occupied connections depends on the browser.
⑤ PG communication: The PG connection occupies one connection resource in the station.
⑥ OPC UA client/server communication: Connection resource allocation for the server, see below
⑦ OPC UA client/server communication: Connection resource allocation for the client, see below

Connection resource for HMI communication
Connection resource for Open User Communication
Connection resource for S7 communication
Connection resource for Web communication
Connection resource for PG communication
Connection resources for OPC UA server communication

Figure 3-269 Allocation of connection resources

Connection resources for HMI communication

With HMI communication, the occupation of connection resources in the station depends on the HMI device being used.

Table 3-32 Maximum occupied connection resources for different HMI devices

HMI device	Maximum occupied connection resources of the station per HMI connection
Basic Panel	1
Unified Basic Panel	3
Comfort Panel	2[1]
Unified Comfort Panel	3
Mobile Panel	2[1]
RT Advanced	2[1]
RT Professional	3
Unified PC	3

[1] If you do not use system diagnostics or alarm configuration, the station occupies only one connection resource per HMI connection.

Example: You have configured the following HMI connections for a CPU 1516-3 PN/DP:

- Two HMI connections to an HMI TP700 Comfort. (2 connection resources each)
- One HMI connection to an HMI KTP1000 Basic. (1 connection resource)

In total 5 connection resources are occupied for HMI communication in the CPU.

Connection resources for OPC UA client communication

Each connection that the OPC UA client of the CPU has established to an OPC UA server occupies a connection resource in the station.

When establishing and closing an OPC UA connection, the OPC UA client temporarily occupies an additional connection resource. According to RFC 793, this connection resource is released again after a wait of approx. 60 seconds.

NOTE

Lack of resources due to temporary connection resources

A lack of connection resources occurs in the following situation:

- The OPC UA client of the CPU establishes or closes several connections simultaneously.
- The number of available connection resources of the station is insufficient for permanent and temporary connection resources of the OPC UA client communication.

Ensure that there are always enough available connection resources in the station to establish and end OPC UA connections.

Measures:

- Plan enough reserve for the OPC UA client connections.
- If necessary, establish or close the OPC UA connections one after the other.

Connection resources for routing

To transfer data beyond S7 subnets ("S7 routing"), an S7 connection is established between two CPUs. The S7 subnets are connected via gateways known as S7 routers. CPUs, CMs and CPs in S7-1500 are S7 routers.

The following applies for a routed S7 connection:

- A routed connection occupies one connection resource each in both end points. STEP 7 shows these connection resources in the "Connection resources" table.
- On the S7 router, two special connection resources are occupied for S7 routing. STEP 7 does not show the special connection resources for S7 routing in the "Connection resources" table. The number of resources for S7 routing depends on the CPU. You will find the resources for S7 routing in the technical specifications of the CPU in "Number of S7 routing connections".

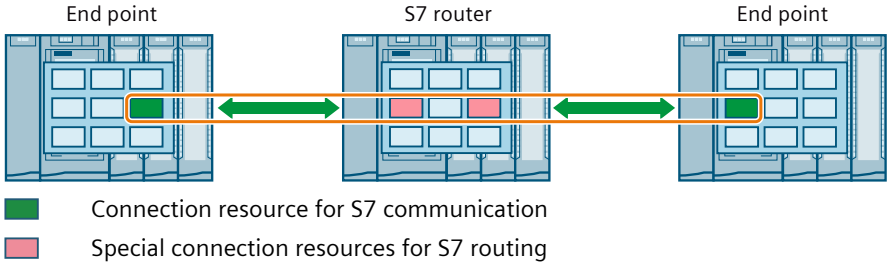


Figure 3-270 Connection resources with S7 routing

Data record routing also enables transfer of data beyond S7 subnets from an engineering station connected to PROFINET to various field devices via PROFIBUS.

With data record routing, as with S7 routing, two of the special connection resources for S7 routing are also occupied on every data record router.

NOTE

Connection resources with data record routing

With data record routing, on the data record router, two special connection resources for S7 routing are occupied. Neither the data record connection nor the allocated connection resources are displayed in the table of connection resources.

When are connection resources occupied?

The time for the occupation of connection resources depends on how the connection is set up (see section Setting up a connection (Page 44)).

- **Programmed setup of a connection**:
  As soon as an instruction to establish a connection is called in the user program (TSEND_C/TRCV_C or TCON), a connection resource is occupied.

  With suitable parameter assignment of the CONT parameter of the TSEND_C/TRCV_C instructions or by calling the TDISCON instruction, the connection can be terminated following data transfer and the connection resource is available again. When the connection is terminated, the connection resources on the CPU/CP/CM are available again.

- **Configured connections** (e.g. S7 connection):
  If you have configured a connection in STEP 7, the connection resource is occupied as soon as the hardware configuration is downloaded to the CPU.

  After using a configured connection for data transfer, the connection is not terminated. The connection resource is permanently occupied. To release the connection resource again, you need to delete the configured connection in STEP 7 and download the modified configuration to the CPU.
- **PG connection**:
  As soon as you have connected the PG to a CPU online in STEP 7, connection resources are occupied.
- **Web server**:
  As long as you have opened the Web server of the CPU in a browser, connection resources are occupied in the CPU.
- **OPC UA server**
  Each connection to the OPC UA server of the CPU occupies a connection resource in the station. This connection resource is released immediately when the connection is terminated.
- **OPC UA client**
  Each connection that the OPC UA client of the CPU has established to an OPC UA server occupies a connection resource in the station. When an OPC UA connection is established, the OPC UA client temporarily occupies an additional connection resource. When an OPC UA connection is terminated, the connection resource is not released again until after a wait time of approx. 60 seconds in accordance with RFC 793.

Monitoring the maximum possible number of connection resources

Offline
During configuration of connections, STEP 7 monitors the occupation of the connection resources. If the maximum possible number of connection resources is exceeded, STEP 7 signals this with a suitable warning.

Online
The CPU monitors the use of connection resources in the automation system. If you establish more connections in the user program than those provided by the automation system, the CPU acknowledges the instruction to establish the connection with an error.

S7-1500 and S7-300 comparison

You will find a comparison of how the communication resources of the S7-1500 and S7-300 are managed in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/109747092).

14.3 Display of the connection resources

Display of the connection resources in STEP 7 (offline view)

You can display the connection resources of an automation system in the hardware configuration. You will find the connection resources in the Inspector window in the properties of the CPU.

Connection resources

	① Station resources			② Module resour...	Module resour...	Module resour...
	Reserved		Dynamic ⚠	PLC_1 [CPU 15...	CM 1542-1_1 [..	CP 1543-1_1 [...
Maximum number of resources:		10	246	128	64	118
	Maximum	Configured	Configured	Configured	Configured	Configured
PG communication:	4	-	-	-	-	-
HMI communication:	4	4	6	6	0	4
S7 communication:	0	-	7	4	3	0
Open user communication:	0	-	13	8	5	0
Web communication:	2	-	-	-	-	-
OPC UA client/server communicatio...	0	-	-	-	-	-
Other communication:	-	-	0	0	0	0
Total resources used:		4	26	18	8	4
Available resources:		6	220	110	56	114

Figure 3-271 Example: Reserved and available connection resources (offline view)

① Station-specific connection resources

The columns of the station-specific connection resources provide information about the used and available connection resources of the station.

In the example, a maximum of 256 station-specific connection resources are available for the automation system.

- 10 reserved connection resources, of which 4 are already in use and a further 6 available. The used resources are divided up as follows:
  - 4 Resources for HMI communication
- 246 dynamic connection resources, of which 26 are already in use and a further 220 available.
  The used resources are divided up as follows:
  - 6 resources for HMI communication
  - 7 resources for S7 communication
  - 13 resources for Open User Communication

The warning triangle in the column of the dynamic station resources is displayed because the sum of the maximum available connection resources of CPU, CP and CM (= 310 connection resources) exceeds the station limit of 256.

NOTE

Available connection resources exceeded

STEP 7 signals the exceeding of the station-specific connection resources with a warning. To make full use of the connection resources from the CPU, CP and CM, either use a CPU with a higher maximum number of available station-specific connection resources or reduce the number of communications connections.

② Module-specific connection resources

The columns of the module-specific connection resources provide information about the use of resources on the CPUs, CPs and CMs of an automation system:

The display is per module and not per interface.

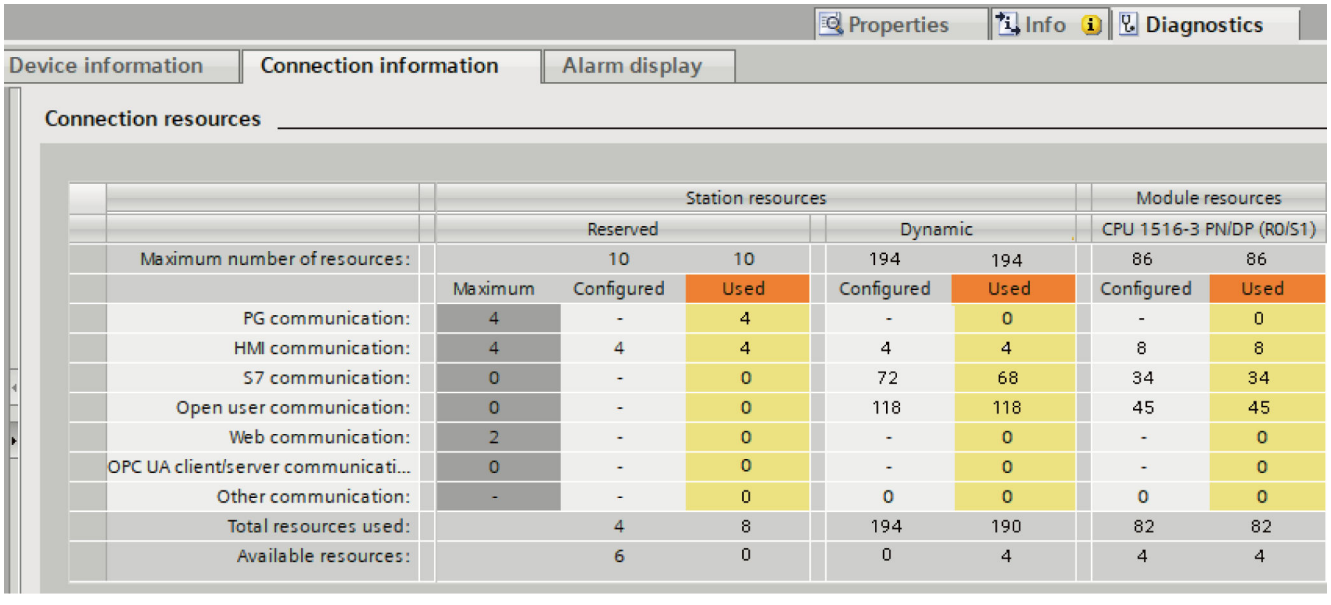
In the example, the CPU makes a maximum of 128 connection resources available, of which 18 are already in use and 110 still available.

The used resources are divided up as follows:

- 6 resources for HMI communication
- 4 resources for S7 communication
- 8 resources for Open User Communication

Display of the connection resources in STEP 7 (online view)

If you are connected to the CPU online, you can also see how many resources are currently being used under "Connection information".



	Station resources					Module resources	
	Reserved			Dynamic		CPU 1516-3 PN/DP (R0/S1)	
Maximum number of resources:		10	10	194	194	86	86
	Maximum	Configured	Used	Configured	Used	Configured	Used
PG communication:	4	-	4	-	0	-	0
HMI communication:	4	4	4	4	4	8	8
S7 communication:	0	-	0	72	68	34	34
Open user communication:	0	-	0	118	118	45	45
Web communication:	2	-	0	-	0	-	0
OPC UA client/server communicati...	0	-	0	-	0	-	0
Other communication:	-	-	0	0	0	0	0
Total resources used:		4	8	194	190	82	82
Available resources:		6	0	0	4	4	4

Figure 3-272 Connection resources - online

The online view of the "Connection resources" table in addition to the offline view also contains columns with the connection resources currently being used. Thus, the online view

displays **all** used connection resources in the automation system, regardless of how the connection was set up.

The "Other communication" row displays connection resources assigned for communication with external devices. The table is updated automatically.

NOTE

If a routed S7 connection goes through a CPU, the required connection resources of the CPU do not appear in the table of connection resources.

Display of the connection resources for HMI

For information regarding the availability and assignment of connection resources for HMI connections, refer to the "Connection resources" properties in the Inspector window of the offline view (in the context of the HMI device).

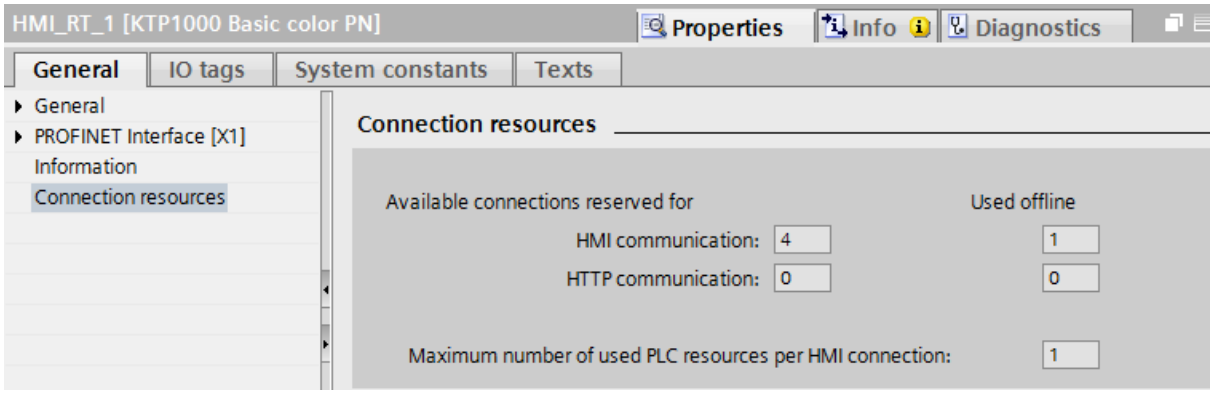


Figure 3-273 Connection resources - HMI communication

The following is displayed in the connection resources area:

- Number of available connections on the HMI reserved for HMI communication and HTTP communication
- Number of connection resources for HMI communication and HTTP communications used offline in the HMI

  If the maximum number of available connection resources for an HMI device is exceeded, a corresponding message is output by STEP 7.
- "Maximum number of used PLC resources per HMI connection". This parameter is a factor that is to be multiplied by the number of HMI connections used offline. The product is the number of HMI resources occupied on the CPU.

Displaying the connection resources in the Web server

You can display the connection resources not only in STEP 7, but also with a browser that displays the relevant page of the Web server.

You will find information on displaying connection resources in the Web server in the Web Server (https://support.industry.siemens.com/cs/us/en/view/59193560) function manual.

Diagnostics and fault correction 15

15.1 Connection diagnostics

Connections table in the online view

After selecting a CPU in the Devices & networks editor of STEP 7, you will see the status of your connections displayed in the online view of the connections table.

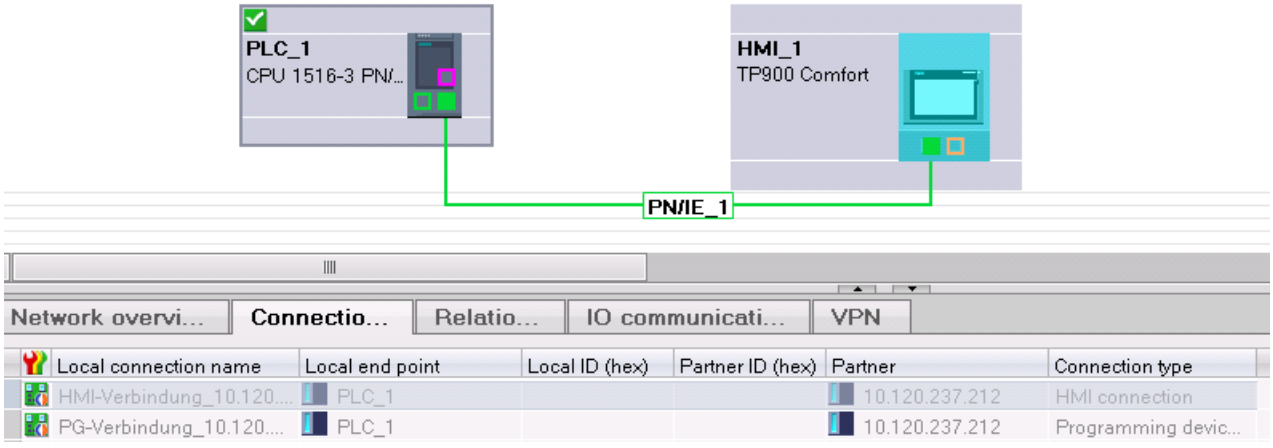


Figure 3-274 Online view of the connections table

After selecting the connection in the connections table, you obtain detailed diagnostic information in the "Connection information" tab.

"Connection information" tab: Connection details

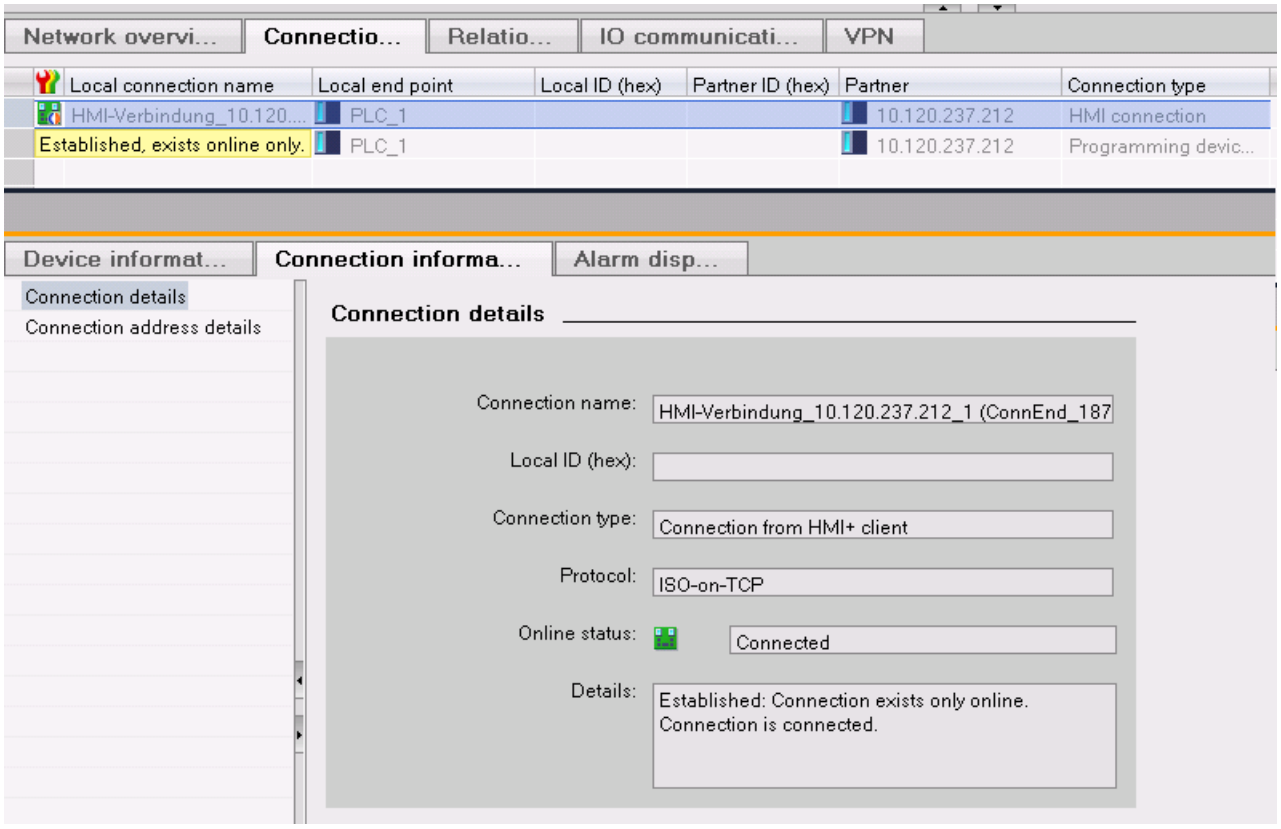


Figure 3-275 Diagnostics of connections - connection details

"Connection information" tab: Address details

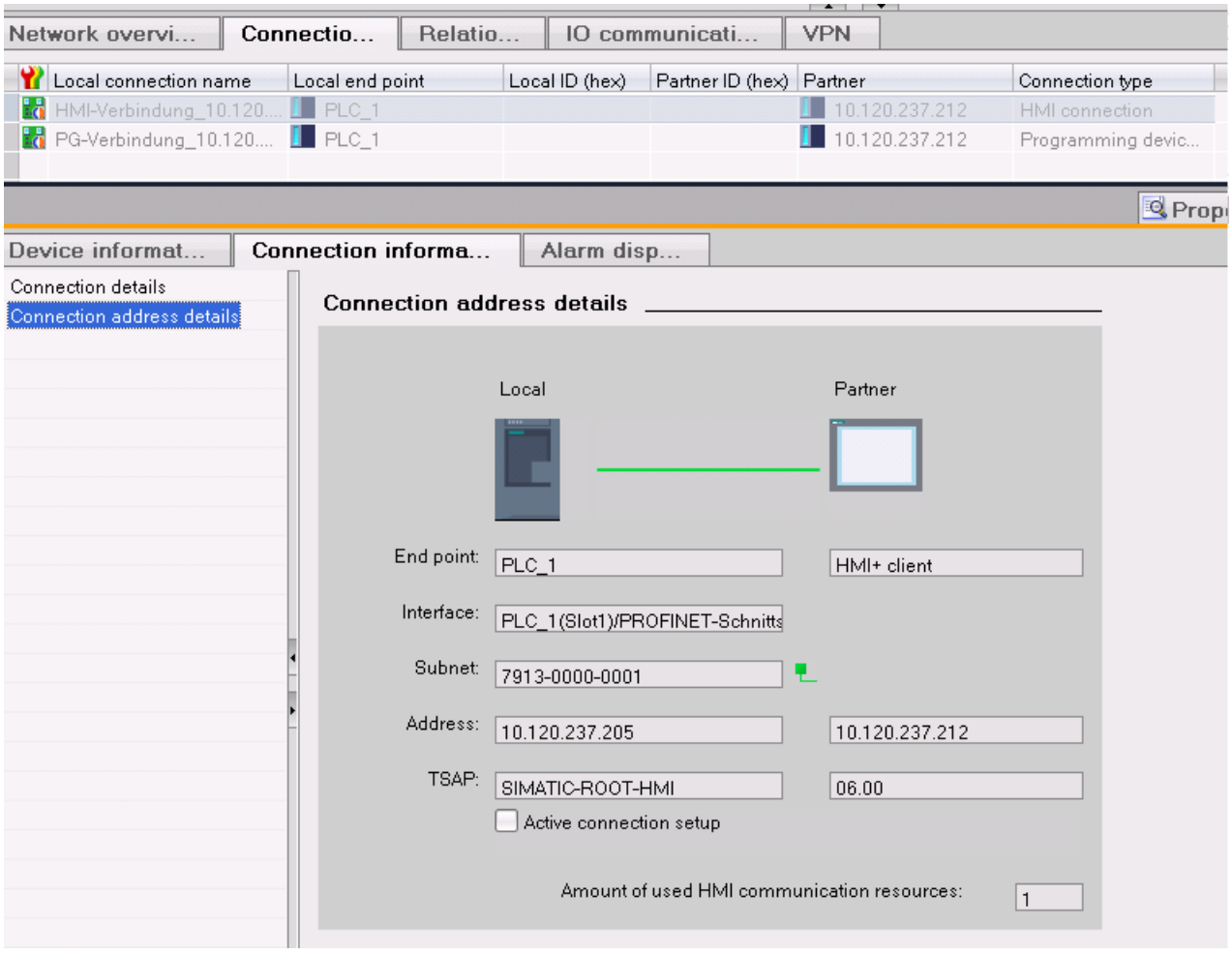


Figure 3-276 Diagnostics of connections - address details

Diagnostics via web server

You can evaluate diagnostic information from the CPU using a web browser via the integrated web server of a CPU.

On the "Communication" Web page, you will find the following information about communication via PROFINET in various tabs:

- Information on the PROFINET interfaces of the CPU (for example addresses, subnets, physical properties).
- Information on the quality of the data transfer (for example number of data packets sent/received error-free).
- Information about the allocation/availability of connection resources.
- The "Connection status" page is similar to the online view in STEP 7 and also provides an overview of all connections with detail view.

Diagnostics with the user program

When you program the T_DIAG instruction, you can evaluate diagnostic information about the configured and programmed connections of the CPU using the user program. For CPUs as of FW version V3.1, you can only use the T_DIAG instruction to evaluate the diagnostics information of OUC connections.

Additional information

You will find the description of the web server functionality in the function manual Web server (https://support.industry.siemens.com/cs/us/en/view/59193560).

15.2 Emergency address

If you cannot reach the CPU via the IP address, you can set a temporary emergency address (emergency IP) for the CPU. Via this emergency address, you can re-establish the connection with a CPU in order to load a device configuration with a valid IP address.

You can set an emergency address regardless of the protection level of the CPU

When do you need an emergency address?

Your CPU cannot be reached in the following cases:

- The IP address of your PROFINET interface is assigned twice.
- The subnet mask is set incorrectly.

Requirements

- You have selected "Set IP address in the project" for the IP protocol in the device configuration in STEP 7.
- No configuration with enabled DCP write protection loaded.
- The CPU is in STOP mode.

Restoring a valid device configuration with an emergency address

1. Set the emergency address for the interface of the CPU with a DCP tool. For example, the SIMATIC Automation Tool has a DCP command "Define IP address".
   The maintenance LED of the CPU lights up. The diagnostic buffer also shows that an emergency address was activated for an Ethernet interface.
2. Load a STEP 7 project with a valid IP address into the CPU.
3. Switch the CPU off and on again.
   The emergency address is reset.

Result

The CPU starts up with the valid IP address.

Communication with the redundant system S7-1500R/H

16

Introduction

Communication with the S7-1500R/H redundant system basically functions as with the S7-1500 standard system.

This chapter describes the special features and restrictions for communication with the S7-1500R/H redundant system.

Communication options for the S7-1500R/H redundant system

- Open User Communication via TCP/IP, UDP, ISO on-TCP and Modbus/TCP
- Secure Open User Communication with exception of the "Secure OUC via e-mail" function (see also Secure Open User Communication (Page 88))
- S7 communication as server
- HMI communication, PG communication
- Data exchange via OPC UA as server
- Secure PG/HMI communication (see also Secure PG/HMI communication (Page 106))
- SNMP
- Time-of-day synchronization via NTP
- Web server (only via Web API)
- Support of the CP 1543-1 communications processor as central plugged module (see also S7-1500R/H System Manual (https://support.industry.siemens.com/cs/us/en/view/109754833))

Restrictions for communication with the S7-1500R/H redundant system

- Open User Communication:
  - no configured connections
  - Email: The S7-1500R/H CPUs support only the versions < V5.0 of the "TMAIL_C" instruction. Versions from V5.0 are not supported.
  - No support of connection descriptions according to "TCON_Param"
- no S7 communication as client
- PG communication: It is not possible to access two CPUs online at the same time. You can either access the primary CPU or the backup CPU.

16.1 System IP addresses for R/H CPUs

Introduction

In addition to the device IP addresses of the CPUs, the S7-1500R/H redundant system also supports these system IP addresses:

- System IP address for the PROFINET interfaces X1 of the two CPUs (system IP address X1)
- System IP address for the PROFINET interfaces X2 of the two CPUs (system IP address X2)
- System IP address for the PROFINET interfaces X3 of the two CPUs (system IP address X3)

You use the system IP addresses for communication with other devices (for example, HMI devices, CPUs, PCs). The devices always communicate over the system IP address with the primary CPU of the redundant system. This ensures, for example, that the communication partner can communicate with the new primary CPU (previously backup CPU) in the RUN-Solo system state after failure of the original primary CPU in redundant operation.

There is a virtual MAC address for each system IP address.

You enable the system IP addresses in STEP 7.

Advantages of system IP addresses compared to device IP addresses

- The communication partner communicates specifically with the primary CPU.
- The S7-1500R/H redundant system can continue to communicate over a system IP address even if the primary CPU fails.

Applications

You use the system IP addresses for the following applications:

- HMI communication with the S7-1500R/H redundant system: You can use an HMI device to control or monitor the process on the redundant S7 1500R/H system.
- Open User Communication with the S7-1500R/H redundant system:
  - Another CPU or an application on a PC accesses data of the S7-1500R/H redundant system.
  - The S7-1500R/H redundant system accesses a different device.

  TCP, UDP and ISO-on-TCP-connections are possible.
- IP forwarding: If you use the system IP addresses as the gateway/default route for IP routes through the S7-1500R/H redundant system, IP packets are forwarded even if a CPU fails.

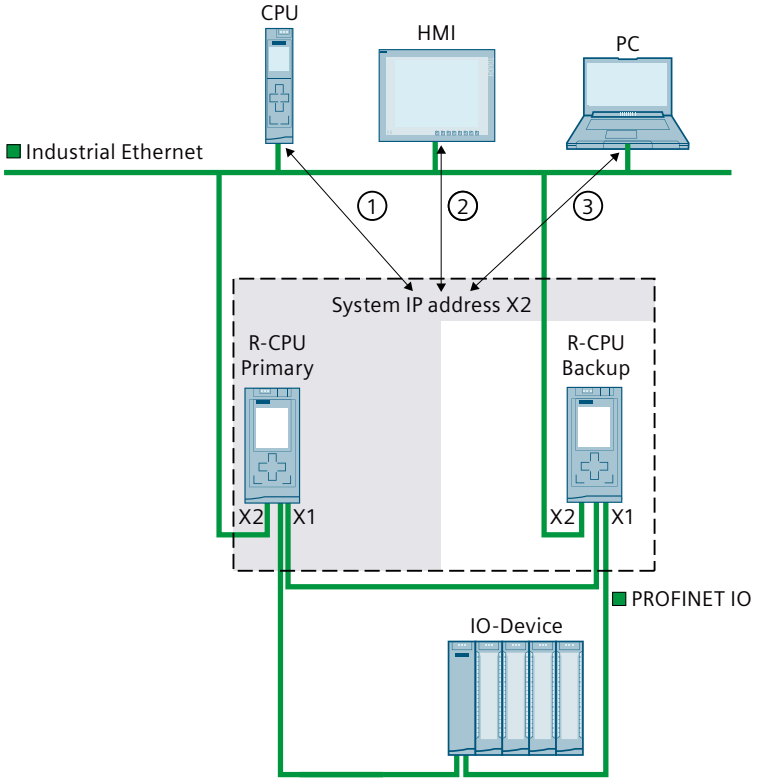
Requirements

- The interface of the communication partner is connected to both CPUs, each via the same interface (e.g. X2).
- The system IP address for the interfaces of the S7-1500R/H system is enabled.

Communication via the system IP addresses X2 and X3

If the CPUs of the redundant S7-1500R/H system have two or three PROFINET interfaces, it is preferable to use the PROFINET interface X2 or X3 for communication with other devices.

The following figure shows a configuration in which the communication partners are connected via the respective PROFINET interfaces X2 with the CPUs of the S7-1500R/H redundant system.

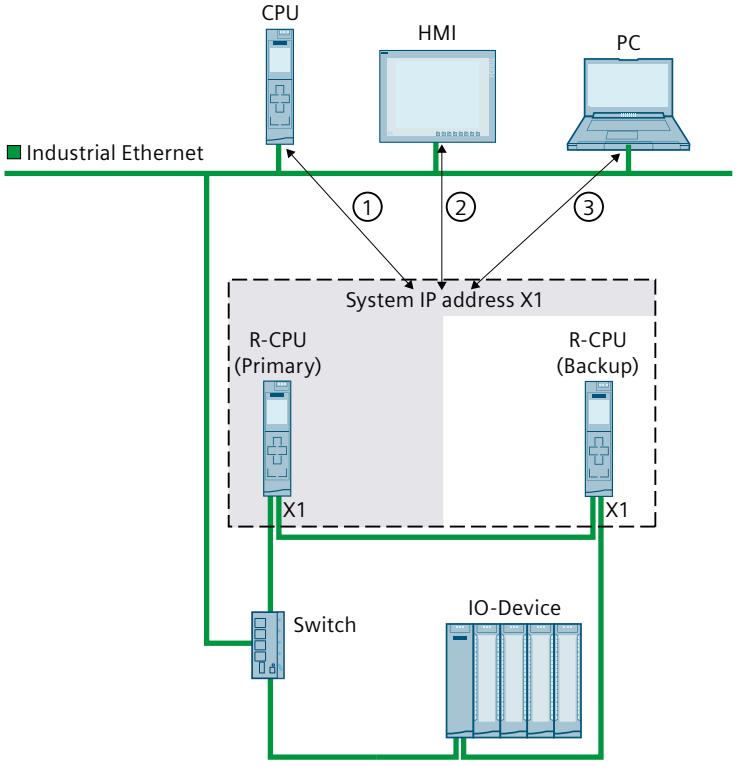


① Open User Communication between another CPU and the S7-1500R redundant system
② HMI communication with the S7-1500R redundant system
③ Open User Communication between the S7-1500R redundant system and a PC

Figure 3-277 Example: Communication of the S7-1515R redundant system via the system IP address X2

Communication via the system IP address X1

The following diagram shows a configuration where the communication partners are connected with a switch to the PROFINET ring of the S7-1500R/H redundant system. The PROFINET ring connects the communication partners with the respective PROFINET interfaces X1 of the two CPUs.
Since the CPU 1513R-1 PN only has one PROFINET interface, connection via the PROFINET ring is the only possibility of communicating via the system IP address X1.

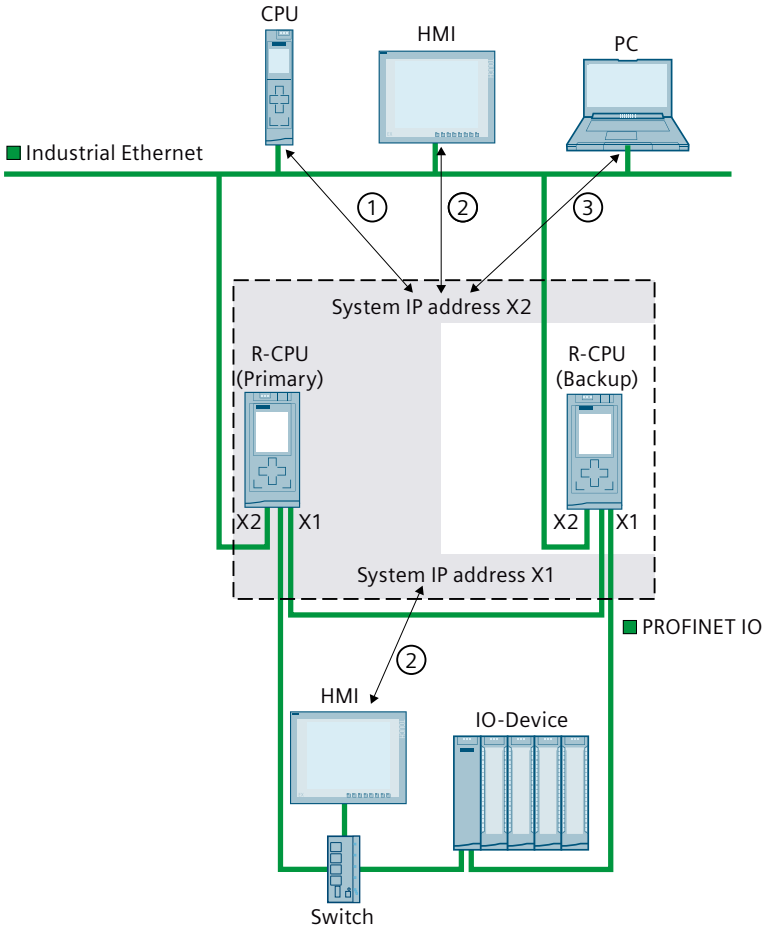


① Open User Communication between the S7-1500R redundant system and another CPU
② HMI communication with the S7-1500R redundant system
③ Open User Communication between the S7-1500R redundant system and a PC

Figure 3-278 Example: Communication of the S7-1513R redundant system via the system IP address X1

Communication via the system IP addresses X1, X2, and X3

You can use one system IP address for each PROFINET interface of the redundant S7-1500R/H system. PROFINET devices which are connected to X1 interfaces of the CPUs communicate via the system IP address X1. PROFINET devices which are connected to X2 interfaces of the CPUs communicate via the system IP address X2. PROFINET devices which are connected to the X3 interfaces of the CPUs communicate via the system IP address X3.



① Open User Communication between the S7-1500R redundant system and another CPU
② HMI communication with the S7-1500R redundant system
③ Open User Communication between the S7-1500R redundant system and a PC

Figure 3-279 Example: Communication of the S7-1515R redundant system via the system IP addresses X1 and X2

With an S7-1500H(F) system, you also have the option of dividing your system into several PROFINET rings.

In this case, you must connect the required S1/S2 devices in a separate PROFINET ring behind a Y-switch.

Recommendation: For increased availability of the S1/S2 devices, you need two Y-switches with DNA redundancy (SCALANCE XF204-2BA DNA). One Y-switch takes on the roles of MRP manager and DNA manager. Another Y-switch takes on the roles of MRP client and DNA client. DNA redundancy is only possible with a connected PROFINET ring.

You can find more information on configuration scenarios with Y-switches in the S7-1500R/H Redundant System (https://support.industry.siemens.com/cs/ww/en/view/109754833) System Manual.

IP forwarding via system IP addresses

If you use the system IP addresses as gateway/default routes for IP routes through the S7-1500R/H redundant system, IP packets are forwarded even if a CPU fails.

In the following figure, the PC is connected to the two X2 interfaces of the S7-1500R CPUs. Enter the system IP address X2 as a gateway in the PC for the route to the HMI device. The HMI device is connected to the PROFINET ring of the S7-1500 redundant system via a switch. The system IP address X1 is configured as the router in the HMI device.

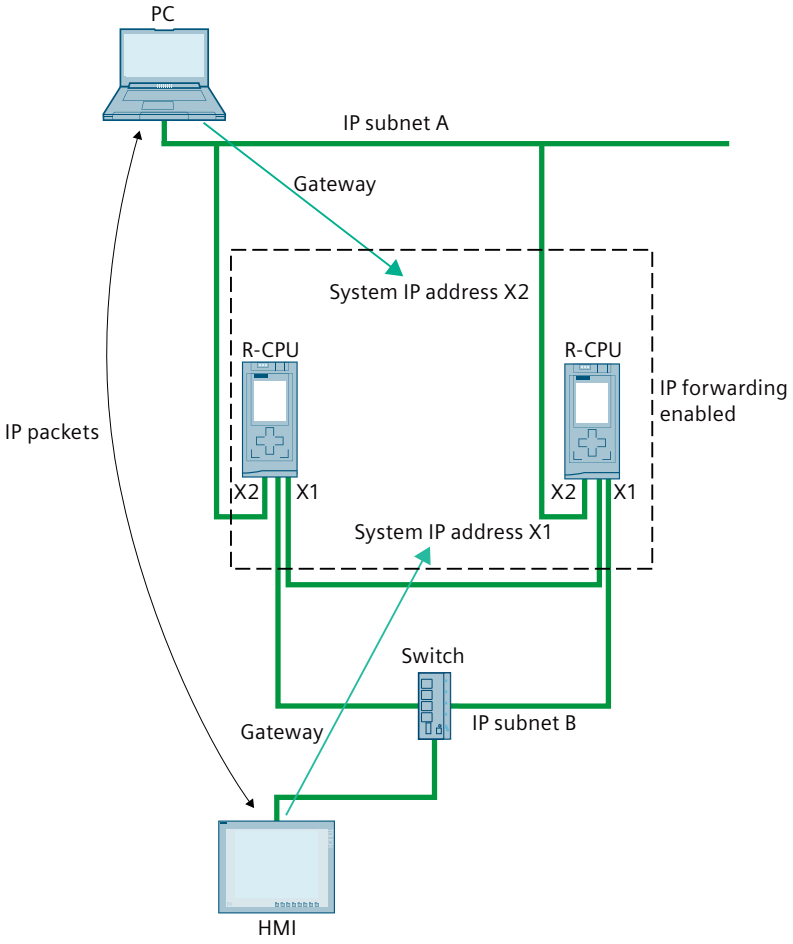


Figure 3-280 Example: IP forwarding via system IP addresses

Enable system IP addresses

Requirements:

- STEP 7 from V15.1
- S7-1500R/H redundant system with two CPUs, e.g. two 1513R-1 PN CPUs

If the CPUs of the S7-1500R/H redundant system have two PROFINET interfaces (X1 and X2), then you can use a system IP address for both PROFINET interfaces. The following describes how to enable the system IP address for the X1 interface.

To activate the system IP address for your S7-1500R/H redundant system, follow these steps:

1. In the network view of STEP 7, select the X1 interface of one of the two CPUs.
2. In the Inspector window, navigate to "Properties > General > Ethernet addresses" in the "System IP address for switched communication" area.
3. Select the check box "Enable the system IP address for switched communication".
   STEP 7 automatically creates a system IP address.

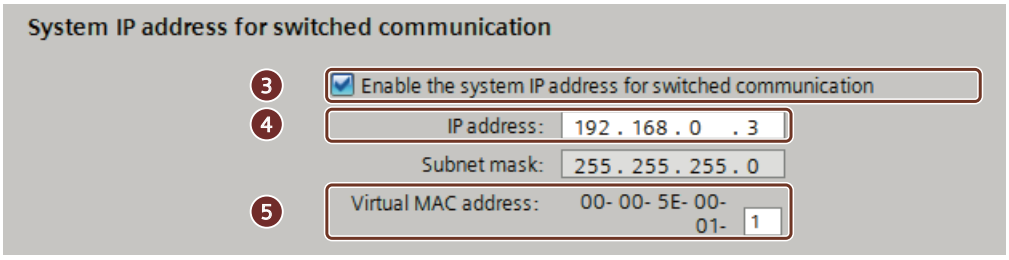


Figure 3-281 Configuring the system IP address

4. Adjust the system IP address as required.
5. If necessary, change the virtual MAC address. To do this, in "Virtual MAC address", assign a project-wide unique value (value range 01_H to FF_H) for the last byte.

NOTE

Uniqueness of the virtual MAC address

The S7-1500R/H redundant system uses a MAC address from the address range 00-00-5E-00-01-00 to 00-00-5E-00-01-00 for each system IP address. This address range is also used for VRRP (Virtual Redundancy Protocol).

If you use devices with VRRP, e.g. switches, ensure the uniqueness of the MAC addresses within an Ethernet broadcast domain.

Result: The X1 system IP address for the X1 PROFINET interface of the two CPUs is enabled.

16.2 System IP addresses for communications processors

Introduction

As of STEP 7 V19, you have the option of expanding redundant S7-1500R/H systems as of FW-version V3.1 with CP 1543-1 communications processors as of FW-version V3.0. When extended with CP 1543-1 communications processors, R/H-CPUs support the configuration of a W1 virtual interface with device and system IP-addresses. The communication partners connected to the CPs communicate with the R/H-CPUs via these IP addresses.

You can enable the system IP address of W1 in STEP 7.

There is a virtual MAC address for each system IP address.

Failure of a communications processor

In the event of a CP 1543-1 communications processor failure, the S7-1500R/H redundant system behaves as follows:

- S7-1500R:
  When a CP fails, the corresponding CPU changes to STOP mode. The S7-1500R system changes to the RUN-Solo system state.
  When the CP at the primary CPU fails, the S7-1500R redundant system performs a primary-backup switchover. The assigned system IP address changes to the new primary CPU. Establishing the new communication connection then takes place via the redundant CP.
  If the CP at the backup CPU fails, this failure has no effect on the existing communication via the system IP address.
- S7-1500H with active backplane bus:
  When a CP fails, the S7-1500H system remains in the RUN-Redundant system state.
  If the CP at the primary CPU fails, the redundant S7-1500H system does not perform a primary-backup switchover. The system IP address W1 is assigned to the failed CP via the primary CPU. To switch the system IP address W1 to the backup CPU, call the "RH_CTRL" instruction with mode=15 in the user program. As a result, the system IP address W1 is assigned to the backup CPU. The new communication connection is then established via the redundant CP of the backup CPU.

  If another CP on the primary CPU fails, the establishment of a new communication connection at the redundant CP is only possible via the assigned device IP address.

NOTE

If you communicate with the redundant system via the device IP addresses, you should preferably use the device IP address of the primary CPU. The transfer rate is better and the communication load is lower via the device IP address of the primary CPU.

You can find more information about the "RH_CTRL" instruction in the online help for STEP 7.

You can find information about configuring the system IP address for the W1 virtual interface and the virtual MAC address in the Redundant System S7-1500R/H (https://support.industry.siemens.com/cs/us/en/view/109754833) System Manual.

Advantages of expansion with CP 1543-1 communications processors

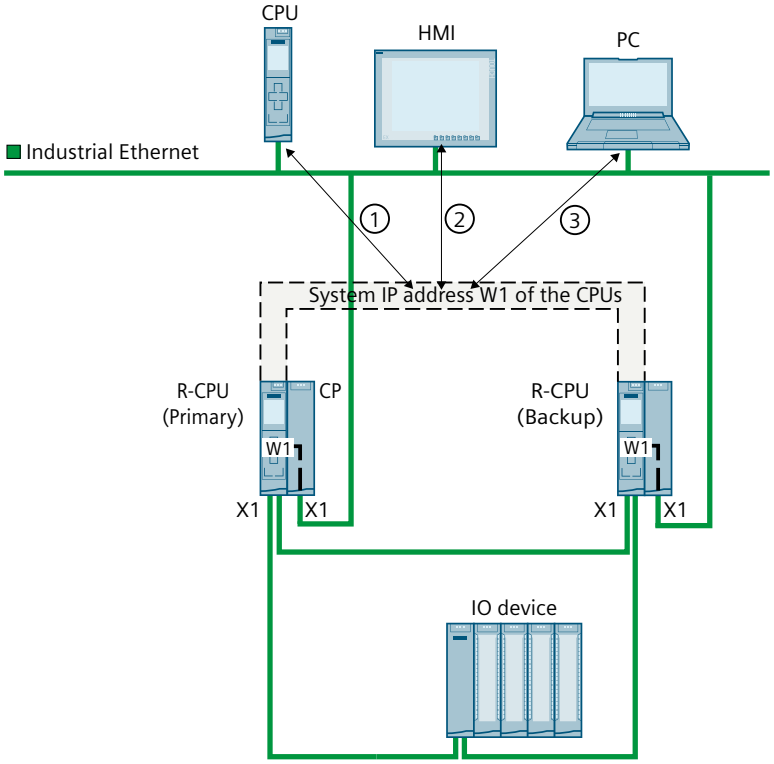
If you expand your redundant system with CP 1543-1 communications processors, additional communications interfaces become available. Use this advantage for a CPU 1513R-1 PN with only one PROFINET interface, e.g. for a network separation.

Requirements for using the W1 system IP address

- A CP 1543-1 is assigned to the W1 virtual interface.
- The system IP address of the W1 virtual interface is activated.
- A system IP address is assigned to the W1 virtual interface.
- A communication partner reaches both CPs via the assigned system IP address.

Communication via the W1 system IP address

The following figure shows the configuration of an S7-1513R redundant system with expansion by CPs. The communication partners communicate with the redundant system via the assigned W1 system IP address.



① Communication between the S7-1500R redundant system and another CPU
② HMI communication with the S7-1500R redundant system
③ Communication between the S7-1500R redundant system and a PC

Figure 3-282 Example: Communication of the S7-1513R redundant system via the assigned W1 system IP address

IP forwarding via system IP addresses

If you use the system IP addresses as gateway/default routes for IP routes through the redundant S7-1500R system, IP packets are forwarded even if a CP fails.

NOTE

Primary-backup switchover in S7-1500H systems with an active backplane bus
If there is a failure of a CP in an S7-1500H system with an active backplane bus, no primary-backup switchover takes place. In this case, set up the primary-backup switchover in your user program if required.

In the following figure, the PC is connected to the two X1 interfaces of the CPs 1543-1. For the route to the HMI device, the assigned W1 system IP address is entered in the PC as the router. The HMI device is connected via a switch to the PROFINET ring of the S7-1500R redundant system. In the HMI device, the X1 system IP address of the CPUs is entered as the router.

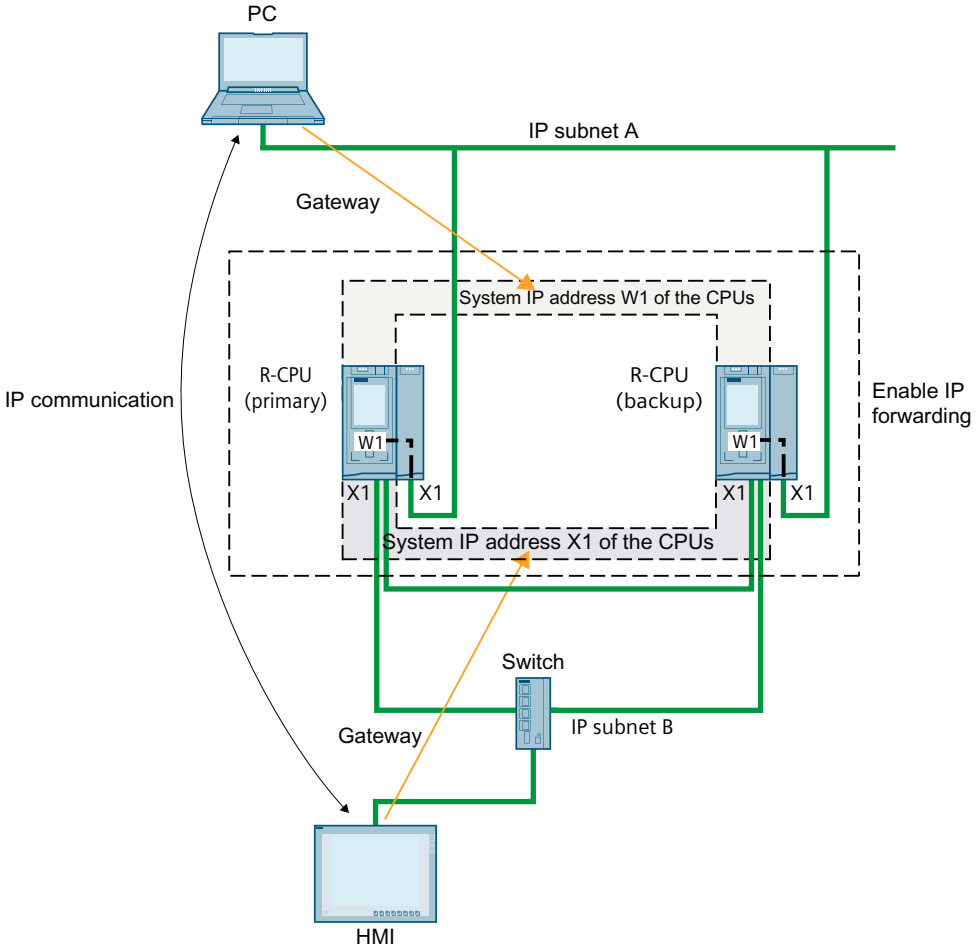


Figure 3-283 Example: IP forwarding via the system IP addresses of CPUs and CPs

Assigning the system IP address to the W1 virtual interface of R/H CPUs

Starting with STEP 7 V19, it is possible to assign a system IP address to the W1 virtual interface of R/H-CPUs. The communication partners that you have connected to the CPs communicate with the R/H system via the assigned system IP address.

To change the system IP address of the W1 virtual interface of the R/H CPUs, follow these steps:

1. Select the R/H CPU on rail_0 in the device view.
2. In the Inspector window, navigate to "Advanced configuration > Access to PLC via communications module".
3. Select the required CP from the "Select communication module" selection list in the "Assign interface [W1]" section.
   After selection, a warning message appears to inform you of possible risks associated with this setting. If you confirm the warning message, the configuration options for the W1 virtual interface are displayed.
4. Navigate to the "Internet protocol version 4 (IPv4)" area.
5. Accept the suggestion or assign a new IP address.
6. Navigate to the "System IP address for switched communication" area.
7. Select the option "Enable the system IP address for switched communication".
8. Accept the suggestion or assign a new system IP address (and virtual MAC address).

9. The R/H CPU on rail_1 automatically adopts the settings.

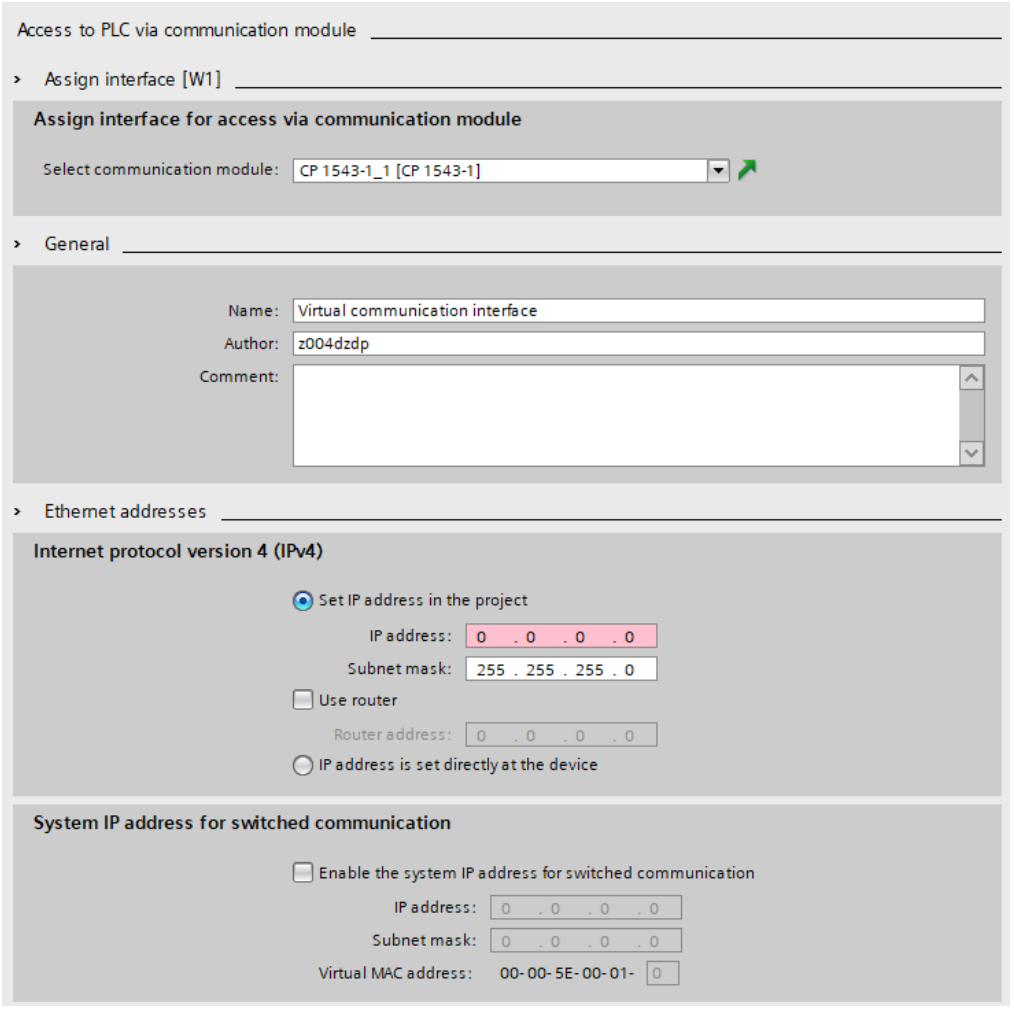


Figure 3-284 Configuring the system IP address of W1

Result: You have assigned a CP 1543-1 to the W1 virtual interface and configured the device/system IP address.

16.3 Improved accessibility by switching the system IP address

Switching the system IP address when CPU cannot be accessed

By default, the system IP addresses are assigned to the primary CPU.

From STEP 7 V20 (CPU firmware version as of V4.0), you can use the "RH_CTRL" instruction to switch the system IP addresses from the primary CPU to the backup CPU and back. For example, you can maintain communication if the primary CPU is not available.

More information

A description of the program-controlled switching of the system IP addresses can be found under the special instructions for redundant systems S7-1500R/H in the System Manual S7-1500R/H (https://support.industry.siemens.com/cs/us/en/view/109754833).

16.4 Behavior during SYNCUP

Response of communication connections via the system IP address in the system state SYNCUP

- HMI, PG- and S7-connections are temporarily closed. For a short time during the SYNCUP it is not possible to establish connections to the S7-1500R/H redundant system.
- All existing connections of Open User Communication are interrupted:
  - Connections set up by the CPUs of the redundant system as an active connection partner are set up again after the SYNCUP.
  - The S7-1500R/H redundant system sets up connection endpoints again for the passive connection establishment after the SYNCUP.
- The processing of running instances of the instructions TSEND and TRCV is stopped. The block parameter STATUS returns $80C4_H$ (temporary communication error).

16.5 Response to primary-backup switchover

Response of communication connections via the system IP address during a primary-backup switchover

- Running instances of the instructions TSEND and TRCV are stopped and return the status $80C4_H$ (temporary communication error).
- Connections successfully established by the S7-1500R/H redundant system are established again by the new primary CPU.
- The new primary CPU sets up connection endpoints again for the passive connection establishment.

NOTE

Increased duration of connection interruption

If the remote system does not transmit actively after the primary-backup switchover, the connection monitoring (e.g. TCP-Keep-Alive or application) may have to be performed by the remote system until the connection can be re-established.

16.6 Connection resources of the redundant system S7-1500R/H

Maximum number of connection resources of the S7-1500R/H redundant system

The maximum number of connection resources for the R/H CPUs depends on the following conditions:

- CPU type
- Firmware version
- Presence of communications processors CPs

You can find the different values in sec. Technical specifications of the equipment manuals of the R/H CPUs.

Allocation of connection resources

Communication connections occupy communication resources in the S7-1500R/H redundant system.

Each communication connection to the redundant system S7 1500R/H occupies connection resources in the S7 1500R/H station. The S7-1500R/H station comprises the hardware setup of both CPUs of the redundant S7-1500R/H system.

Depending on the IP address used, a communication connection also uses connection resources in one or both CPUs of the redundant S7-1500R/H system. The S7-1500R/H station can also be used to establish a communication connection.

The following table shows in which CPU a communication connection occupies connection resources depending on the IP address used.

Connect via...	Connection resources of the station	Connection resources CPU with redundancy ID 1	Connection resources CPU with redundancy ID 2
a system IP address	X	X	X
a device IP address of the CPU with redundancy ID 1	X	X	-
a device IP address of the CPU with redundancy ID 2	X	-	X

Display of the occupied connection resources in STEP 7

Requirement: Online connection to the redundant system S7-1500R/H

You will find the online display of the connection resources in the inspector window under "Diagnostics" > "Connection information". STEP 7 always displays the connection resources of the selected CPU and the S7-1500R/H-station.

Connection resources

	Station resources					Module resources	
	Reserved			Dynamic		CPU 1517H-3 PN (R0/S1)	
Maximum number of resources:		10	10	150	150	160	160
	Maximum	Configured	Used	Configured	Used	Configured	Used
PG communication:	4	-	2	-	0	-	2
HMI communication:	4	0	0	0	0	0	0
S7 communication:	0	-	0	0	0	0	0
Open user communication:	0	-	0	0	0	0	0
Web communication:	2	-	0	-	0	-	0
Other communication:	-	-	0	0	0	0	0
Total resources used:		0	2	0	0	0	2
Available resources:		10	8	150	150	160	158

Figure 3-285 Display of the connection resources of the S7-1500R/H redundant system in STEP 7

16.7 HMI communication with the redundant system S7-1500R/H

16.7.1 HMI connection via the system IP address

Requirements

- A S7-1500R/H redundant system, e.g. CPU 1513R-1PN
- System IP address is enabled
- HMI device with PROFINET interface

Procedure

To set up a HMI connection to an S7-1500R/H redundant system, follow these steps:

1. In the network view of STEP 7, select a PROFINET interface of the HMI device.
2. Using a drag&drop operation, draw a line between the PROFINET interface of the HMI device and a PROFINET interface of the S7-1500R/H redundant system.
   The HMI device and the S7-1500R/H redundant system are networked together.

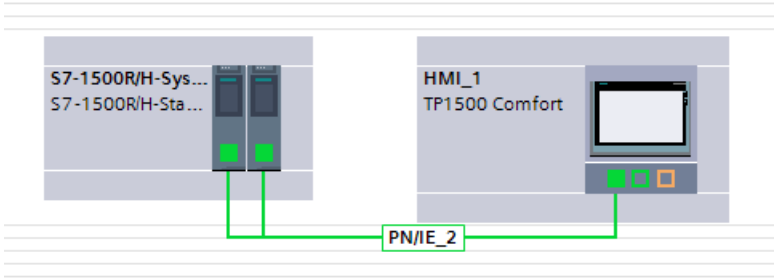


Figure 3-286 Networking an HMI device with the S7-1500R/H redundant system

3. In the list of functions, click the "Connections" icon. This activates connection mode.
4. Using a drag-and-drop operation, draw a line between the HMI device and a CPU of the S7-1500R/H redundant system.
   The list "Connection partners" opens.

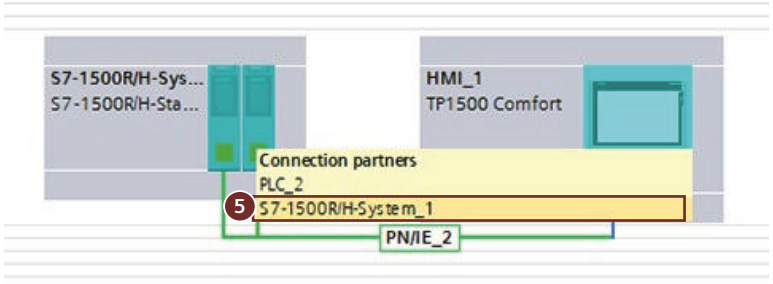


Figure 3-287 Setting up an HMI connection to the S7-1500R/H redundant system

5. Select the S7-1500R/H redundant system in the list "Connection partners".

Result: You have set up a HMI connection between the HMI device and the S7-1500R/H redundant system. The HMI connection uses the system IP address. The HMI device always connects to the primary CPU.

Changing the HMI connection over to the device IP address

To permanently change the HMI connection over to the selected CPU, clear the check box "Use the system IP address for switched communication" in the properties of the HMI connection. The HMI connection then uses the device IP address of the PROFINET interface. In the event of the failure of this CPU, then the HMI connection to this CPU permanently fails.

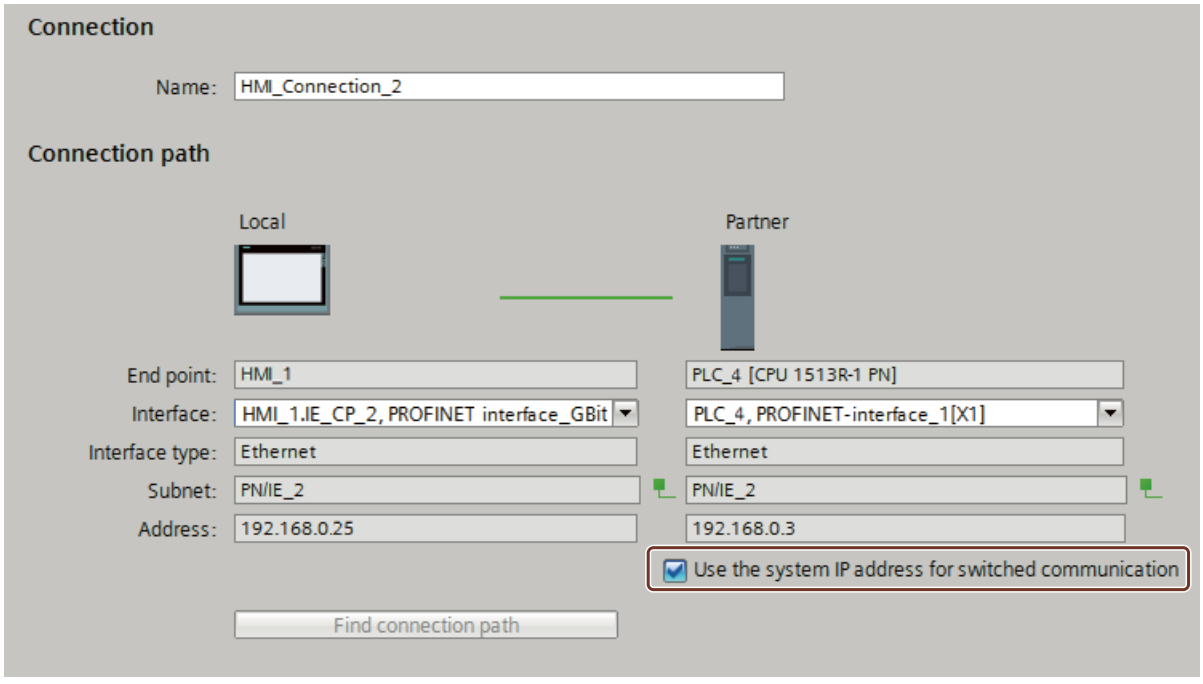


Figure 3-288 Properties of the HMI connection

NOTE

Automatic setup of HMI connection

When you drag-and-drop a tag from the S7-1500R/H redundant system into an HMI screen or into the HMI tag table, STEP 7 automatically sets up an HMI connection. This HMI connection exists by default between the PROFINET interface of the HMI device and the PROFINET interface X1 of the CPU with redundancy ID 1. The connection uses the device IP address of the PROFINET interface X1.

You can change the HMI connection to a system IP address in the properties of the HMI connection.

More information

You can set up an HMI connection to the S7-1500R/H redundant system via the devices IP address. With help of scripts in the HMI configuration, the connection of the failed CPU are switched automatically to the still running CPU. A description to this procedure can be found in the following FAQ (https://support.industry.siemens.com/cs/us/en/view/109781687).

16.8 Open User Communication with the redundant system S7-1500R/H

Introduction

S7-1500R/H systems as of FW version V3.1 also support Secure Open User Communication (Secure OUC).

If you extend an S7-1500R/H system as of FW version V3.1 with CP 1543-1 communications processors, you can also use Secure OUC via these connected CPs.

Requirements:

- STEP 7 as of V19
- CP 1543-1 as of FW version V3.0

Secure Open User Communication protocols for the S7-1500R/H redundant system

The following table shows which protocols of the Open User Communication you can use for the S7-1500R/H redundant system and the matching system data types and instructions.

Table 3-33 Protocols, system data types, and instructions that can be used for Open User Communication with the S7-1500R/H redundant system

Protocol	System data type	Instructions
TCP TLS over TCP	• TCON_QDN • TCON_QDN_SEC • TCON_IP_v4 • TCON_IP_V4_SEC	Establish connection and send/receive data via: • TSEND_C/TRCV_C or • TCON, TSEND/TRCV or • TCON, TUSEND/TURCV (connection can be terminated via TDISCON)
ISO-on-TCP	• TCON_IP_RFC	
UDP	• TCON_IP_v4 • TADDR_Param • TADDR_SEND_QDN • TADDR_RCV_IP	Establish connection and send/receive data via: • TSEND_C/TRCV_C • TUSEND/TURCV/TRCV (connection can be terminated via TDISCON)
Modbus TCP	• TCON_IP_v4 • TCON_IP_V4_SEC • TCON_QDN • TCON_QDN_SEC	• MB_CLIENT • MB_RED_CLIENT • MB_SERVER • MB_RED_SERVER

16.8.1 Setting up the connection of the Open User Communication with the redundant S7-1500R/H system

Open User Communication via integrated PROFINET interfaces of the CPU

The S7-1500R/H redundant system can communicate with other devices via Open User Communication.

You set up the connections in the user program, e.g. via the "TSEND_C" instruction. The S7-1500R/H redundant system does not support configured connections.

You can set up the connections via the following IP addresses of the integrated PROFINET interfaces:

- Device IP addresses:
  In redundant mode, the redundant system can establish or terminate connections and send or receive data via all device IP addresses of the redundant system.
  If you set up the connection via a device IP address, communication is routed via the associated CPU. If the CPU fails, then all communication through the device IP addresses of that CPU fails.
- System IP addresses:
  If you set up the connection via a system IP address, communication is always routed via the primary CPU.

Decide how you want to set up the connections based on your use case.

Open User Communication via CP 1543-1 communications processors

If you extend an S7-1500R/H redundant system with CP 1543-1 communications processors, you can then also use the following communication options:

- Local X1 interface of the CP 1543-1
- Own device IP address for the W1 virtual interface of each R/H CPU
- Common system IP address for the W1 virtual interface of the R/H system

You can find information on how to use a CP 1543-1 for a S7-1500R/H system in the System IP addresses for communications processors (Page 442) section.

Setting up a connection via a system IP address

The following describes how to set up a connection to a partner CPU via a system IP address of an integrated PROFINET interface of the redundant S7-1500R/H system.

You can set up the connection in the user program of the redundant S7-1500R/H system, e.g. with a TSEND_C instruction. In the user program of the partner CPU, create a corresponding TRCV_C instruction.

The procedure is described using the example of a TCP connection between the S7-1500R/H redundant system and a CPU 1516-3PN/DP.

Requirements

- A redundant S7-1500R/H system as TCP client, e.g. 2 CPUs 1513-1PN
- System IP address of the PROFINET interface X1 is enabled
- Connection partner as TCP server, e.g. CPU 1516-3 PN/DP
- The X1 PROFINET interfaces of the redundant 1513R CPUs and the X2 PROFINET interface of the CPU 1516-3PN/DP are located in the same subnet.

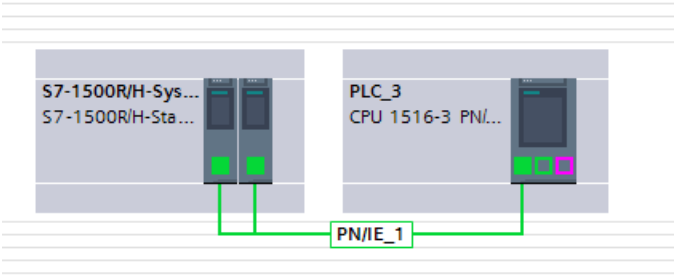


Figure 3-289 Example configuration for TCP-connection

TSEND_C instruction in the user program of the S7-1500R/H redundant system

To set up a TCP-connection to a different CPU, follow these steps:

1. Create a "TSEND_C" instruction in the user program.

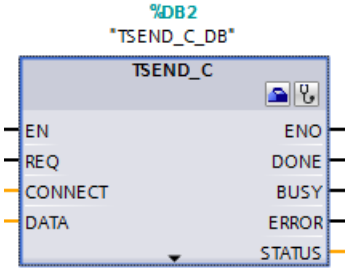


Figure 3-290 S7-1500R/H: "TSEND_C" instruction

2. Select the "TSEND_C" instruction.
3. In the Inspector window, go to "Properties" > "Configuration" > "Connection parameters". On the left-hand side you can see the S7-1500R/H redundant system as a local end point of the connection:
   - "Interface:": X1 is the preset interface.
   - "Subnet:": If the interface X1 is assigned to an S7-subnet, then STEP 7 displays the name of the S7-subnet.
   - The "Use system IP address" check box is enabled. The system IP address of the S7-1500R/H redundant system is in "Address".

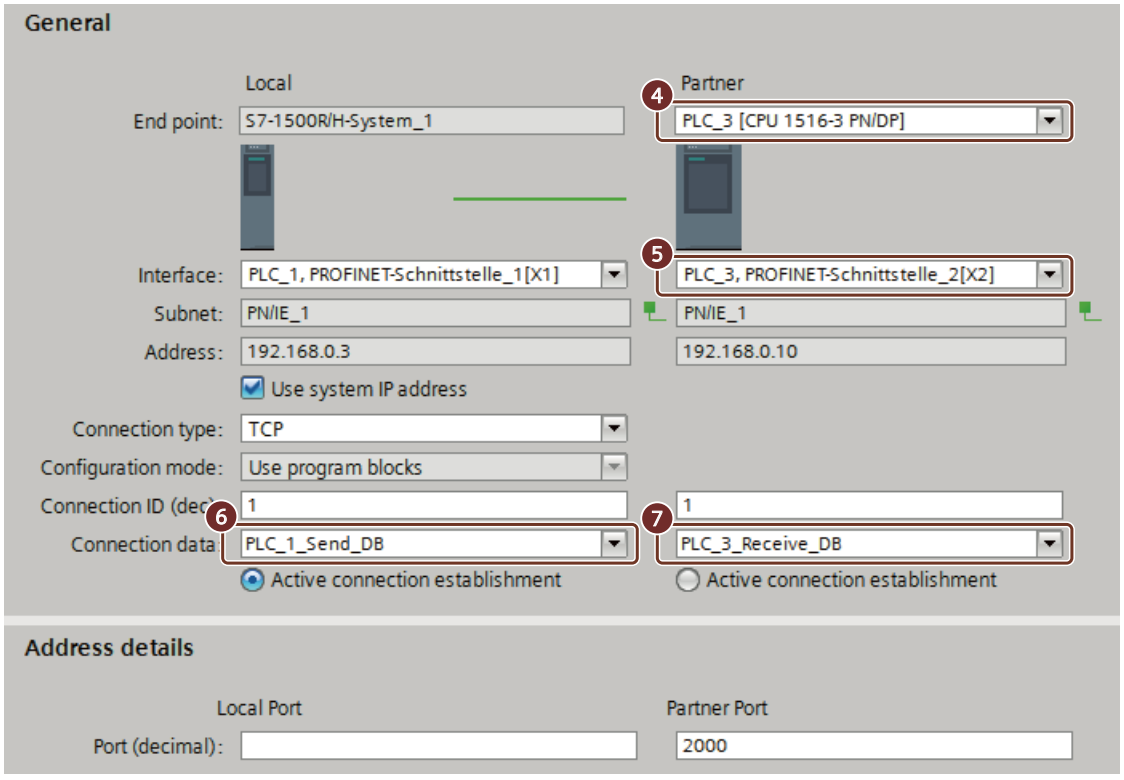


Figure 3-291 S7-1500R/H: Assigning parameters to the TSEND_C instruction in STEP 7

4. In "Partners" under "End point:" select the CPU 1516-3PN/DP as the communication partner.
5. In "Partners" under "Interface:" select the PROFINET interface X2 of the CPU 1516-3PN/DP.
6. In "Local" under "Connection data" select the setting "<new>".
   STEP 7 creates a data block for the connection data in the user program of the S7-1500R/H redundant system, for example "PLC_1_Send_DB".
   "TCP" is set by default as the connection type.
7. In "Partners" under "Connection type" select the setting "NEW".
   STEP 7 creates a data block for the connection data in the user program of the other CPU, for example "PLC_3_Receive_DB".

TRCV_C instruction in the user program of the CPU 1516 3PN/DP

Create a TRCV_C instruction in the user program of the CPU 1516-3PN/DP and assign parameters as below:

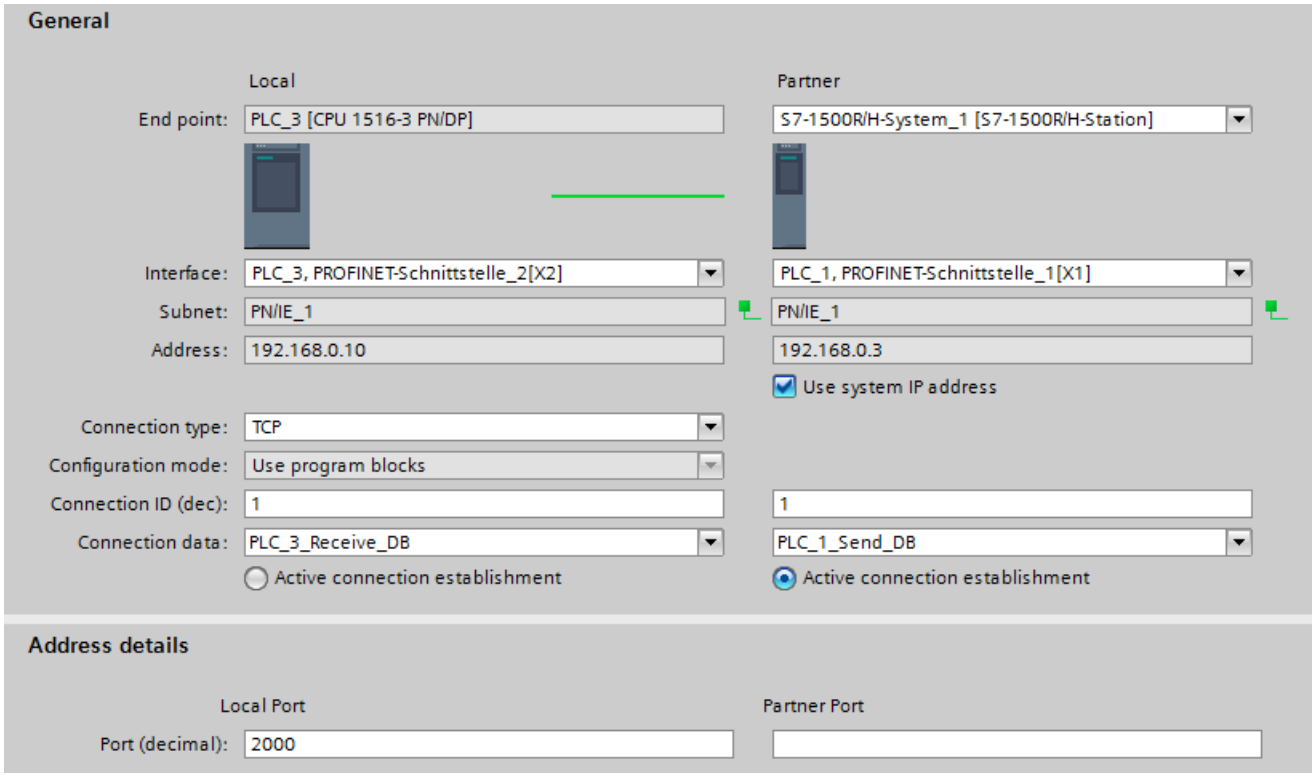


Figure 3-292 S7-1500-3PN/DP: Assigning parameters to the TRCV_C instruction in STEP 7

Setting up a connection via a device IP address

To set up an OUC-connection via a device IP address of one of the two CPUs:

- Select a suitable PROFINET interface of the S7-1500R/H redundant system.
- Clear the "Use system IP address" check box.

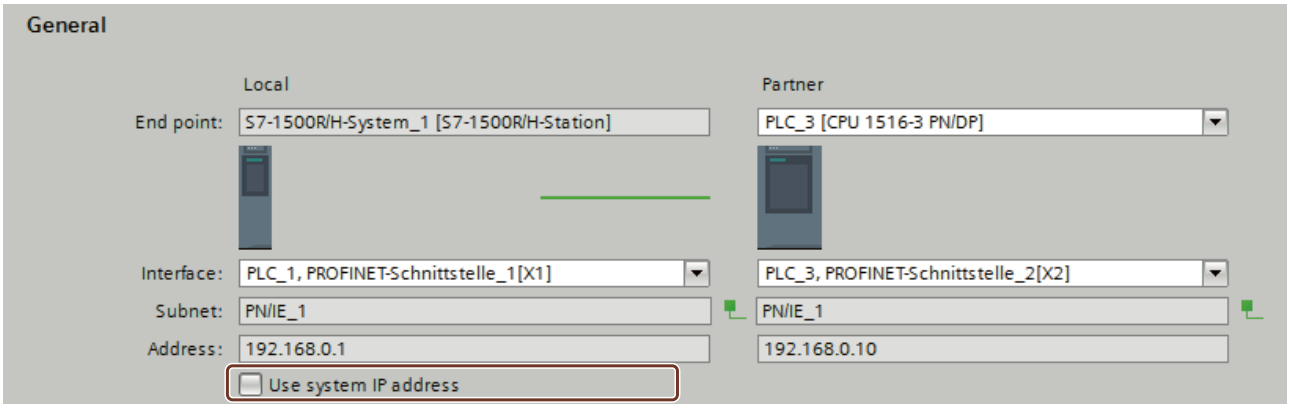


Figure 3-293 OUC-connection via a device IP address

More information

You can find more information on system states in the S7-1500R/H (https://support.industry.siemens.com/cs/ww/en/view/109754833) system manual.
You can find more information on the configuration and parameter assignment of your PROFINET IO system in the PROFINET Function Manual (https://support.industry.siemens.com/cs/ww/en/view/49948856).

16.8.2 Open User Communication with CP 1543-1 communications processors

Introduction

You can use both Open User Communication (OUC) as well as Secure OUC via the CP 1543-1 communications processors.
If you want to use Secure OUC, the following additional requirements must be met so that you can handle the device and CA certificates:

- Project protection is activated
- Security functions are enabled in each CP 1543-1 you want to use for Secure OUC.
- Same security settings in each CP on both primary and backup CPUs in the same slot
- The same CA certificates are configured for both CPs
- The device certificates of the CPs each refer to both CPs, e.g. configure an Subject Alternative Name (SAN) in both device certificates

NOTE
No automatic synchronization of the security settings
In STEP 7, the security settings are not automatically synchronized between the CPs. Therefore, configure the CPs in the same slot of the primary and backup CPUs identically.

Connection options for Open User Communication via CPs

For the following configurations, the OUC connection to a partner always goes via the local CP interface, regardless of whether OUC or Secure OUC is being used. Depending on which configuration you use, you have to adapt the connection parameters when setting up the communication connection. Select the corresponding HW identifier of the interface at the connection parameters using one of the following options:

- Use the CP interface with a local IP address:
  For the "InterfaceId" connection parameter, specify the HW identifier of the local Ethernet interface of a CP, e.g. "Local1~CP_1543-1_1~Ethernet_interface_1". Use the CP interfaces of both primary and backup CPUs in the RUN-Redundant system state.
- Use the W1 virtual interface of the CPU with a configured device IP address:
  For the "InterfaceId" connection parameter, specify the HW identifier of the virtual interface of a CPU, e.g. "Local1~Virtual_communication_interface". Use the virtual W1 interfaces of both the primary and backup CPUs in the RUN-Redundant system state
- Use the virtual W1 interface of the CPU with a configured system IP address:
  For the "InterfaceId" connection parameter, specify the HW identifier of the object with the string "...HSystemIPRef..." and the "Virtual" identifier in the default name, e.g. "Local1~Virtual_communication_interface~HsystemIPRef_1". This object then references the system IP address of the virtual W1 interface of the CPU.

Creating a connection via CPs

You can create the connection as for an integrated PROFINET interface of the S7-1500R/H redundant system. However, you have to adapt the connection parameters accordingly. Select the CP 1543-1 communications processor to be used in the "Interface" selection list.

If you want to use the "Use system IP address" option, a system IP address must be configured for the W1 virtual interface.

Selecting certificates for Secure Open User Communication via CPs

Depending on how you configure the S7-1500R/H station with a CP 1543-1, the following certificate rules are valid for communication with connection partners:

- Communication via CP interface with local IP address:
  Use the device certificate of the CP for authentication. For the connection partner to be able to validate the device certificate, the CA certificate of the CP must be available there under "Certificates of the partner devices".
- Communication via the virtual W1 interfaces of the CPUs with configured system IP address:
  Use a device certificate of the CPU for authentication. So that the connection partner can validate the device certificate, the certificate authority of the CPU must be present there under "Certificates of the partner devices".

More information

You can find information on how to create or assign certificates in the Managing certificates (Page 62) section.

You can find information about Secure Open User Communication via a CP interface in the Secure OUC via CP interface (Page 96) section.

16.9 Using an OPC UA server in an S7-1500R/H system

16.9.1 Information worth knowing on the OPC UA server in the S7-1500R/H system

As of firmware version V3.1, S7-1500R/H CPUs support OPC UA server functions. An OPC UA client is not supported.
As of firmware version V4.1, the OPC UA server and the web server of S7-1500R/H CPUs support the management of certificates, trust and revocation lists at runtime via GDS Push. You can find information on certificate management via GDS in the section Certificate management via Global Discovery Server (GDS) (Page 193).

The extensions for the OPC UA server of S7-1500R/H systems comply with the OPC 10000-4 specification: Services (Rel. 1.04), taking into account the restrictions described below.

The OPC UA server is accessible via all the integrated interfaces of the CPUs as well as via a CP 1543-1. To this end, the CP must be connected via the virtual interface W1 of the CPU (area "Access to PLC via communication module" in the CPU properties).

An OPC UA server facilitates open and standardized access to the CPU. In the R/H system, an OPC UA server runs on each of the two CPUs. The OPC UA servers of the primary and backup CPUs synchronize via redundancy mechanisms. In redundant operation, it is 1 server application from the perspective of an OPC UA client.

Compared to standard CPUs, S7-1500R/H CPUs offer an advanced information model. With this advanced information model, it is possible for clients to take into account the specific features of the redundant system.

From the perspective of an OPC UA client, the same mechanisms are used to access the S7-1500R/H system (e.g. Discovery Service) as when accessing standard S7-1500 CPUs.

Restrictions for the OPC UA servers

When the OPC UA server is used in the S7-1500R/H system, there are restrictions as compared to the scope of capabilities of standard S7-1500 CPUs:

- Data access only via server interfaces. The standard SIMATIC server interface is not supported. Therefore, a nodeset export (OPC UA XML file of the standard SIMATIC server interface) is also not supported.
- No support of Alarms & Conditions.
- No access to the address space of a CPU's own OPC UA server via the OPC_UA_ReadList and OPC_UA_WriteList instructions.

  That is, the functions described in the following sections of the TIA Portal information system are not possible:
  - Diagnosing the OPC UA server with OPC_UA_ReadList
  - Set OPC UA-DataValue with OPC_UA_WriteList
- The resolution of the time stamps provided by the server is 1 ms (standard CPU: 1 ns).

An overview of the general restrictions of the S7-1500R/H redundant system compared to the S7-1500 automation system can be found in the section "Application planning > Restrictions" in the S7-1500R/H redundant system System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833).

You can find a description of how to configure an OPC UA server (e.g. creating server interfaces) in the OPC UA communication (Page 165) section or in the information system of the TIA Portal.

Limiting the amount of data for read and write accesses

The limitation of the data volume for write and read accesses applies to all R-CPUs. For H-CPUs as of FW version V4.0, the limitation does not apply.

In order to limit the time variance ("jitter") when accessing large amounts of data, the amount of data for read and write accesses is limited to **32 KB** when the OPC UA server is enabled.

- The write accesses also include the input arguments of method calls.
- The read accesses also include subscriptions and output arguments of method calls.

The limitation affects the OPC UA side, i.e. after S7 data has been encoded for transfer on the line or before it has been mapped to S7 data. It is therefore not just pure "Net data" or payload, but also contains metadata for coding.

The amount of metadata depends on the data types used. With basic data types or elementary data types, the amount of user data is large in relation to the metadata.

Complex data types require more metadata. The limitation on the OPC UA side concerns the OPC UA data type OPC UA variant, see OPC UA variant specification (https://reference.opcfoundation.org/Core/Part6/v105/docs/5.1.9).

Influence on cycle and response times

If you enable the OPC UA server of an S7-1500R/H system, this will affect the cycle and response times.

You must consider the following effects:

- The cycle time for an S7-1500R/H system in the RUN-Redundant system state is extended by activating the OPC UA server.
- The accuracy with which higher-priority alarms interrupt a cycle OB, for example, decreases. Example: The "Jitter" for a cyclic interrupt increases.
- Otherwise, the basic rules from the following document apply: Function Manual "Cycle and Response Times" (https://support.industry.siemens.com/cs/us/en/view/59193558).

⚠ CAUTION

Thorough testing of the maximum cycle time during the commissioning phase
During the commissioning phase, check whether the S7-1500R/H system works reliably with the set maximum cycle time even under worst-case conditions (alarms, communication load from maximum number of clients including connection/disconnection).

Requirements

- TIA Portal V19 with installed Hardware Support Package (HSP) "HSP_V19_0445_001_S71500_RH_3.1".
  The S7-1500R/H CPUs are installed with this HSP.

Redundancy at OPC UA

The redundant system consisting of two or more servers is called a "Redundant Server Set" in OPC UA. Server redundancy in accordance with the OPC UA specification recognizes the following operating modes (Modes of Redundancy):

- Transparent Mode (transparent Redundancy)
  In transparent operating mode, the server is solely responsible for failover in the event of an error (Failover). The OPC UA client does not require any redundancy knowledge to continue the data exchange. To work in Transparent Mode, the client must connect to the system IP address of the CPU interface. If you are using a CP 1543-1, use the virtual interface W1 of the CPU with the configured system IP address.
- Non-transparent Mode (non-transparent Redundancy)
  In non-transparent mode, the client is responsible for switching from one server to the other in the event of an error (Failover). The client must initiate the required actions in order to benefit from the redundant system. To work in non-transparent Mode, the client must connect to the corresponding device IP addresses of the R/H CPUs. If you are using a CP 1543-1, use the virtual interfaces W1 of the CPUs with configured device IP addresses

An S7-1500R/H system supports both operating modes.

The Redundant Server Set provides access to information on availability via the "ServiceLevel" variable; a byte that numerically reflects the "Health status" of a server.

The ServiceLevel allows conclusions to be drawn about the redundancy status, e.g. whether the CPU is the primary or backup CPU or whether the system is in the RUN-Redundant system state. You can find information on the ServiceLevel in the section on non-transparent mode (Page 463).

More information

You can find additional and up-to-date information on using the OPC UA server with S7-1500R/H systems in the following entry: FAQ How do you use the OPC UA server in an S7-1500 R/H system? (https://support.industry.siemens.com/cs/ww/en/view/109822965)

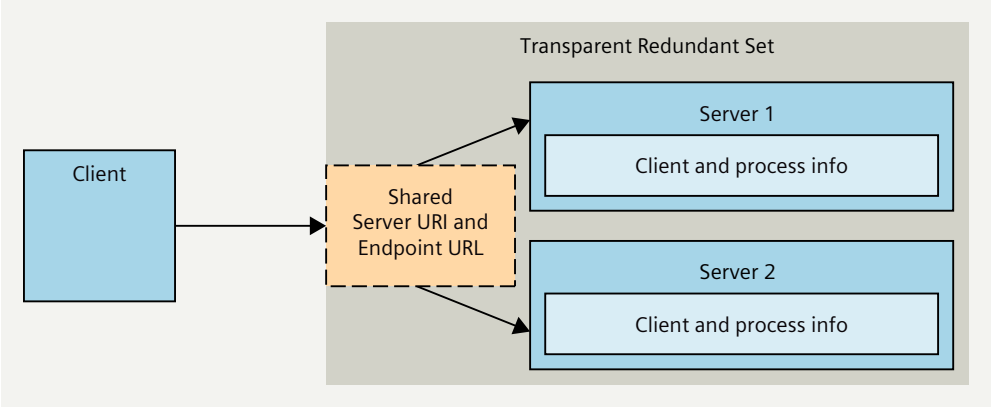
16.9.2 Transparent Mode (transparent Redundancy)

Details on transparent redundancy are explained below - an operating mode that allows a client to deal with the redundant system as with a single system or with an OPC UA server of a standard CPU.

Primary CPU always accessible via system IP address

For an S7-1500R/H station, use the system IP address for transparent redundancy. With the system IP address, a client accesses the primary CPU, i.e. the CPU that is currently hosting this IP address.

The following figure shows an example of the use of the transparent redundancy according to OPC UA 10000-4.



Response upon loss of primary CPU (RUN-Redundant > RUN-Solo)

In the event of an error (failover), communication between the client and server is briefly interrupted. All established sessions and subscriptions are retained and can be resumed - with the new primary CPU. In this case, the behavior from the client's point of view corresponds to the behavior in the event of temporary communication errors in which the session is also resumed.

As soon as the new primary CPU can be accessed after the failover via the system IP address, the client can resume communication (reactivate session).

Behavior when restoring redundancy (SYNCUP > RUN-Redundant)

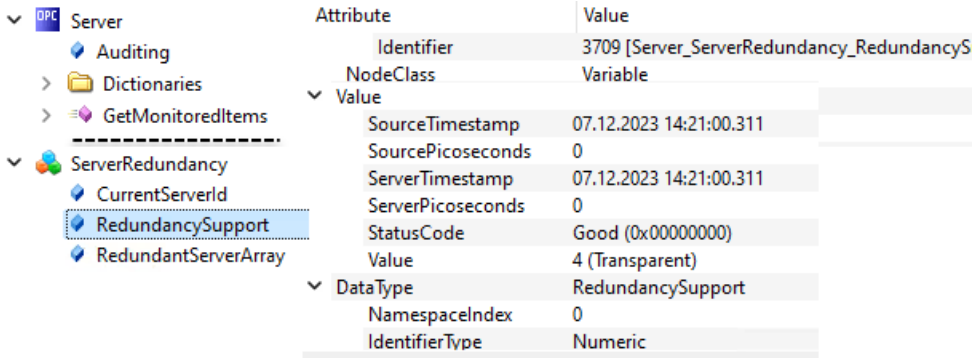
If the initial state of the redundant system is restored after a failover, e.g. after replacing the faulty CPU, the system performs a SYNCUP.

During SYNCUP, the OPC UA servers are restarted in both CPUs. All existing sessions and subscriptions are deleted.

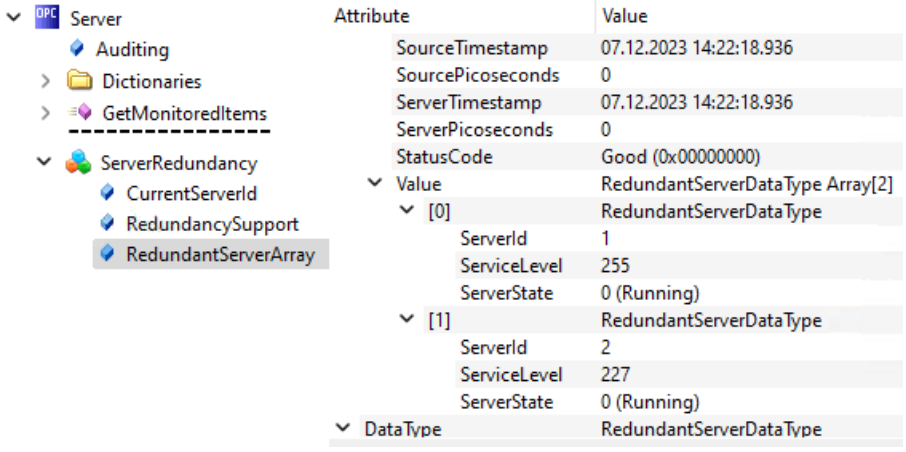
As soon as the server of the primary CPU is accessible again, the client must recreate the sessions and subscriptions.

Relevant nodes in the information model for transparent redundancy

Information in the information model on transparent mode of the R/H station can be found under the "ServerRedundancy" object (namespace index "0" or namespace "http://opcfoundation.org/UA/").



You can determine the ServerState and ServiceLevel of the redundant servers using the RedundantServerArray:



You can find more information on the ServiceLevel in the next section.

16.9.3 Non-transparent Mode (non-transparent Redundancy)

In the following, details on non-transparent redundancy are explained. In this operating mode, OPC UA provides the following information for a client:

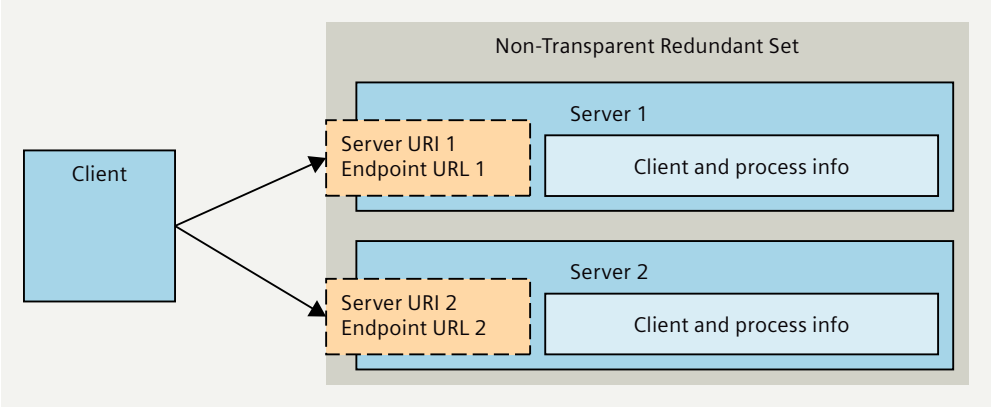
- Which servers are available in the Redundant Server Set
- Which types of failover between the available servers are supported

This information allows the client to determine what it needs to do to achieve switchover. The client must not only be able to interpret the ServerRedundancy attribute, but also know the extended information model of the redundant server.

Address parameters of the redundant OPC UA server in an R/H system

In contrast to transparent redundancy, the servers in the R/H system are addressed via their unique IP address (device IP address or virtual IP address in the case of a configured CP 1543-1).

The following figure shows an example of the use of the non-transparent redundancy according to OPC UA 10000-4.



Response upon loss of primary CPU: Failover modes

According to OPC 1000-4: Services, servers can support different failover modes: Cold, Warm, Hot and HotAndMirrored.

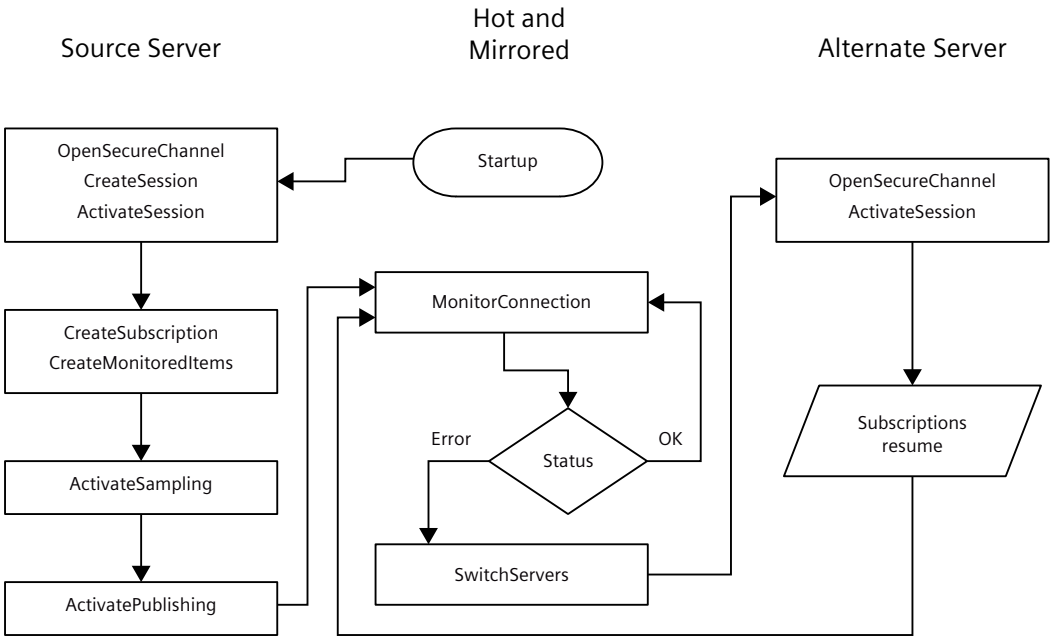
The OPC UA server of an S7-1500R/H CPU supports "HotAndMirrored" failover mode.

The client must know that the OPC UA server is a redundant server and must perform the failover process in a certain way due to the supported Failover modes.

The way in which the failover process should take place is described in the OPC 10000-4 specification: Services, section "Client failover behavior - HotAndMirrored". The client is responsible for tracking the status of the server, i.e. periodically querying the ServiceLevel and switching to the alternative server (in the case of an S7-1500R/H system, this means the backup CPU) in the event of an error. This type of redundancy control offers the following advantages:

- The client has full control in the selection of the alternative server.
- The client can access the OPC UA server via separate networks.

The following figure from the specification OPC 10000-4: Services shows the steps that the client goes through when it receives the signal to switch to the "Alternate server" due to a low ServiceLevel value for the "Source server".



ServiceLevel

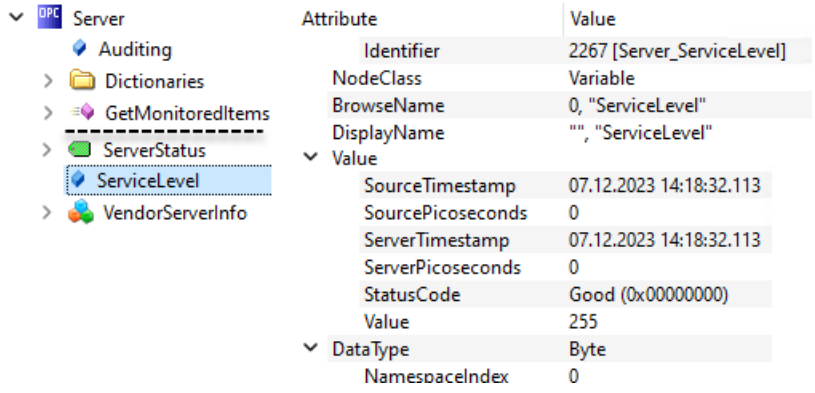
ServiceLevel is a variable that is modeled as a property of the ServerType object in the address space of the server. You use the ServiceLevel to find out whether the addressed server is still supplying data, for example. The ServiceLevel is a numerical value for the "Health status" of the server and thus provides the client with a trigger for switching the server.

The structure of the ServerType object is described in the OPC 10000-5: Information Model specification, section "ServerType".

For S7-1500R/H, the following ServiceLevel values apply to the respective OPC UA server:

- **RUN-Redundant**: ServiceLevel primary CPU = 255 (CPU in RUN), service level backup CPU = 227 (CPU in RUN).
- **CPU in STOP**: ServiceLevel of the failed CPU (RUN STOP transition) = 1 (NoData). This is the trigger for the client for the failover.

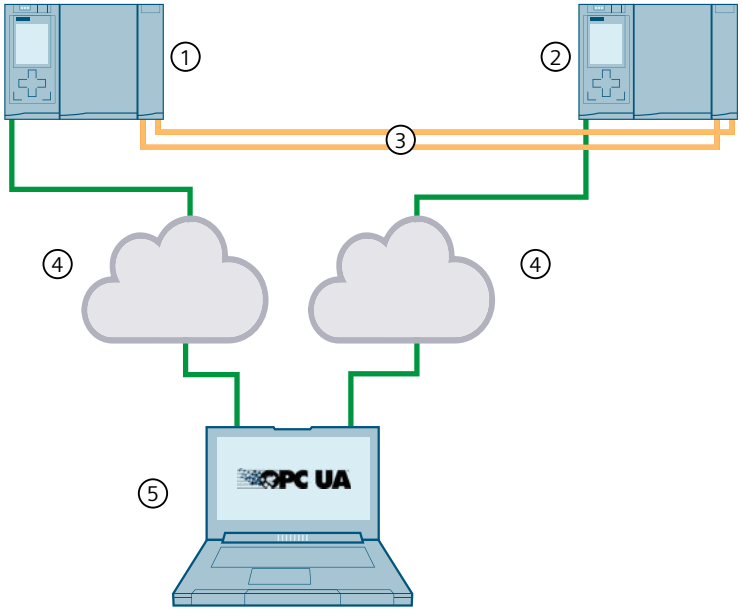
Example for a primary CPU in RUN:



Application of non-transparent redundancy

If a client accesses the OPC UA server via different, i.e. independent subnets, transparent redundancy using the system IP address is not possible.

The following figure shows a configuration with an H system that is connected to a client via two subnets.

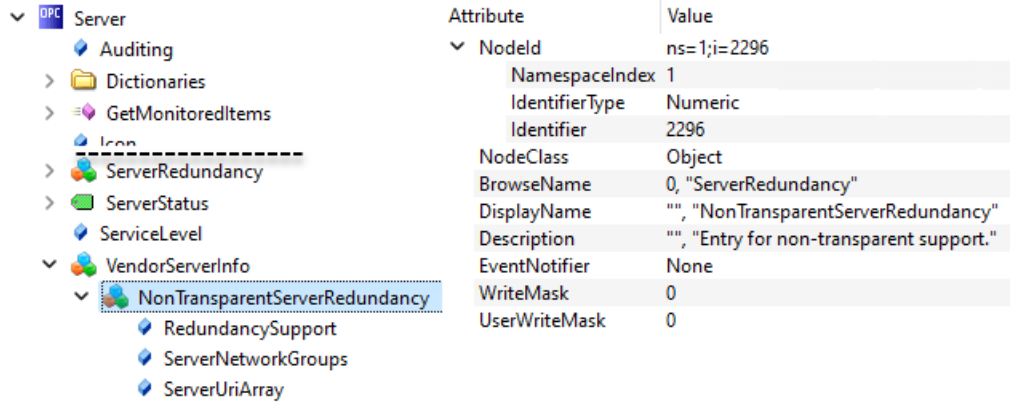


The client can connect to the H system via the two independent networks. The two H CPUs are not connected via one of the networks. In this way, the failure of a network can be tolerated.

Independent subnets are not a requirement for non-transparent mode. You can also use non-transparent mode for configurations with a subnet.

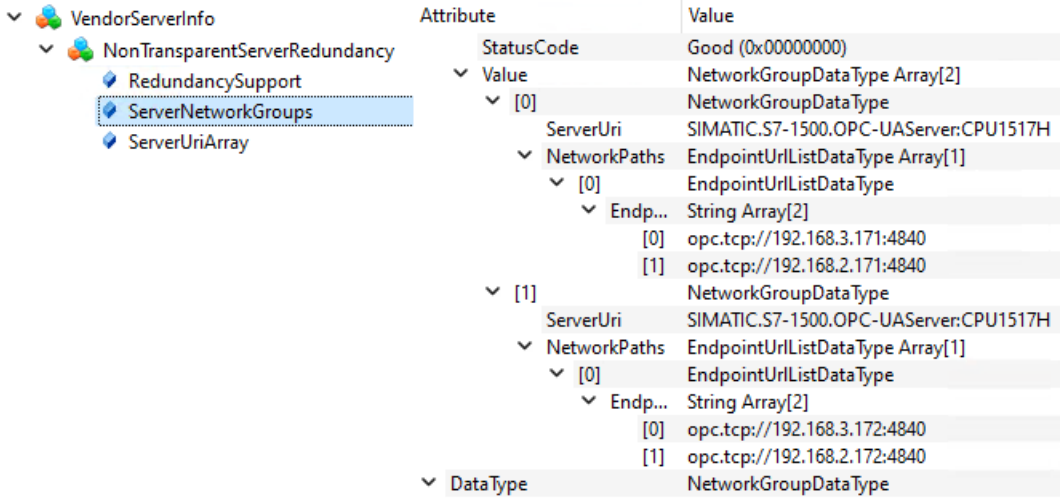
Relevant nodes in the information model for non-transparent redundancy

The information in the information model of the R/H station that is relevant for non-transparent mode is located under the "VendorServerInfo" object, a placeholder object for vendor-specific information about the OPC UA server. This vendor-specific node and the nodes below it are located in the namespace for the local server,
e.g. urn: SIMATIC.S7-1500.OPC-UA.Application:PLC_1 with namespace index 1.



In the ServerRedundancy object below, a client can find all the required information to connect to the R/H system.

The ServerUriArray-Property allows a client to select a suitable server. The information on which network paths can be used to access the servers can be found via the object type NonTranparentNetworkRedundancyType - a subtype of NonTransparentRedundancyType. The object type NonTranparentNetworkRedundancyType references the ServerNetworkGroups variable, which contains an array of servers (EndpointUrlList) together with information on which redundant network paths exist for each server (NetworkPaths).



You can find a detailed description of the relevant nodes with their references below the VendorServerInfo node in the OPC UA specification (OPC 10000-5: Information Model).

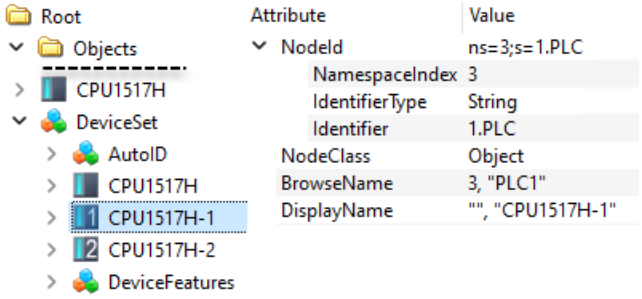
For an S7-1500R/H system, the EndpointUrlList contains an entry for each device IP address or virtual device IP address (if configured together with a CP 1543-1) via which the servers of the S7-1500R/H system can be accessed. In the event of a failure, the client can decide whether to connect to the same server via a different path or whether to choose the redundant server.

16.9.4 Information model in detail

The following sections show the structure of the information model of an S7-1500R/H system in detail. The information model is suitable for both clients that access the R/H system like a standard CPU and clients that want to have full control over the R/H system.

Advanced information model for redundant systems

The following figure shows by way of example how the R/H system is modeled in the DeviceSet node as a separate object next to the individual R/H CPUs.



R/H system as a separate node in the information model

Under the DeviceSet node, in addition to the nodes for each R/H CPU, there is also a node as a representative for the R/H system.

The OPC UA server is temporarily not available in the SYNCUP system state (RUN-Syncup mode for primary CPU). The server restarts in this state.

The nodes represent the following information:

Node <configured name>	Contents	Accessible data in the RUN-Redundant system state	Accessible data in the RUN-Solo system state
<R/H system>	Information regarding the R/H system	Server interface data (identical for both CPUs) CPU-specific information of the primary CPU	Client is connected with: • Primary CPU: Data of the server interface of the primary CPU. • Backup CPU: Server interface data (if ServiceLevel = NoData: server interface data is invalid or not available).
<PLC 1>	Information via R/H CPU with redundancy ID 1	Server interface data (identical for both CPUs) CPU-specific information of the CPU with redundancy ID 1	Client is connected with: • PLC 1 (= primary CPU): Data of the server interface of the primary CPU. • PLC 1 (= backup CPU): Server interface data (ServiceLevel = NoData signifies the data is invalid or not available). • PLC 2 (= backup CPU): No data (access error BadInvalidState / (BadResourceUnavailable))

Node <configured name>	Contents	Accessible data in the RUN-Redundant system state	Accessible data in the RUN-Solo system state
<PLC 2>	Information via R/H CPU with redundancy ID 2	Server interface data (identical for both CPUs) CPU-specific information of the CPU with redundancy ID 2	Client is connected with: • PLC 2 (= primary CPU): Data of the server interface of the primary CPU. • PLC 2 (= backup CPU): Server interface data (ServiceLevel = NoData signifies the data is invalid or not available). • PLC 1 (= backup CPU): No data (access error BadInvalidState / (BadResourceUnavailable))

Nodes below the device nodes

Device nodes are the nodes below the DeviceSet node (R/H system, PLC 1, PLC 2).

The "OperatingMode" and "RedundancyMode" attributes are of particular interest.

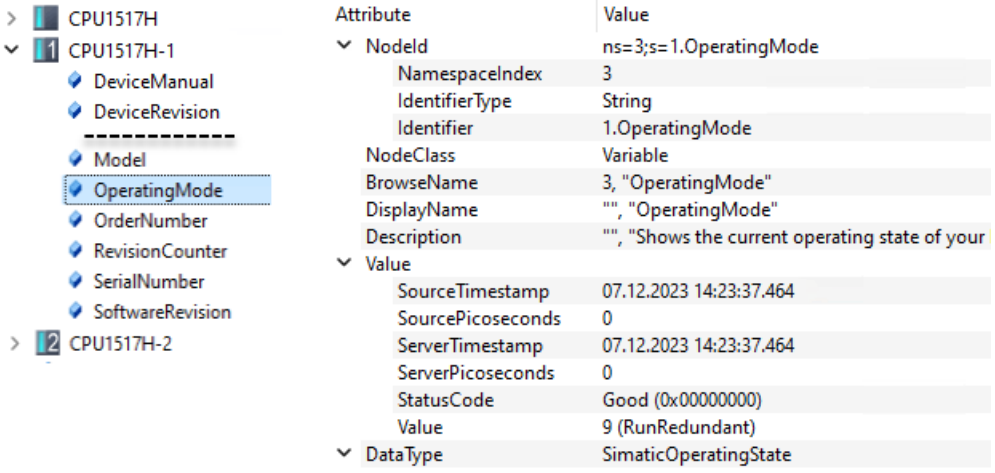
Operating mode

The OperatingMode-Property below the R/H system node shows the operating mode of the primary CPU for the R/H system node.

The following values are defined for the individual CPUs of the R/H system and for the R/H system:

OperatingMode	R/H system	R/H CPU
1 (STOP - FW update)	x	x
3 (STOP - Initialization)	x	x
4 (STOP)	x	x
6 (Startup)	x	x
8 (RUN)	x	x
9 (RUN-Redundant)	x	x
10 (HOLD)	x	x
13 (Defective)	x	x
14 (Troubleshooting)	x	x
15 (No power)	x	x
17 (STOP - no de-energized/substitute value switch for outputs)	x	x
18 (RUN - de-energized/substitute value switch for outputs)	x	x
19 (Program test)	x	x
20 (Run program test)	8 (RUN)	x (primary; backup in test mode)
21 (RUN Syncup)	8 (RUN)	x
22 (Syncup)	8 (RUN)	x
31 (Remote unknown)	x	-

Example with node attributes for OperatingMode:

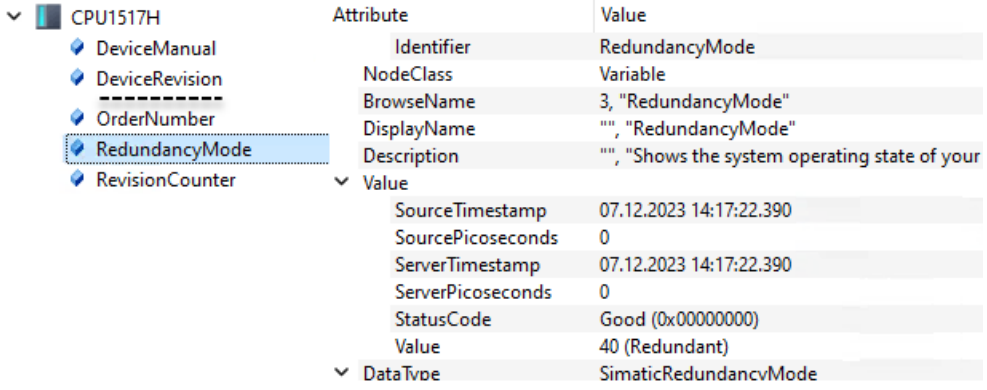


RedundancyMode

The RedundancyMode-Property shows the system status of the R/H system and is only available in the R/H system node.

RedundancyMode	R/H system	R/H CPU
32 (No power)	x	-
33 (STOP)	x	-
34 (HOLD)	x	-
35 (Startup)	x	-
37 (RUN-Solo)	x	-
38 (Syncup)	x	-
39 (Program test)	x	-
40 (Redundant)	x	-

Example with node attributes for RedundancyMode:



16.9.5 Updated instructions for server methods

To implement server methods in an S7-1500 CPU, use the "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost" instructions. Details of the new version V1.1 of these two instructions are explained below.

- For S7-1500R/H CPUs as of FW version V3.1, version V1.1 of the server instructions is mandatory - the use of version V1.0 is not permitted.
- The recommendation applies to S7-1500 standard CPUs: For new projects starting from TIA Portal V19 and CPU firmware version V3.1, always use the new server instruction version V1.1 or higher.
- Within a project, you can use both the instructions with version V1.0 and the instructions with version V1.1. You can only use one version within a CPU user program.

To implement server methods in the user program, use the example program published here and not the example from the TIA Portal help system.

Implementing server methods in the user program

First, here is a brief summary of the procedure for providing an OPC UA method to the OPC UA server of an S7-1500 CPU via the user program. This method can then be called by any OPC UA client.

- A function block (FB) represents the server method in the user program.
- This FB must be called cyclically (e.g. by OB 1).
- In the FB, the "OPC_UA_ServerMethodPre" instruction must first be called in order to map the input parameters of the method that the client has given to the call to the corresponding CPU variables (input data transfer).
- After the "OPC_UA_ServerMethodPre" instruction has been called, the programmed algorithm (the method itself with processing of the input parameters and preparation of the output parameters) is processed.
- Once the programmed algorithm has been run and the output parameters have been calculated, the "OPC_UA_ServerMethodPost" instruction must be called. The "OPC_UA_ServerMethodPost" instruction ensures that the valid output data of the method is made available to the client.
- Observe the naming conventions when creating the OPC UA methods:
  - When calling the server methods, the function must be created as a multi-instance; the name of the multi-instance must be "OPC_UA_ServerMethodPre_Instance"/"OPC_UA_ServerMethodPost_Instance" so that the method is created in the address space.
  - When defining input parameters for the OPC UA method in the static area of the block, the name of the variable must be "UAMethod_InParameters" so that the input parameters of the method are displayed.
  - When defining the output parameters of the OPC UA method in the static area of the block, the name of the variable must be "UAMethod_OutParameters" so that the output parameters of the method are displayed.

Sequence of the user program

The two "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost" instructions are asynchronous instructions that do not have a "REQ input" that triggers the start of the respective instruction.

The "OPC_UA_ServerMethodPre" instruction is triggered implicitly by the OPC UA client calling the OPC UA method (edge trigger). This means that, whenever the method has not been called by the client in a cycle and is called in the following cycle, the following happens:

- The STATUS changes from 0x7000 (no call) to 0x7001 (first call). The BUSY output parameter is set to "1".
- If the data transfer takes longer than one cycle, the status changes to 0x7002 (intermediate call) after the first cycle.
- When the input data transfer is complete:
  - DONE changes to "1".
  - UAMethodCalled changes to "1".
  - BUSY is reset to "0".
- "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost":
  - When the output data transfer is completed for the OPC_UA_ServerMethodPost instruction, DONE changes to "1".
    This is the condition for resetting the input parameters "UAMethod_Finished" and "UMethod_Result" (see example program).
  - After a further cycle, all output parameters are reset (corresponds to a falling edge for REQ-triggered instructions).
  - The respective instances of the instructions are then released again (max. 20 instances can be active at the same time).

Compatibility between version V1.0 and V1.1 of the instructions

There are the following differences between version V1.0 and V1.1 with regard to the server instructions:

- Resetting the output parameter "UAMethod_Called" of the server instruction "OPC_UA_ServerMethodPre":
  - V1.0: "UAMethod_Called" is automatically reset if both "DONE" of the "OPC_UA_ServerMethodPre" instruction and "DONE" of the "OPC_UA_ServerMethodPost" instruction are reset. "UAMethod_Called" is therefore only reset when "OPC_UA_ServerMethodPost" is completed.
  - V1.1: "UAMethod_Called" is automatically reset when output parameter "DONE" of the "OPC_UA_ServerMethodPre" instruction is reset.
- Release of the instances of "OPC_UA_ServerMethodPre" and "OPC_UA_ServerMethodPost":
  - V1.0: No cyclic call of the server instructions required.
  - V1.1: Mandatory cyclical call of the server instructions required.

NOTE

When switching to the OPC UA server methods from version V1.0 to version V1.1, check whether your user program takes into account the described rules and the adapted functionality. Adjust the program if necessary.

Example program

```
FUNCTION_BLOCK "mySERVER_METHOD"
{ S7_Optimized_Access := 'TRUE' }
VERSION : 0.1
 VAR DB_SPECIFIC
 UAMethod_InParameters : Struct
 IN_BOOL : Bool;
 IN_INT : Int;
 END_STRUCT;
 UAMethod_OutParameters : Struct
 OUT_BOOL : Bool;
 OUT_INT : Int;
 END_STRUCT;
 END_VAR
 VAR
OPC_UA_ServerMethodPre_Instance {InstructionName :=
'OPC_UA_ServerMethodPre'; LibVersion := '1.1'} :
OPC_UA_ServerMethodPre;
 DONE_PRE { S7_SetPoint := 'True'} : Bool;
 BUSY_PRE : Bool;
 ERROR_PRE : Bool;
 STATUS_PRE : DWord;
 UAMethod_Called : Bool;
 OPC_UA_ServerMethodPost_Instance {InstructionName :=
'OPC_UA_ServerMethodPost'; LibVersion := '1.1'} :
OPC_UA_ServerMethodPost;
 UAMethod_Result { S7_SetPoint := 'True'} : DWord;
 UAMethod_Finished : Bool;
 DONE_POST { S7_SetPoint := 'True'} : Bool;
 BUSY_POST : Bool;
 ERROR_POST : Bool;
 STATUS_POST : DWord;
 END_VAR
BEGIN
 #OPC_UA_ServerMethodPre_Instance(Done => #DONE_PRE,
 Busy => #BUSY_PRE,
 Error => #ERROR_PRE,
 Status => #STATUS_PRE,
 UAMethod_Called => #UAMethod_Called,
 UAMethod_InParameters := #UAMethod_InParameters);

//Method is called
IF #UAMethod_Called AND NOT #ERROR_PRE THEN

(* Functionality:
InParameters are valid
and copied to OutParameters *)

#UAMethod_OutParameters.OUT_BOOL := #UAMethod_InParameters.IN_BOOL;

#UAMethod_OutParameters.OUT_INT := #UAMethod_InParameters.IN_INT;


(* If Method is finished without errors
prepare output parameters of OPC_UA_ServerMethodPost accordingly *)

#UAMethod_Result := 0;
 #UAMethod_Finished := TRUE;
 END_IF;



#OPC_UA_ServerMethodPost_Instance(UAMethod_Result :=
```

```
#UAMethod_Result,
 UAMethod_Finished := #UAMethod_Finished,
 Done => #DONE_POST,
 Busy => #BUSY_POST,
 Error => #ERROR_POST,
 Status => #STATUS_POST,
 UAMethod_OutParameters := #UAMethod_OutParameters);

//Reset Input Parameters after OPC_UA_ServerMethodPost is done
IF #DONE_POST OR #ERROR_POST THEN

#UAMethod_Finished := FALSE;
 #UAMethod_Result := 0;

END_IF;



END_FUNCTION_BLOCK
```

Industrial Ethernet Security with CP 1543-1 17

All-round protection - the task of Industrial Ethernet Security

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. Data transfer can also be protected by a combination of different security measures:

- Data espionage
- Data manipulation
- Unauthorized access

Security measures

- Firewall
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)
  - Bandwidth limitation
  - Global firewall rules

  All network nodes located in the internal network segment of a CP 1543-1 are protected by its firewall. Exception: If you access the CPU via the interface of the CP with the "Access to PLC via communication module" function, the firewall does not protect this connection.
- Logging

  To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a Syslog server.
- HTTPS

  For encrypted transfer of websites, for example during process control.
- FTPS (explicit mode)

  For encrypted transfer of files.
- Secure NTP

  For secure time-of-day synchronization and transmission.
- SNMPv3

  For secure transmission of network analysis information safe from eavesdropping.
- VPN groups
  You can combine the CP 1543-1 with other security modules into VPN groups through configuration. IPsec tunnels are established between all the security modules of a VPN group (VPN). All internal nodes of these security modules can communicate securely with each other through this tunnel.
- Protection for devices and network segments

  The firewall and VPN groups protective functions can be applied to the operation of single devices, multiple devices, or entire network segments.

Additional information

An overview with links to the most important contributions on Industrial Security is available in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/92651441).

17.1 Firewall

Tasks of the firewall

The purpose of the firewall functionality is to protect networks and stations from outside influences and disturbances. This means that only certain previously specified communications relations are permitted.

To filter the data traffic, IPv4 addresses, IPv4 subnets, port numbers or MAC addresses among other things can be used.

The firewall functionality can be configured for the following protocol levels:

- IP firewall with stateful packet inspection (layer 3 and 4)
- Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)

Firewall rules

Firewall rules describe which packets are permitted or forbidden in which direction.

17.2 Logging

Functionality

For test and monitoring purposes, the security module has diagnostics and logging functions.

- Diagnostics functions
  These include various system and status functions that you can use in online mode.
- Logging functions
  This involves the recording of system and security events. Depending on the event type, the recording is made in volatile or non-volatile local buffer areas of the CP 1543-1. As an alternative, it is also possible to record on a network server.
  The parameter assignment and evaluation of these functions is only possible with a network connection.

Recording events with logging functions

You specify which events should be recorded with the log settings. Here you can configure the following recording variants:

- Local logging
  With this variant, you record the events in local buffers of the CP 1543-1. In the online dialog of the Security Configuration Tool, you can then access these recordings, visualize them and archive them on the service station.
- Network Syslog
  With the network Syslog, you use a Syslog server in the network. This records the events according to the configuration in the log settings.

17.3 NTP client

Functionality

To check the time validity of a certificate and the time stamp of log entries, the date and time are maintained on the CP 1543-1 as on the CPU. This time can be synchronized with NTP. The CP 1543-1 forwards the synchronized time to the CPU via the backplane bus of the automation system. This way the CPU also receives a synchronized time for the time events in program execution.

The automatic setting and periodic synchronization of the time takes place either via a secure or non-secure NTP server. You can assign a maximum of 4 NTP servers to the CP 1543-1. A mixed configuration of non-secure and secure NTP servers is not possible.

17.4 SNMP

Functionality

Like the CPU, the CP 1543-1 supports the transfer of management information using the Simple Network Management Protocol (SNMP). To achieve this, an "SNMP agent" is installed on the CP/CPU that receives and responds to the SNMP queries. Information about the properties of devices capable of SNMP is contained in so-called MIB files (Management Information Base) for which the user needs to have the appropriate rights.

With SNMPv1, the "community string" is also sent. The "community string" is like a password that is sent along with the SNMP query. The requested information is sent when the "community string" is correct. The request is discarded when the string is incorrect.

With SNMPv3, data can be transferred encrypted. To do this, select either an authentication method (e.g. SHA) or an authentication and encryption method (e.g AES).

You can activate and deactivate the use of SNMP for the CP/CPU. Deactivate SNMP if the security guidelines in your network do not permit SNMP or if you use your own SNMP solution.

To find out how to activate and deactivate SNMP for the CPU, refer to section SNMP (Page 117).

17.5 VPN

Functionality

For security modules that protect the internal network, VPN (Virtual Private Network) tunnels provide a secure data connection through the non-secure external network.

The module uses the IPsec protocol (tunnel mode of IPsec) for tunneling.

In STEP 7 you can assign VPN groups to security modules. VPN tunnels are automatically established between all modules of a VPN group. A module in one project can belong to several different VPN groups at the same time in the process.

SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200BL, ET 200AL, ET 200pro, ET 200eco PN, ET 200clean PROFINET with STEP 7

Function Manual

Introduction 1

Safety instructions 2

Industrial cybersecurity 3

Description 4

Parameter assignment/addressing 5

Diagnostics and maintenance 6

Functions 7

PROFINET with the redundant S7-1500R/H system 8

11/2025
A5E03444486-AQ

Table of contents

1 Introduction 7

1.1 SiePortal 12

1.2 Function manuals documentation guide 13
1.2.1 Information classes Function Manuals 13
1.2.2 Basic tools 15
1.2.3 S7 Port Configuration Tool (S7-PCT) 17
1.2.4 S7 Failsafe Configuration Tool (S7-FCT) 17
1.2.5 MultiFieldbus Configuration Tool (MFCT) 17
1.2.6 SIMATIC Technical Documentation 18

2 Safety instructions 21

2.1 General security information 21

3 Industrial cybersecurity 22

3.1 Introduction to industrial cybersecurity 22

3.2 Cybersecurity information 22

3.3 Cybersecurity-related information in this manual 23

4 Description 24

4.1 Introduction to PROFINET 24
4.1.1 PROFINET terms 26
4.1.2 Basic terminology of communication 29
4.1.3 PROFINET interface 32
4.1.4 Implementation of the PROFINET device model in SIMATIC 35

4.2 PROFINET Security Class 1 36

4.3 Setting up PROFINET 39
4.3.1 Active Network Components 40
4.3.2 Cabling technology 42
4.3.3 Wireless design 44
4.3.3.1 Basics 44
4.3.3.2 Tips on assembly 46
4.3.4 Network security 47
4.3.4.1 Basics 47
4.3.4.2 Network components and software 49
4.3.4.3 Application example 50

5 Parameter assignment/addressing 52

5.1 Assigning an IO device to an IO controller 53

5.2 Device name and IP address 54
5.2.1 Device name 55
5.2.2 IP address 57
5.2.3 Assigning a device name and IP address 60
5.2.4 Assign device name via communication table 65
5.2.5 Permitting changes to the device name and IP address directly on the device 68

5.3 Configuring an IO device through hardware detection 70

5.4 Specifying the router for a PROFINET IO device 71

5.5 Configuring topology 74
5.5.1 Topology view in STEP 7 77
5.5.2 Interconnecting ports in the topology view 79
5.5.3 Interconnecting ports - Inspector window 80
5.5.4 Automatic assignment of devices by offline/online comparison 81
5.5.5 Apply the port interconnections identified online manually to the project 82
5.5.6 Include the devices identified online manually in the project 83
5.5.7 Automatic assignment of devices by advanced offline/online comparison 83

6 Diagnostics and maintenance 84

6.1 Diagnostics mechanisms of PROFINET IO 84
6.1.1 Diagnostics levels in PROFINET IO 85

6.2 Diagnostics via the display of the S7-1500 CPUs 88

6.3 Diagnostics via Web server 91

6.4 Online diagnostics with STEP 7 94

6.5 Extended maintenance concept 96

6.6 Diagnostics of the network topology 99

6.7 Diagnostics in the user program 100
6.7.1 Diagnostics and configuration data records 100
6.7.2 Evaluate diagnostics in the user program 102

6.8 Maintenance 104
6.8.1 I&M data (identification and maintenance) 104
6.8.2 Loading I&M data to PROFINET IO devices and your modules 104
6.8.3 Asset management 105
6.8.3.1 Further information about asset management at PROFINET 105
6.8.3.2 Content and structure of an asset management record 107
6.8.3.3 Asset management data record for I-devices 112

7 Functions 117

7.1 Connecting other bus systems 117
7.1.1 Linking PROFINET and PROFIBUS 118
7.1.2 Connect the DP slave via the IE/PB Link to a PROFINET IO system 119

7.2 Intelligent IO devices (I-devices) 121
7.2.1 I-device functionality 121
7.2.2 Properties and Advantages of the I-Device 122
7.2.3 Characteristics of an I-Device 123

7.2.4 Data Exchange between higher- and lower-level IO system 127
7.2.5 Configuring the I-device 129
7.2.6 Program examples 132
7.2.7 Diagnostics and interrupt characteristics 135
7.2.8 Rules for the Topology of a PROFINET IO System with I-Device 137
7.2.9 Boundary conditions when using I-devices 140
7.2.10 Configuring PROFIenergy with I-devices 141
7.2.11 Enabling/disabling I-device in the user program of the I-device CPU 142

7.3 Shared device 148
7.3.1 Useful information on shared devices 148
7.3.2 Shared device and assigned IO controllers in the common project 150
7.3.3 Configuring a shared device in a common project 152
7.3.4 Shared device and assigned IO controllers in different projects 155
7.3.5 Configuring a shared device for different projects 158
7.3.6 Shared I-device and assigned IO controllers in the common project 162
7.3.7 Configuring a shared I-device in the common project 163
7.3.8 Configuring a shared I-device in different projects 167
7.3.9 Module-internal shared input/shared output (MSI/MSO) 175

7.4 Media redundancy (ring topologies) 181
7.4.1 Media Redundancy Protocol (MRP) 182
7.4.2 Configuring media redundancy 185
7.4.3 Media redundancy with planned duplication of frames (MRPD; not for S7-1500R/H) 187
7.4.4 Multiple rings 189
7.4.5 MRP interconnection 194

7.5 Real-time communication 197
7.5.1 Introduction 197
7.5.2 RT 198
7.5.3 IRT 199
7.5.4 Comparison of RT and IRT 201
7.5.5 Configuring PROFINET IO with IRT 202
7.5.6 Setting the bandwidth usage for the send clock 205
7.5.7 Setup recommendations for optimizing PROFINET 207
7.5.8 Limitation of the data infeed into the network 210

7.6 PROFINET with performance upgrade 211
7.6.1 Dynamic frame packing 212
7.6.2 Fragmentation 215
7.6.3 Fast forwarding 216
7.6.4 Configuration of IRT with high performance 217
7.6.5 Sample configuration for IRT with high performance 220

7.7 Isochronous mode 220
7.7.1 What is isochronous mode? 220
7.7.2 Use of isochronous mode 222
7.7.3 Time sequence of synchronization on PROFINET IO 223
7.7.4 Configuring isochronous mode 224
7.7.4.1 Introduction 224
7.7.4.2 Configuring isochronous mode on PROFINET IO 225
7.7.4.3 Setting the application cycle and delay time 227
7.7.5 Programming isochronous mode 228
7.7.5.1 Basics of Programming 228

7.7.5.2 Program execution according to the IPO model ... 229
7.7.5.3 Program execution according to the OIP model ... 230
7.7.6 Operating multiple PROFINET networks in isochronous mode ... 232
7.7.6.1 Useful information on the operation of several PROFINET networks in isochronous mode ... 232
7.7.6.2 Configuring the synchronization of the send clocks of PROFINET interfaces ... 233
7.7.6.3 Operating several CPUs in isochronous mode ... 235
7.7.6.4 Programming manual synchronization ... 237
7.7.7 Operating multiple projects isochronously ... 240
7.7.7.1 Cross-project clock synchronization with an I-device ... 241

7.8 Direct data exchange ... 247
7.8.1 Introduction ... 247
7.8.2 Configuring direct data exchange between two S7-1500 CPUs ... 250
7.8.3 Configuring direct data exchange between multiple IO controllers ... 253

7.9 Device replacement without exchangeable medium ... 257
7.9.1 Device replacement without exchangeable medium/PG function ... 258
7.9.2 Replacing an IO device without exchangeable medium ... 259
7.9.3 Permit overwriting of PROFINET device name ... 260

7.10 Standard machine projects ... 264
7.10.1 Multiple use IO systems ... 265
7.10.1.1 What you should know about multiple use IO systems ... 265
7.10.1.2 Configuring multiple use IO systems ... 268
7.10.1.3 Adapt multiple use IO systems locally ... 271
7.10.2 Configuration control for IO systems ... 273
7.10.2.1 Information about configuration control of IO systems ... 273
7.10.2.2 Configuring IO devices as optional ... 275
7.10.2.3 Enabling optional IO devices in the program ... 276
7.10.2.4 Configuring flexible order of IO devices ... 282
7.10.2.5 Customizing arrangement of IO devices in the program ... 284
7.10.2.6 System behavior and rules ... 287

7.11 Saving energy with PROFIenergy ... 288

7.12 Docking systems ... 291
7.12.1 Configuring docking systems ... 293

7.13 Accelerating startup ... 296
7.13.1 Options for accelerating the startup of IO devices ... 296
7.13.2 Prioritized startup ... 297
7.13.3 Configuring prioritized startup ... 298
7.13.4 Optimize the port settings ... 299
7.13.5 Optimize the cabling of the ports ... 300
7.13.6 Measures in the user program ... 301

7.14 Dealing with timeouts while exchanging data ... 302
7.14.1 Terminating communication relation during faults ... 302
7.14.2 Enabling maintenance of the communication relation in the CPU properties ... 303
7.14.3 Enabling maintenance of the communication relation by data record transfer ... 305
7.14.4 Example: Transfer data record for behavior change via FB ... 306

7.15 PROFINET Security ... 310

7.15.1 Configuring the SNMP 310
7.15.2 Configuring DCP 316

8 PROFINET with the redundant S7-1500R/H system 319

8.1 Media redundancy in the redundant S7-1500R/H system 320
8.2 H-Sync Forwarding 320
8.3 System redundancy S2 322
8.4 System redundancy R1 323
8.5 Switched S1 device 325
8.6 Main differences between IO device with system redundancy S2, R1 and standard IO device 328
8.7 Installation guidelines 329
8.8 Configuring PROFINET IO on a redundant S7-1500R/H system 330
8.9 Assigning IO device to the redundant S7-1500R/H system 337
8.10 Configuring media redundancy (MRP) for a configuration with the redundant S7-1500R/H system 339
8.11 MRP interconnection with the redundant system S7-1500R/H 342

Introduction

1

Purpose of the documentation

This Function Manual provides an overview of the PROFINET communications system together with SIMATIC STEP 7.

STEP 7 is integrated into the high-performance, graphical Totally Integrated Automation Portal (TIA Portal), the integration platform for all automation software tools.

This Function Manual supports you in planning a PROFINET system. The manual is structured into the following subject areas:

- PROFINET basics
- PROFINET diagnostics
- PROFINET functions

Basic knowledge required

The following knowledge is required in order to understand the manual:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge about the use of Windows-based computers
- Knowledge about how to use STEP 7 (TIA Portal)

Scope

This documentation is the basic documentation for all SIMATIC products from the PROFINET environment. The product documentation is based on this documentation.

The examples are based on the functionality of the S7-1500 automation system.

What's new in the PROFINET Function Manual, Edition 11/2025 compared to Edition 11/2024?

Function	What are the customer benefits?	Where can I find this information?
Confirming authenticity of PROFINET GSD files with distributor ID	As of STEP 7 V21, you can add your distributor ID to an I-device. This allows you to digitally sign the exported GSD file in a GSDX file and thus confirm the authenticity of the GSD file. For the I-device, use the PROFINET interface of an S7-1500 CPU as of FW version V4.1 in order to be able to add a distributor ID.	Section PROFINET Security Class 1 (Page 36)
Operating multiple projects isochronously	You can implement IRT clock synchronization in multiple projects with a S7-1500 CPU as of FW version V4.1. The CPU must support the "PROFINET with IRT" functionality on several PROFINET interfaces.	Section Operating multiple projects isochronously (Page 240)

What's new in the PROFINET Function Manual, Edition 11/2024 compared to Edition 11/2023

Function	What are the customer benefits?	Where can I find this information?
Implementation of PROFINET Security Class 1	You read which configuration options for protocols and processes in STEP 7 V20 have been adapted for PROFINET Security Class 1.	Section PROFINET Security Class 1 (Page 36)
Shared device	As of STEP 7 V20, S7-1500 Software Controllers also support the shared I-device functionality. As of STEP 7 V20, you can also use CM 1542-1 communications modules as assigned IO controllers for shared devices. As of STEP 7 V20, you can also load shared device configurations into a project that is not empty.	Section Shared device (Page 148)
Configuring SNMP and DCP	As of STEP 7 V20, you can configure the SNMP and DCP settings for an entire PROFINET IO system centrally. IO devices that support configuration of SNMP and DCP synchronize to the SNMP/DCP settings of the PROFINET interface of their higher-lever IO controller by default.	Section PROFINET Security (Page 310)
Increase of the configuration limits	For S7-1500 CPUs as of FW version V4.0, you can connect a larger number of IRT-capable devices per PROFINET interface through skillful configuration.	Section PROFINET with performance upgrade (Page 211)
Operating several PROFINET networks in isochronous mode	As of STEP 7 V20, you can operate multiple PROFINET networks in isochronous mode at S7-1500 CPUs. The CPU must support the PROFINET functionality "PROFINET with IRT" at both PROFINET interfaces.	Section Operating multiple PROFINET networks in isochronous mode (Page 232)
	You implement IRT isochronous mode between S7-1500 CPUs as of FW version V4.0 in multiple projects through use of PN/PN couplers as of FW version V6.0.	Function Manual SIMATIC S7-1500/S7-1500T Synchronous operation functions (https://support.industry.siemens.com/cs/ww/en/view/109817888)

What's new in the PROFINET Function Manual, 11/2023 edition compared to 11/2022 edition

Function	What are the customer benefits?	Where can I find this information?
Implementation of PROFINET Security Class 1	You read which configuration options for protocols and processes in STEP 7 V19 have been adapted for PROFINET Security Class 1.	Section PROFINET Security Class 1 (Page 36)
Configuring SNMP and DCP	As of V19, STEP 7 offers extended configuration options for the SNMP and DCP protocols in order to meet the requirements for PROFINET Security Class 1.	Section PROFINET Security (Page 310)
Project-internal shared device / shared I-device	As of STEP 7 V19, a shared device/shared I-device can be created together with a maximum of two IO controllers in a project. Previously, the 2nd IO controller required a separate project.	Section Shared device (Page 148)
Handling timeouts during data exchange	In the case of high network loads, timeouts may occur during data record communication in PROFINET IO devices. Previously, PROFINET IO communication was terminated by the CPU in this case. As of STEP 7 V19 and FW version V3.1, you can configure the behavior of the respective PROFINET interface.	Section Dealing with timeouts while exchanging data (Page 302)

What's new in the PROFINET Function Manual, 11/2022 edition compared to 05/2021 edition

Function	What are the customer benefits?	Where can I find this information?
Project-internal shared device	As of STEP 7 V18, it is also possible to configure project-internal shared devices under certain conditions.	Section Shared device (Page 148)
Maintenance of the communication relation (AR)	In the event of high network load, the communication relation is terminated by the CPU. As of FW version V3.0, the communication relation can be maintained by writing a data record.	Section Dealing with timeouts while exchanging data (Page 302)
Support PROFINET system redundancy R1	As of FW version V3.0, the S7-1500H supports PROFINET system redundancy R1. R1 devices are equipped with two interface modules compared to S2 devices. If one interface module fails, the R1 device can still be reached by the H-CPUs via the second interface module. Thus, R1 devices have a higher availability than S2 devices.	Section PROFINET with redundant S7-1500R/H system (Page 319)
MRP interconnection	As of FW version V3.0, the CPUs of the S7-1500H redundant system may be located in 1 or 2 rings during MRP interconnection.	Section MRP Interconnection with the redundant S7-1500R/H system (Page 342)

What's new in the PROFINET Function Manual, Edition 05/2021 compared to Edition 11/2018

Function	What are the customer benefits?	Where can I find this information?
MRP interconnection	The MRP interconnection procedure is an extension of MRP. MRP interconnection allows the redundant coupling of 2 or more rings with MRP in PROFINET networks. MRP interconnection offers the following advantages: There is no limit to the maximum number of 50 devices in a ring when setting up redundant network topologies. Monitoring of larger topologies with ring redundancy.	Section MRP interconnection (Page 194) Section MRP interconnection with the redundant system S7-1500R/H (Page 342)
Enable/disable the I-device	You can use the "D_ACT_DP" instruction to locally disable or enable the I-device function in the user program of the I-device CPU.	Section Enabling/disabling I-device in the user program of the I-device CPU (Page 142)

What's new in the PROFINET Function Manual, Edition 11/2019 compared to Edition 10/2018

Function	What are the customer benefits?	Where can I find this information?
Direct data exchange	In the case of direct data exchange, an S7-1500 CPU provides cyclic net data from the I/O area to one or more partners. The "Direct data exchange" function enables deterministic, isochronous IO communication between multiple S7-1500 CPUs.	Section Direct data exchange (Page 247)
Switched S1 device	The "Switched S1 device" function of the CPU enables operation of standard IO devices in the S7-1500R/H redundant system.	Section Switched S1 device (Page 325)

What's new in the PROFINET Function Manual, Edition 10/2018 compared to Edition 12/2017

This manual (version 10/2018) includes the following new functions compared to the previous version (version 12/2017):

Function	Applications	Your benefits
PROFINET IO with the redundant S7-1500R/H system	In a PROFINET IO system with the redundant S7-1500R/H system, the IO communication continues even when one CPU fails.	The redundant S7-1500R/H system offers a high degree of reliability and system availability. A redundant configuration of the most important automation components reduces the probability of production downtimes and the consequences of component failures.

What's new in the PROFINET Function Manual, version 12/2017 compared to version 09/2016

This manual (version 12/2017) encompasses the following new functions compared to the previous version (version 09/2016):

Function	Applications	Your benefits
Specifying the router for a PROFINET IO device	You can specify the IP address of a router for each IO device. You reach the IO device from outside the IP subnet through the router.	In the past, it was only possible to specify a router for a PROFINET IO interface at the IO controller. The IO devices inherited the setting of the IO controller interface. Now you can set the router address independently of the IO controller setting. This allows, for example, a router address at the IO device although you have not set a router address or have set a different address at the IO controller.
Configuring an IO device through hardware detection	You can detect an existing IO device and enter it in your project.	STEP 7 inserts the IO device with all the modules and submodules into the project. Article numbers and firmware versions between real and configured IO devices match. You reduce the configuration effort required.
Asset management	You can centrally manage non-PROFINET components (assets) of a PROFINET device. The PROFINET device makes the identification data of the assets available for evaluation via a standardized data record.	The new standardized PROFINET service makes it possible to manage all the hardware and firmware components of PROFINET devices centrally. The possibilities available for filtering device data, for example, depend on the range of performance of the evaluating application.
Asset management data record for I-devices	Special application of asset management: From the point of view of a higher-level IO controller, the modules plugged into the I-device represent assets. The user program in the I-device compiles the asset management data record. The IO controller can read identification data of the I-device modules through this data record.	See Asset management.

What's new in the PROFINET Function Manual, Version 09/2016 compared to Version 12/2014

This manual (version 09/2016) encompasses the following new functions compared to the previous version (version 12/2014):

Function	Applications	Your benefits
PROFINET IO on the 2nd PROFINET interface	You can operate another PROFINET IO system on the CPU or connect additional IO devices.	You use a fieldbus type in the plant. The CPU can perform fast and deterministic data exchange as an I-device with a higher-level controller (PROFINET/Ethernet) through the second line.
IRT with very short data cycle times down to 125 µs	You realize high-end applications with IO communication which place very high performance demands on the IO processing.	You make PROFINET IO communication and standard communication possible via one cable even with a send clock of 125 µs.
MRPD: Media Redundancy with Planned Duplication of frames	PROFINET IO IRT enables you to realize applications that place particularly high demands on the reliability and accuracy (isochronous mode).	By sending the cyclic IO data in both directions in the ring, the communication to the IO devices is maintained even when the ring is interrupted and does not result in device failure even with fast update times. You achieve higher reliability than with MRP.

Function	Applications	Your benefits
PROFINET performance upgrade	You can implement applications with high speed and send clock requirements. This is of interest to applications with high demands on performance.	Better utilization of the bandwidth results in short reaction times.
Limitation of the data infeed into the network	You limit the network load for standard Ethernet communication to a maximum value.	You flatten peaks in the data feed. You share the remaining bandwidth based on demand.

Conventions

STEP 7: We refer to "STEP 7" in this documentation as a synonym for the configuration and programming software "STEP 7 as of V12 (TIA Portal)" and subsequent versions.

This documentation contains pictures of the devices described. The figures may differ slightly from the device supplied.

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product, on handling of the product and on the section of the documentation to which you should pay particular attention.

1.1 SiePortal

You can find current information on the following topics quickly and easily here:

- **Catalog and ordering system**
  Ordering system for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).
- **Product support**
  All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.
- **Application examples**
  Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.
- **Services**
  Information about Industry Services, Field Services, Technical Support, spare parts and training offers.
- **Forums**
  For answers and solutions concerning automation technology.
- **mySiePortal**
  Your personal work area in the SiePortal for notifications, support requests, and configurable documents.

This information is provided by SiePortal on the Internet (https://sieportal.siemens.com/).

1.2 Function manuals documentation guide

1.2.1 Information classes Function Manuals



The documentation for the SIMATIC S7-1500 automation system, for the 1513/1516pro-2 PN, SIMATIC Drive Controller CPUs based on SIMATIC S7-1500 and the SIMATIC ET 200MP, ET 200SP, ET 200AL and ET 200eco PN distributed I/O systems is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742705).

Basic information



The system manuals and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500, SIMATIC Drive Controller, ET 200MP, ET 200SP, ET 200AL and ET 200eco PN systems. Use the corresponding operating instructions for 1513/1516pro-2 PN CPUs.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- Getting Started S7-1500
- System manuals
- Operating instructions ET 200pro and 1516pro-2 PN CPU
- Online help TIA Portal

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment manuals for CPUs
- Equipment manuals for interface modules
- Equipment manuals for digital modules
- Equipment manuals for analog modules
- Equipment manuals for communication modules
- Equipment manuals for technology modules
- Equipment manuals for power supply modules
- Equipment manuals for BaseUnits

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC Drive Controller and the S7-1500 automation system.

Examples:

- Function Manual Diagnostics
- Function Manual Communication
- Function Manuals Motion Control
- Function Manual Web Server
- Function Manual Cycle and Response Times
- PROFINET Function Manual
- PROFIBUS Function Manual

Product Information

Changes and supplements to the manuals are documented in a Product Information. The Product Information takes precedence over the device and system manuals.

You will find the latest Product Information on the Internet:

- S7-1500/ET 200MP (https://support.industry.siemens.com/cs/de/en/view/68052815)
- SIMATIC Drive Controller (https://support.industry.siemens.com/cs/de/en/view/109772684/en)
- Motion Control (https://support.industry.siemens.com/cs/de/en/view/109794046/en)
- ET 200SP (https://support.industry.siemens.com/cs/de/en/view/73021864)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109765611)

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- S7-1500/ET 200MP/SIMATIC Drive Controller (https://support.industry.siemens.com/cs/ww/en/view/86140384)
- ET 200SP (https://support.industry.siemens.com/cs/ww/en/view/84133942)
- ET 200AL (https://support.industry.siemens.com/cs/ww/en/view/95242965)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109781058)

1.2.2 Basic tools

Tools

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SIMATIC Automation Tool

You can use the SIMATIC Automation Tool to perform commissioning and maintenance activities on various SIMATIC S7 stations as bulk operations independent of TIA Portal.

The SIMATIC Automation Tool offers a wide range of functions:

- Scanning of a PROFINET/Ethernet system network and identification of all connected CPUs
- Assignment of addresses (IP, subnet, Gateway) and device name (PROFINET device) to a CPU
- Transfer of the date and the programming device/PC time converted to UTC time to the module
- Program download to CPU
- RUN/STOP mode switchover
- CPU localization through LED flashing
- Reading out of CPU error information
- Reading the CPU diagnostic buffer
- Reset to factory settings
- Firmware update of the CPU and connected modules

You can find the SIMATIC Automation Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/98161300)

PRONETA

SIEMENS PRONETA (PROFINET network analysis) is a commissioning and diagnostic tool for PROFINET networks. PRONETA Basic has two core functions:

- In the network analysis, you get an overview of the PROFINET topology. Compare a real configuration with a reference installation or make simple parameter changes, e.g. to the names and IP addresses of the devices.
- The "IO test" is a simple and rapid test of the wiring and the module configuration of a plant, including documentation of the test results.

You can find SIEMENS PRONETA Basic on the Internet:
(https://support.industry.siemens.com/cs/ww/en/view/67460624)

SIEMENS PRONETA Professional is a licensed product that offers you additional functions. It offers you simple asset management in PROFINET networks and supports operators of automation systems in automatic data collection/acquisition of the components used through various functions:

- The user interface (API) offers an access point to the automation cell to automate the scan functions using MQTT or a command line.
- With PROFIenergy diagnostics, you can quickly detect the current pause mode or the readiness for operation of devices that support PROFIenergy and change these as needed.
- The data record wizard supports PROFINET developers in reading and writing acyclic PROFINET data records quickly and easily without PLC and engineering.

You can find SIEMENS PRONETA Professional on the Internet.
(https://www.siemens.com/proneta-professional)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

1.2.3 S7 Port Configuration Tool (S7-PCT)

SIMATIC S7-PCT

The Port Configuration Tool (PCT) is a PC-based software for the parameter assignment of Siemens IO-Link Master modules and IO-Link devices from any manufacturer.

You integrate IO-Link-devices using the standardized device description "IODD", which you get from the respective device manufacturer. S7-PCT supports version 1.0 and V1.1 of the IODD.

S7-PCT is called via the hardware configuration of the IO-Link Master from STEP 7. When STEP 7 is not used or the IO-Link Master is not operated on a SIMATIC controller, "standalone"-operation is also possible.

You can find additional information on IO-Link on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/io-link.html).

1.2.4 S7 Failsafe Configuration Tool (S7-FCT)

SIMATIC S7-FCT

Failsafe Configuration Tool (FCT) enables you to GSD configure the following devices in third-party engineering systems:

- Selected, functionally fail-safe SIMATIC I/O devices
- Functionally fail-safe SIRIUS ACT PROFINET interfaces

The engineering system must meet the following requirements for this:

- Support of the CPD system integration acc. to "PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO"
- TCI implementation to Conformance Class C3

Additional information on S7-FCT can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109762827).

1.2.5 MultiFieldbus Configuration Tool (MFCT)

MultiFieldbus Configuration Tool

MultiFieldbus Configuration Tool (MFCT) is a PC-based software and supports the configuration of MultiFieldbus- and DALI-devices. In addition, the MFCT offers convenient options for mass firmware updates of ET 200 devices with MultiFieldbus- support and reading service data for many other Siemens devices.

Functional scope of the MFCT

- MultiFieldbus configuration:
  Engineering, configuration and diagnostics of MultiFieldbus-devices, provision of the required project files (project, UDT-, CSV- and EDS-file), transfer/export of the files to device and/or data memory.
- DALI configuration:
  Device selection and online configuration of DALI devices.

- TM FAST:
  Generation and download of FPGA-UPD- and FPGA-DB-files.
- Maintenance:
  Topology scan of a Ethernet network, reading of service data, parameter assignment and firmware update.
- Settings:
  Language switching German / English, network scanner speed, setting of the network adapter, installation of GSDML-and EDS-files.

System/installation requirements for MFCT

The MFCT runs under Microsoft Windows and does not require installation or administrator rights.

For MFCT you must also install the following software:

- Microsoft .NET Framework 4.8 (You can find an Offline Installer on the Internet. (https://support.microsoft.com/en-us/topic/microsoft-net-framework-4-8-offline-installer-for-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0))
- NPcap from directory "Misc"
- PG/PC interface from directory "Misc"
- Microsoft C++ Redistributable for x86-systems (you can find the installation data for download on the Internet. (https://aka.ms/vs/15/release/vc_redist.x86.exe))

The download of the tool and further information as well as documentation on the individual functions of the MFCT can be found on the Internet.
(https://support.industry.siemens.com/cs/de/en/view/109773881)

1.2.6 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International
(https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:



Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)



YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.

Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

Safety instructions

2

2.1 General security information

Note the security-relevant information provided in the corresponding system manual.

You can find information relevant to cybersecurity in the section Industrial cybersecurity (Page 22).

Industrial cybersecurity 3

3.1 Introduction to industrial cybersecurity

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the System Manual and the Security guidelines for SIMATIC HMI devices (https://support.industry.siemens.com/cs/us/en/view/109481300) for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information pertaining to the communication of your SIMATIC system.

NOTE

Security-related changes to software or devices are documented in the section Introduction (Page 7).

3.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

3.3 Cybersecurity-related information in this manual

Observe all security-related notes on topics in this Function Manual.

Security-relevant notes on ...	Section
PROFINET Security Class 1	PROFINET Security Class 1 (Page 36)

You can find security-relevant information on communication-specific topics, e.g. information on protocols in the Communication (https://support.industry.siemens.com/cs/us/en/view/59192925) Function Manual.

You can find information on creating a network concept and a secure network design in the following Internet entry (https://support.industry.siemens.com/cs/ww/en/view/109802750).

Description

4

4.1 Introduction to PROFINET

What is PROFINET IO?

Within the framework of Totally Integrated Automation (TIA), PROFINET IO is the logical further development of:

- PROFIBUS DP, the long-established fieldbus and
- Industrial Ethernet

PROFINET IO is based on 20 years of experience with the successful PROFIBUS DP and combines the normal user operations with the simultaneous use of innovative concepts of Ethernet technology. This ensures the integration of PROFIBUS DP into the PROFINET world.

PROFINET IO as the Ethernet-based automation standard of PROFIBUS/PROFINET International defines a cross-vendor communication, automation, and engineering model.

Objectives of PROFINET

The objectives of PROFINET:

- Industrial networking, based on Industrial Ethernet (open Ethernet standard)
- Compatibility of Industrial Ethernet and standard Ethernet components
- High robustness due to Industrial Ethernet devices. Industrial Ethernet devices are suited to the industrial environment (temperature, noise immunity, etc.).
- Use of IT standards such as TCP/IP, http.
- Real-time capability
- Seamless integration of other fieldbus systems

Implementation of PROFINET in SIMATIC

PROFINET is implemented in SIMATIC as follows:

- We have implemented communication between field devices in SIMATIC with **PROFINET IO**.
- Installation technology and network components are available as SIMATIC NET products.
- Ethernet standard protocol and procedures (e.g., SNMP = Simple Network Management Protocol for network parameter assignment and diagnostics) are used for remote maintenance and network diagnostics.

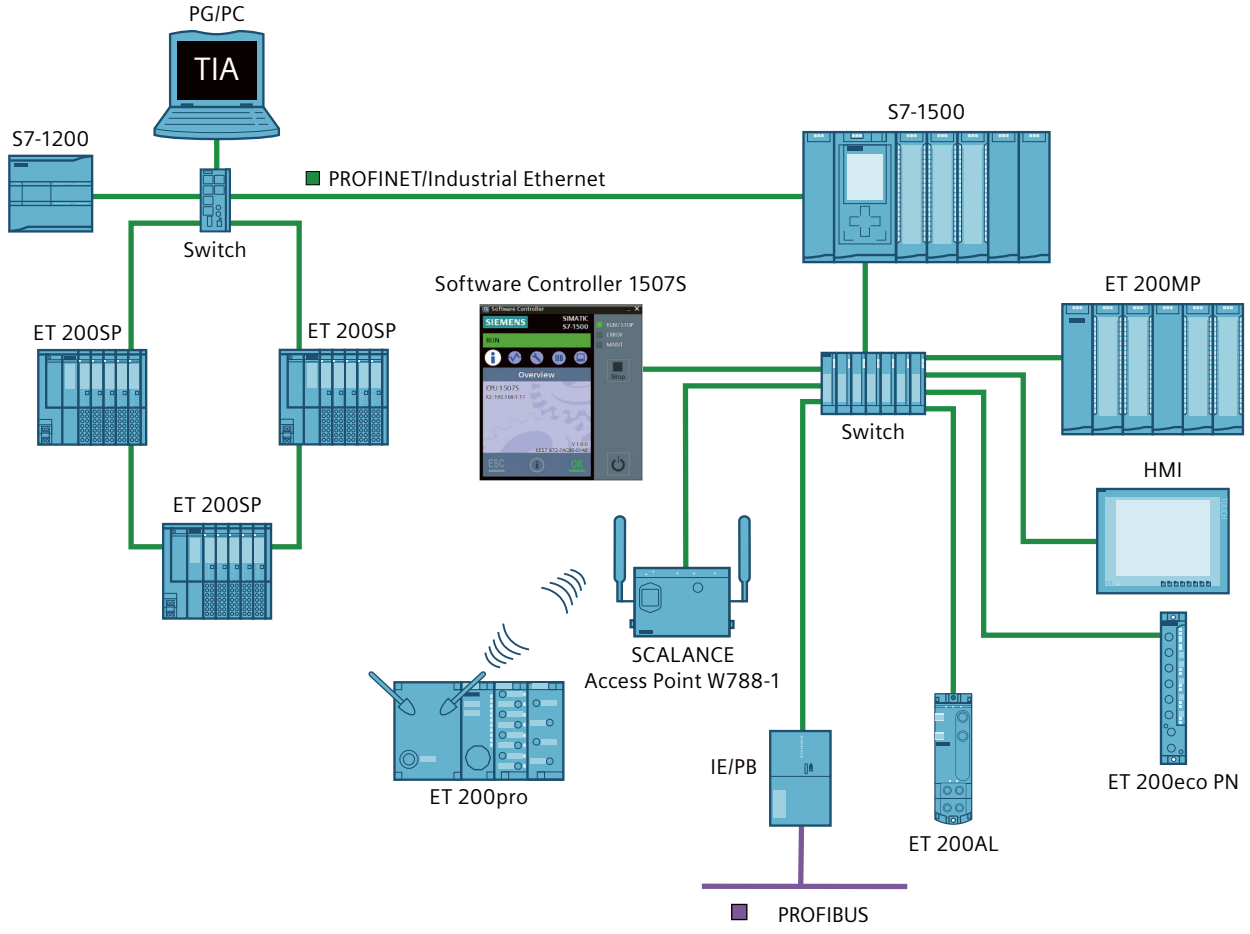


Figure 3-294 PROFINET overview configuration

STEP 7

The STEP 7 engineering tool supports you in setting up and configuring an automation solution. STEP 7 provides a uniform application view over all bus systems.

Documentation from PROFIBUS & PROFINET International on the Internet

You will find numerous documents on the topic of PROFINET at the Internet address (http://www.profibus.com) of the "PROFIBUS & PROFINET International" PROFIBUS user organization, which is also responsible for PROFINET.

Additional information can be found on the Internet (http://www.siemens.com/profinet).

Overview of the most important documents and links

A compilation of the most important PROFINET application examples, FAQs and other contributions in the Industry Online Support is available in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/108165711).

4.1.1 PROFINET terms

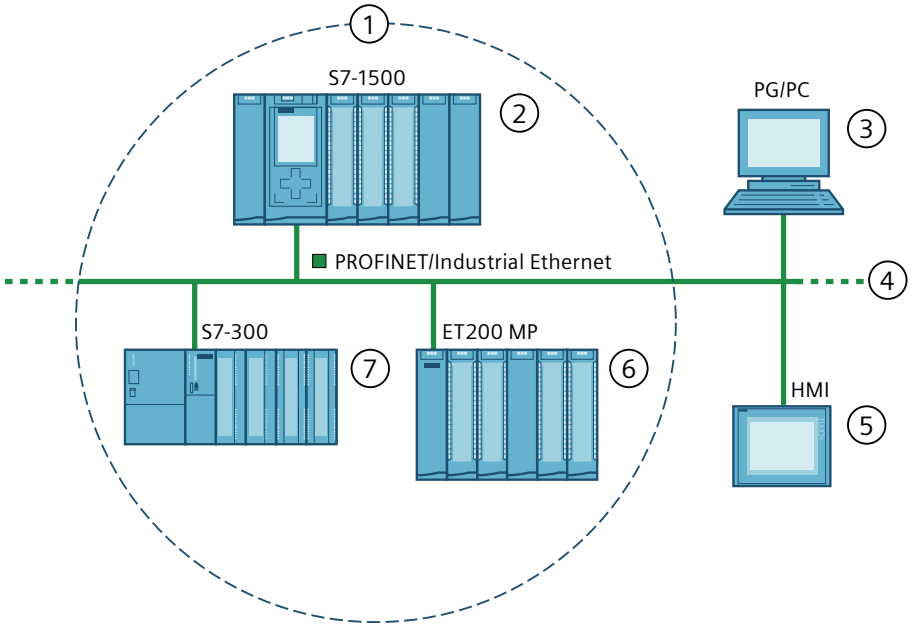
Definition: Devices in the PROFINET environment

In the PROFINET environment, "device" is the generic term for:

- Automation systems (PLC, PC, for example)
- Distributed I/O systems
- Field devices (for example, hydraulic devices, pneumatic devices)
- Active network components (for example, switches, routers)
- Gateways to PROFIBUS, AS interface or other fieldbus systems

PROFINET IO devices

The following graphic shows the general names used for the most important devices in PROFINET. In the table below the graphic you can find the names of the individual components in the PROFINET IO context.

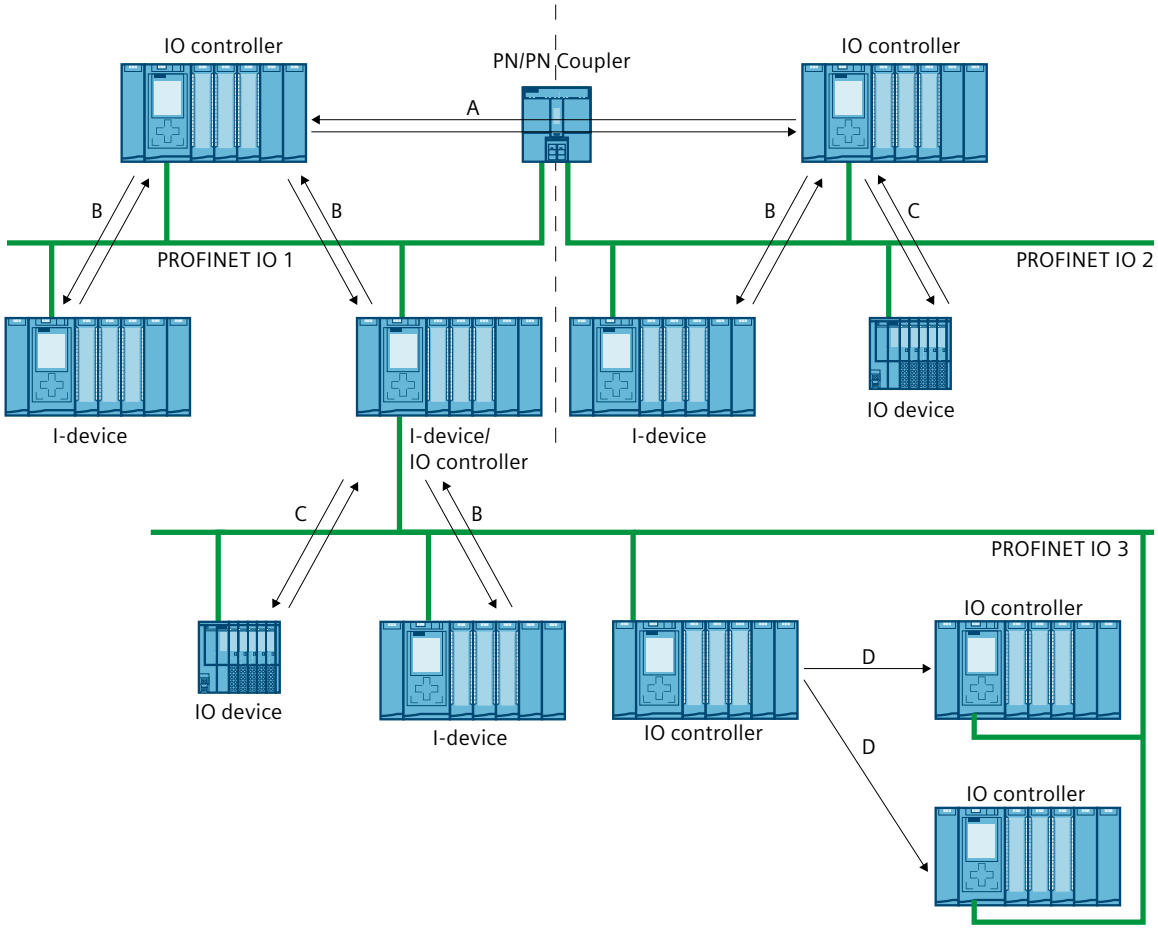


Number	PROFINET	Explanation
①	PROFINET IO System	
②	IO controller	Device used to address the connected IO devices. This means that: The IO controller exchanges input and output signals with field devices.
③	Programming device / PC (PROFINET IO supervisor)	PG/PC/HMI device used for commissioning and for diagnostics
④	PROFINET/Industrial Ethernet	Network infrastructure
⑤	HMI (Human Machine Interface)	Device for operating and monitoring functions.
⑥	IO device	A distributed field device that is assigned to one of the IO controllers (e.g., Distributed IO, valve terminals, frequency converters, switches with integrated PROFINET IO functionality)
⑦	I-device	Intelligent IO device

Figure 3-295 PROFINET devices

IO communication via PROFINET IO

The inputs and outputs of distributed I/O devices are read and written by means of PROFINET IO using what is referred to as IO communication. The following figure provides an overview of IO communication by means of PROFINET IO.



A IO controller - IO controller communication via PN/PN coupler
B IO controller - I-device communication
C IO controller - IO-device communication
D Direct data exchange between S7-1500-CPUs

Figure 3-296 IO communication via PROFINET IO

IO communication via PROFINET IO

Table 3-34 IO communication via PROFINET IO

Communication between ...	Explanation
IO controllers and IO devices	The IO controller sends data cyclically to the IO devices of its PROFINET IO system and receives data from these devices.
IO controller and I-device	A fixed quantity of data is transferred cyclically between the user programs in CPUs of IO controllers and I-devices. The IO controller does not access the I/O module of the I-device, but instead accesses configured address ranges, i.e. transfer ranges, which may be located

Communication between ...	Explanation
	inside our outside the process image of the CPU of the I-device. If parts of the process image are used as transfer ranges, it is not permitted to use these for real I/O modules. Data transfer takes place using load- and transfer operations via the process image or via direct access.
IO controller and IO controller (PN/PN coupler)	A fixed quantity of data is cyclically transferred between the user programs in CPUs of IO controllers. A PN/PN coupler is required as additional hardware. The IO controllers mutually access configured address ranges, i.e. transfer ranges, which may be located inside or outside the process image of the CPU. If parts of the process image are used as transfer ranges, it is not permitted to use these for real I/O modules. Data transfer takes place using load- and transfer operations via the process image or via direct access. I/O communication with PN/PN coupler is possible between two PROFINET IO systems.
S7-1500-CPU and S7-1500-CPU (direct data exchange)	In the case of direct data exchange, an S7-1500 CPU provides cyclic user data from the I/O area to one or more partners. The direct data exchange is based on PROFINET with IRT and isochronous mode. The data exchange takes place via transfer areas.

More information

You can find more information in the sections Network security (Page 47) and Functions (Page 117) as well as in the Communication (http://support.automation.siemens.com/WW/view/en/59192925) Function Manual.

4.1.2 Basic terminology of communication

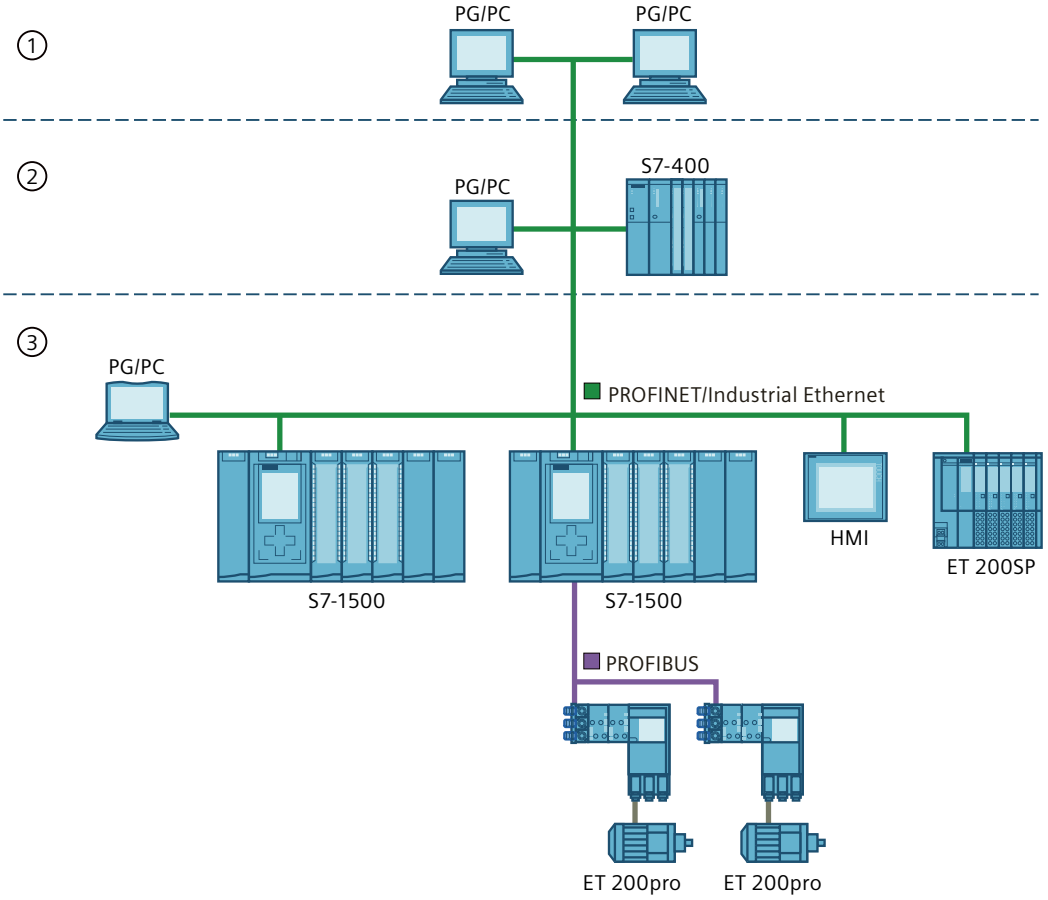
PROFINET communication

PROFINET communication takes place via Industrial Ethernet. The following transmission types are supported:

- Acyclic transmission of engineering and diagnostics data and interrupts
  - Acyclic PROFINET communication is used for non-time-critical data (non-real-time).
- Cyclic transmission of user data
  - The PROFINET-IO communication takes place in real-time.

Transparent data access

Access to process data from different levels of the factory is supported by PROFINET communication. By using Industrial Ethernet, standard mechanisms of communication and information technology such as OPC can now be used along with standard protocols such as UDP/TCP/IP and HTTP in automation engineering. This allows transparent access from company management level directly to the data from the automation systems at the control level and production level.



① Management level
② Control level
③ Production level

Figure 3-297 Access to process data

Update time

The update time is the time interval within which the IO controller and the IO device / I-device exchange IO data cyclically in the IO system. The time interval can be configured separately for each IO device and determines the following time intervals:

- Sending the output data from the IO controller to the IO device / I-device (output module/submodule)
- Sending the input data from the IO device / I-device to the IO controller (input module/submodule)

STEP 7 calculates the update time automatically in the default setting for each IO device of the PROFINET IO system, taking into account the volume of data to be exchanged as well as the set send clock.

Watchdog time

The watchdog time is the time interval that an IO controller or IO device permits, without receiving IO data. If the IO device is not supplied by the IO controller with data within the watchdog time, the IO device detects the missing frames and outputs substitute values. This is reported in the IO controller as a station failure.

In STEP 7, the watchdog time is made up from an integral multiple of the update time and can be set by the user.

Send clock

The period of time between two consecutive communication cycles. The send clock is the shortest possible interval in data exchange and thus also the smallest value that can be set for the update time.

Relationship between the update time and send clock

The calculated update times are reduction ratios (1, 2, 4, 8, ..., 512) of the send clock. The minimum possible update time thus depends on the minimum send clock of the IO controller that can be set and the efficiency of the IO controller and IO device. Depending on the send clock, it can be that only some of the reduction ratios are available (STEP 7 guarantees this through a pre-selection).

The following tables illustrate the dependency of the update time that can be set on the send clock, using an example of the CPU 1516-3 PN/DP. The update times satisfy the requirements of the PROFINET standard IEC 61158.

Table 3-35 With real-time communication the following applies:

Send clock	Update time	Reduction ratios
250 µs	250 µs to 128 ms	1,2, ..., 512
500 µs	500 µs to 256 ms	1,2, ..., 512
1 ms	1 ms to 512 ms	1,2, ..., 512
2 ms	2 ms to 512 ms	1,2, ..., 256
4 ms	4 ms to 512 ms	1,2, ..., 128

More information

You can find more information on real-time communication and the update time in the Real-time communication (Page 197) section.

4.1.3 PROFINET interface

Overview

PROFINET devices of the SIMATIC product family have one or more PROFINET interfaces (Ethernet controller/interface). The PROFINET interfaces have one or more ports (physical connection options).

In the case of PROFINET interfaces with multiple ports, the devices have an integrated switch.

PROFINET devices with two ports on one interface allow you to configure the system in a line or ring topology. PROFINET devices with three or more ports on one interface are also ideal for setting up tree topologies.

Properties and rules for naming the PROFINET interface and its representation in STEP 7 are explained in the following.

Properties

Every PROFINET device on the network is uniquely identified via its PROFINET interface. For this purpose, each PROFINET interface has:

- A MAC address (cannot be changed)
- A PROFINET device name
- An IP address

Identification and numbering of the interfaces and ports

Interfaces and ports for all modules and devices in the PROFINET system are identified with the following characters:

Table 3-36 Identification for interfaces and ports of PROFINET devices

Element	Symbol	Description
Interface	X	In ascending order starting from number 1
Port	P	In ascending order starting from number 1 (for each interface)
Ring port	R	These ports can be used for a ring topology.

Examples of identification

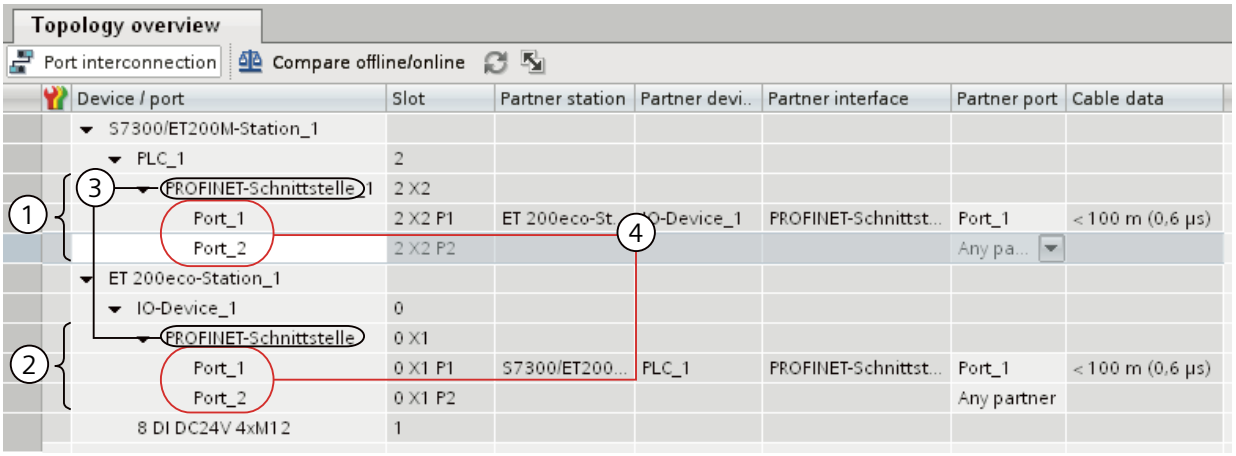
Three examples illustrate the rules for identifying PROFINET interfaces:

Table 3-37 Examples for identifying PROFINET interfaces

Sample labeling	Interface	Port
X2 P1	2	1
X1 P2	1	2
X1 P1 R	1	1 (ring port)

Representation of PROFINET Interfaces in the Topology Overview in STEP 7

You can find the PROFINET interface in the topology overview in STEP 7. The PROFINET interface for an IO controller and an IO device is represented as follows in STEP 7:



Number	Description
①	PROFINET interface of an IO controller in STEP 7
②	PROFINET interface of an IO device in STEP 7
③	These lines represent the PROFINET interface.
④	These lines represent the ports of a PROFINET interface.

Figure 3-298 Representation of the PROFINET interfaces in STEP 7

Schematic Representation of a PROFINET Interface with Integrated Switch

The following schematic diagram shows the PROFINET interface with integrated switch and its ports for all PROFINETdevices.

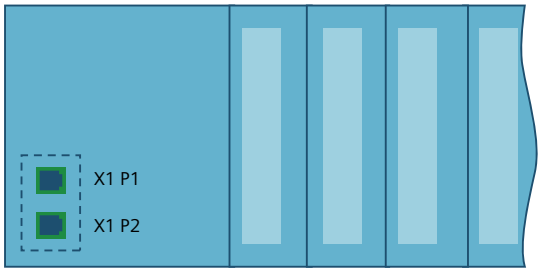


Figure 3-299 PROFINET interface with integrated switch

Functional differences of the PROFINET interfaces

PROFINET interfaces can provide different functions. PROFINET interface functions include identification, configuration, diagnostics and communication services (e.g., open communication). PROFINET interfaces that provide PROFINET IO functions and network security functions are also available.

The following table illustrates the differences using the example of the CPU 1516-3 PN/DP (as of firmware version V2.0), which features two PROFINET interfaces with different functionality.

Table 3-38 Differences between the PROFINET interfaces of the CPU 1516-3 PN/DP (as of firmware version V2.0)

PROFINET interface (X1) with 2 ports	PROFINET interface (X2) with 1 port
Identification, configuration and diagnostics	
PG communication	
HMI communication	
S7 communication	
Time-of-day synchronization	
Web server	
Open communication	
OPC UA server	
IO controller	
I-device	
RT	
IRT	-
Isochronous mode	-
Media redundancy	-
Prioritized startup	-

S7-1500 CPUs with two ports each at PROFINET interfaces X1 and X2 support the same functionalities at the PROFINET interface X2 as at the PROFINET interface X1, with the exception of prioritized startup. This includes, for example the following CPUs as of firmware version V4.0:

- CPU 1517(F)-3 PN
- CPU 1518(F)-3 PN
- CPU 1516T(F)-3 PN
- CPU 1517T(F)-3 PN
- CPU 1518T(F)-3 PN

S7-1500H CPUs as of FW version V4.0 have two ports at PROFINET interface X2, but do not support media redundancy (ring topology) at this PROFINET interface.

To find out which protocols are supported by IO devices, refer to the relevant equipment manual.

Additional Information on the Functionality of PROFINET interfaces

You can find information on the number and functionality of the interfaces of a PROFINET device in the documentation for the specific PROFINET device.

PROFINET communication services are described in the Communication function manual (http://support.automation.siemens.com/WW/view/en/59192925).

In the Network security (Page 47) section you can find components that are used to protect networks against hazards.

The Functions (Page 117) section describes the PROFINET IO functions.

4.1.4 Implementation of the PROFINET device model in SIMATIC

Slots and modules

A PROFINET device can have a modular and compact structure. A modular PROFINET device consists of slots into which the modules are inserted. A module can contain multiple submodules. The modules have channels which are used to read and output process signals. A compact device has the same design and can include modules, however, it cannot be physically expanded, which means that no modules can be inserted.

This is illustrated by the following graphic.

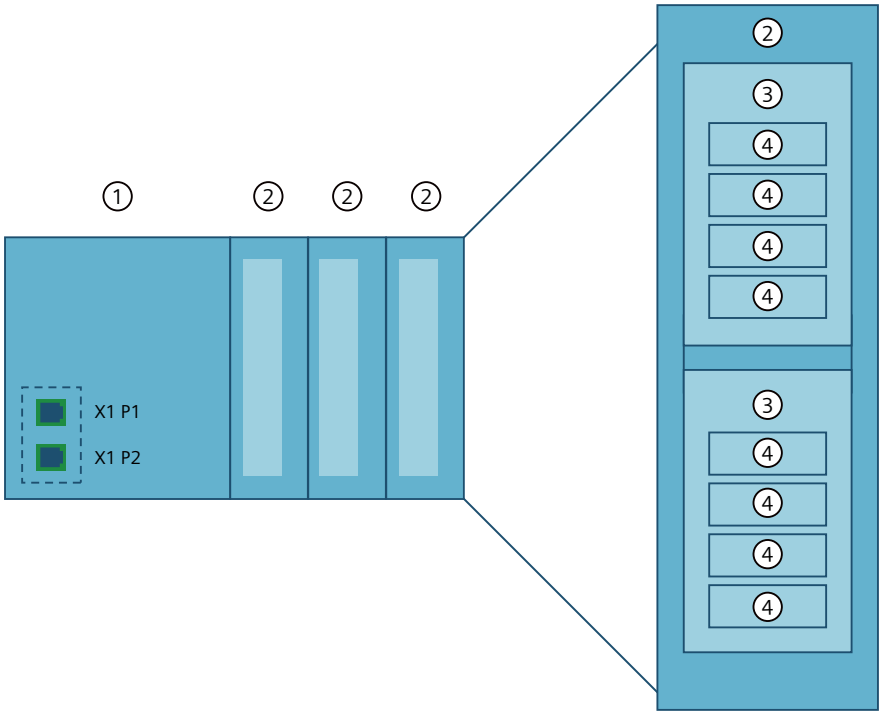


Figure 3-300 Configuration of a PROFINET device

Number	Description
1	Slot with bus interface

② Slot with module
③ Subslot with submodule
④ Channel

Representation of PROFINET Device Model in the Device View of STEP 7

The following figure shows the representation of the PROFINET device model in the device view of STEP 7, based on the example of a distributed I/O system ET 200MP:

Device overview

Module	Rack	Slot	I address	Q address	Type
IO-Device_1	0	1			IM 155-5 PN ST
PROFINET-Schnittstelle	0	1 X1			PROFINET interface
Port_1	0	1 X1 P1			Port
Port_2	0	1 X1 P2			Port
DI 32x24VDC HF_1	0	2	16...19		DI32 x 24VDC HF
DQ 32x24VDC/0.5A ST_1	0	3		0...3	DQ32 x 24VDC / 0.5A ST

Figure 3-301 PROFINET device model in the device view of STEP 7

4.2 PROFINET Security Class 1

Introduction

With the introduction of the PROFINET Security Class 1, additional security settings were integrated to harden the PROFINET network.

Like in other areas of IT security, PROFINET security is based on the Defense-in-Depth concept. Multiple independent methods provide multi-layered protection against attacks or inadvertent changes.

PROFINET Security Class 1 includes the following security mechanisms for protecting your PROFINET network:

- Configuration options for the SNMP and DCP protocols
- Digital signature of PROFINET GSD files

These introductory sections provide information on which configuration options have been modified for PROFINET Security Class 1.

Simple Network Management Protocol (SNMP)

SNMP is used for simple, network-based device management. For example, PROFINET devices support the following SNMP functions:

- Monitoring and diagnostics of the network topology through network management services
- Reading device-specific information

Since STEP 7 V18, SNMP has been disabled in the basic settings of a CPU. You can enable or disable SNMP via the configuration or by writing a data record from the user program. You enter the community strings for read and write access via the configuration.

As of STEP 7 V19, you can configure SNMP both for CPUs and for IO devices for the following access types:

- Read and write access
- Read access only

As of STEP 7 V20, you can configure SNMP for an entire PROFINET IO system at the PROFINET interface of the IO controller. The SNMP settings on the PROFINET interface do not affect the IO controller but serve as a central specification for the connected PROFINET IO system.

If IO devices support the configuring of SNMP, the PROFINET interface of the higher-level IO controller synchronizes the SNMP settings in the device properties of the IO devices by default. Changes to the SNMP settings are also automatically synchronized. Alternatively, you can change the default behavior in the module properties of IO devices and set your own SNMP settings.

To determine whether IO devices support the configuration of SNMP, refer to the respective equipment manuals. IO devices that support the configuration of SNMP behave as follows during configuration or initial loading of the hardware configuration:

- STEP 7 < V19: SNMP is enabled on the IO device. When SNMP is enabled, the community strings are set to the following default values:
  - Read-only (read-only community string): public
  - Read and write access (read-write community string): private
- STEP 7 V19 and higher: SNMP is deactivated as default. Changed SNMP settings do not take effect until the hardware configuration has been loaded.

Discovery Configuration Protocol (DCP)

DCP helps locate PROFINET devices in the network and enables the basic settings, e.g. assignment of IP address or PROFINET device name.

Since STEP 7 V19, the "Activate DCP write protection" option is available for DCP. This "PROFINET Security Class 1" function prevents write access to PROFINET devices via DCP during IO data exchange and thus, for example, provides protection from unwanted interruptions of application relationships (ARs).

As of STEP 7 V20, you can configure DCP for an entire PROFINET IO system at the PROFINET interface of the IO controller. If IO devices support the configuring of DCP, the PROFINET interface of the higher-level IO controller synchronizes the DCP settings in the device properties of the IO devices by default. Changes to the DCP settings are also automatically synchronized.

If the IO controller and IO device support the write protection function for DCP, this option is enabled by default for the corresponding communication relation. An enabled DCP write protection function takes effect in the following cases:

- On the IO controller side: An IO controller sets up the communication relation with a corresponding IO device (the IO device does not need to be accessible for this purpose).
- On the IO device side: There is an active communication relation between the IO controller and the IO device.

When the write protection function of DCP is in effect, for example, Set commands (DCP Set) are rejected.

When the write protection option of DCP is enabled, ongoing operation is secured as follows:

- DCP only has read access to the device information of the IO device.
- Changes to the basic settings of IO devices are no longer possible.

Authenticity of PROFINET GSD files

The manufacturer provides a general station description file (GSD file) for each PROFINET device. The GSD file describes the properties of the device in a machine readable XML format and contains all properties of a PROFINET-device that are needed for configuring.

With the introduction of PROFINET Security Class 1, GSD files together with other related files, such as images or text files, are provided in a GSDX file with a verified manufacturer signature. A GSDX file can contain multiple GSD files, such as all GSD files of a device family. The included signature confirms the integrity and authenticity of the contained files. This ensures that the files contained in the GSDX file originate from the expected manufacturer and have not been altered after generation of the signature.

If your engineering system does not support the import of GSDX files, continue using GSD files as up to now.

Confirming authenticity of PROFINET GSD files with the distributor ID

If a GSDX file contains a digital signature, the signature confirms the authenticity and integrity of the GSD files it contains. A GSDX file can only contain a single signature. Only signed GSDX files fulfill the requirements of PROFINET Security Class 1.

When importing GSDX files for standard IO devices, STEP 7 uses the signature to check whether the GSD files in the GSDX file originate from the corresponding device manufacturer. A GSDX file that contains the manufacturer's own devices as GSDML files is successfully checked during import based on the signature it contains.

In addition to checking the digital signature, the identity of the creator of the GSDX file is also verified. Because both device manufacturers and suppliers (distributors) can create and sign GSDX files, identity verification is also mandatory for suppliers. A distinction must therefore be made between the following roles:

- The device manufacturer (vendor):
  A device manufacturer, e.g. SIEMENS, can export the devices it manufactures as a GSD file, pack them into a GSDX file and sign the GSDX file. When importing, STEP 7 can successfully check the file, since the identity of the device manufacturer matches the vendor ID in the GSD file.
- The supplier (distributor):
  A supplier, e.g. system manufacturer, uses the devices of a third-party manufacturer. The supplier would like to publish these third-party devices as GSD file in the form of a signed GSDX file. Because the provider is not the device manufacturer, the provider needs its own identity for the signature process.

Both device manufacturers and suppliers can apply for a signature card (smart card) from the PNO (https://www.profibus.com/products/gsd-files/gsd-signing). The signature card is issued for the corresponding identity (vendor ID or distributor ID). This signature card can be used to create valid GSDX files and make them available for use in engineering tools, such as STEP 7.

In STEP 7 from V21, you can add a distributor ID to an I-device during configuration. In this case, you must create the I-device from a CPU with FW version V4.1 or higher. When exporting the configured I-device, the distributor ID is transferred to the generated GSD file. You can pack this generated GSD file into a GSDX file and sign it.

More information

You can find detailed information on SNMP in the Communication (https://support.industry.siemens.com/cs/us/en/view/59192925) Function Manual.

For information on how to configure SNMP in your PROFINET network, see section Configuring the SNMP (Page 310).

For information on how to configure DCP in your PROFINET network, see section Configuring DCP (Page 316).

You can read how to add a distributor ID to an I-device in the section Configuring the I-device (Page 129).

4.3 Setting up PROFINET

Contents of this chapter

The following chapter provides background information on building your communication network.

- Overview of the most important passive network components: These are network components that forward a signal without the possibility of actively influencing it, for example, cables, connectors, etc.
- Overview of the most important active network components: These are network components that actively affect a signal, for example switches, routers, etc.
- Overview of the most common network structures (topologies).

Physical connections of industrial networks

The networking of PROFINET devices in industrial systems is generally possible in 2 different physical ways:

- Connected line
  - By means of electrical pulses via copper cables
  - By means of optical pulses via fiber-optic cables
- Wireless via wireless network using electromagnetic waves

PROFINET devices and cabling technology in SIMATIC are suited for industrial use, as they are based on Fast Ethernet and Industrial Ethernet.

- **Fast Ethernet**

  With Fast Ethernet, you transfer data at a speed of 100 Mbps. This transfer technology uses the 100 Base-T standard for this.
- **Industrial Ethernet**

  Structure of Ethernet in industrial environment.

  The biggest difference from standard Ethernet is the mechanical current carrying capacity and noise immunity of the individual components.

4.3.1 Active Network Components

Introduction

The following active network components are available for PROFINET:

- Switch
- Router

Switched Ethernet

PROFINET IO is based on switched Ethernet with full-duplex operation and a bandwidth of 100 Mbps. In this way, the network can be used much more efficiently through the simultaneous data transfer of several devices. The PROFINET IO frames are processed with high priority.

Switches

Switches are network components used to connect several terminal devices or network segments in a local network (LAN).

For the communication of a device with several other devices on PROFINET, the device is connected to the port of a switch. Other communication devices (including switches) can then be connected to the other ports of the switch. The connection between a communication device and the switch is a point-to-point connection.

A switch has the task of receiving and distributing frames. The switch "learns" the Ethernet address(es) of a connected PROFINET device or additional switches and only forwards those frames that are intended for the connected PROFINET device or the connected switch.

Switch variants

Switches are available in two models:

- Integrated into a PROFINET device

  PROFINET devices with multiple ports per interface are devices with an integrated switch (for example, CPU 1516-3 PN/DP)
- As autonomous device (for example, switches of the SCALANCE product family)

Selection Guide for Switches

To use PROFINET with the RT class "RT", you can use any switch of "PROFINET Conformance Class A" or higher. All switches of the SCALANCE product family meet these requirements.

If you want to use PROFINET functions that provide an additional value, such as topology recognition, diagnostics, device exchange without exchangeable medium/programming device, you have to use a switch of the "PROFINET Conformance Class B" or higher.

To use PROFINET with the RT class "IRT", you must use a switch of "PROFINET Conformance Class C". With switches of the SCALANCE product family, watch out for the catalog feature "IRT PROFINET IO switch".

To select appropriate switches, we recommend the SIMATIC NET Selection Tool on the Internet (http://support.automation.siemens.com/WW/view/en/39134641).

Switches of the SCALANCE product family

Use the switches of the SCALANCE product family if you want to use the full scope of PROFINET. They are optimized for use in PROFINET IO.

In the SCALANCE X device family, you will find switches with electrical and optical ports and with a combination of both variants. SCALANCE X202-2IRT, for example, has two electrical ports and two optical ports and supports IRT communication.

Beginning with the SCALANCE X200, you can configure, diagnose and address switches of the SCALANCE X device series as PROFINET IO devices using STEP 7.

Router

A router connects separated network segments with each other (e.g. management level and control level). The volume of data volume must be coordinated with the services of the respective network segment. A router also separates two networks and acts as a mediator between both networks. It thus reduces the network load. Routing functionality is provided in the SCALANCE X device family, with SCALANCE X300 or higher.

Communication devices on different sides of a router can only communicate with one another if you have explicitly enabled communication between them via the router.

If you want to access manufacturing data directly from SAP, for example, use a router to connect your Industrial Ethernet in the factory with the Ethernet in your office.

NOTE

If devices need to communicate beyond the limits of a network, you must configure the router so that it allows this communication to take place.

Information on routing with STEP 7 is available in the function manual Communication (http://support.automation.siemens.com/WW/view/en/59192925).

4.3.2 Cabling technology

Cables for PROFINET

Electrical and optical cables are available for PROFINET. The type of cable depends on the data transfer requirements and on the ambient conditions.

Simple method for the prefabrication of twisted pair cables

When you set up your PROFINET system, you can cut the twisted-pair cable to the required length on site, strip it with the *stripping tool* (for Industrial Ethernet), and fit the *Industrial Ethernet Fast Connect RJ45 plugs* using the cut-and-clamp method. For more information on installation, refer to the installation instructions in the "SIMATIC NET Industrial Ethernet Network Manual" (http://support.automation.siemens.com/WW/view/en/8763736).

NOTE

A maximum of four connector pairs are allowed between two switches per Ethernet path.

Simple method for the prefabrication of fiber-optic cables

The FastConnect FO cabling system is available for the easy, fast and error-free prefabrication of fiber-optic cables. The glass-fiber optic cable consists of:

- FC FO Termination Kit for SC and BFOC plug (cleave tool, Kevlar scissors, buffer grip, fiber remains container)
- FC BFOC Plug
- FC SC Duplex plug
- FO FC Standard cable
- FO FC Trailing cable

Simple method for the prefabrication of POF and PCF cables

The following special tools provide an easy and safe way to prefabricate POF / PCF cables and fit the SC RJ POF plugs:

- POF cable
  Prefabrication case IE Termination Kit SC RJ POF plug
- PCF cable
  Prefabrication case IE Termination Kit SC RJ PCF plug

Overview of transmission media with PROFINET

The following table summarizes the technical specifications of a PROFINET interface with integrated switch or an external switch, and possible transmission media.

Table 3-39 Transmission media with PROFINET

Physical properties	Connection methods	Cable type / transmission medium standard	Transmission rate / mode	Max. segment length (between two devices)	Advantages
Electrical	RJ45 connector ISO 60603-7	100Base-TX 2x2 twisted, symmetrical and shielded copper cable, CAT 5 transmission requirement IEEE 802.3	100 Mbps, full duplex	100 m	Simple and cheap cable connection
Optical	SCRJ 45 ISO/IEC 61754-24	100Base-FX POF fiber-optic cable (Polymer Optical Fiber, POF) 980/1000 µm (core diameter / external diameter) ISO/IEC 60793-2	100 Mbps, full duplex	50 m	Use when there are large differences in potential Insensitive towards electromagnetic radiation Low line attenuation Considerably longer segments possible[1]
		Plastic-cladded glass fiber (Polymer Cladded Fiber, PCF) 200/230 µm (core diameter / external diameter) ISO/IEC 60793-2	100 Mbps, full duplex	100 m	
	BFOC (Bayonet Fiber Optic Connector) and SC (Subscriber Connector) ISO/IEC 60874	Monomode glass fiber optic cable 10/125 µm (core diameter / external diameter) ISO/IEC 60793-2	100 Mbps, full duplex	26 km	
		Multimode glass fiber optic cable 50/125 µm and 62.5/125 µm (core diameter / external diameter) ISO/IEC 9314-4	100 Mbps, full duplex	3000 m	
	LC (Lucent Connector) ISO/IEC 61754-20	Fiberglass FOC single-mode fiber 9/125 µm (core diameter / external diameter) ISO/IEC 60793-2	100 Mbps, full duplex	10 km (IRT) 20 km (RT)	
Electromagnetic wave	-	IEEE 802.11 x	Depends on the extension used (a, g, h, etc.)	100 m	Greater mobility Cost-effective networking to remote, difficult to access devices

[1] Applies for fiber-optic cables only

More information

For information on the PROFINET interface, refer to the section PROFINET interface (Page 32).

More information about Industrial Ethernet networks with the help of SIMATIC NET components can be found in the SIMATIC NET (http://support.automation.siemens.com/WW/view/en/27069465) System Manual.

You can find the installation guideline for PROFINET in the following Internet entry (https://www.profibus.com/download).

4.3.3 Wireless design

4.3.3.1 Basics

What is Industrial Wireless LAN?

In addition to data communication in accordance with the IEEE 802.11 standard, the SIMATIC NET Industrial Wireless LAN provides a number of enhancements which offer significant benefits for industrial customers. IWLAN is particularly suitable for demanding industrial applications that require reliable wireless communication. This is supported by the following properties:

- Automatic roaming when the connection to Industrial Ethernet is interrupted (Forced Roaming)
- Cost savings generated by using a single wireless network for reliable operation of a process with both process-critical data (alarm message, for example) and non-critical communication (service and diagnostics, for example)
- Cost-effective connection to devices in remote environments that are difficult to access
- Predictable data traffic (deterministic) and defined response times
- Cyclical monitoring of the wireless link (link check)

Objectives and advantages of Industrial Wireless LAN

Wireless data transmission achieves the following objectives:

- Seamless integration of PROFINET devices into the existing bus system via the wireless interface
- Mobile use of PROFINET devices for different production-linked tasks
- Flexible configuration of the system components for fast development in accordance with customer requirements
- Maintenance costs are minimized by savings in cables

Application examples

- Communication with mobile subscribers (mobile controllers and devices, for example), conveyor lines, production belts, translation stages , and rotating machines
- Wireless coupling of communication segments for fast commissioning or cost-effective networking where routing of wires is extremely expensive (e.g. public streets, railroad lines)
- Stacker trucks, automated guided vehicle systems and suspended monorail systems

The following graphic illustrates the many possible applications and configurations for SIMATIC device family wireless networks.

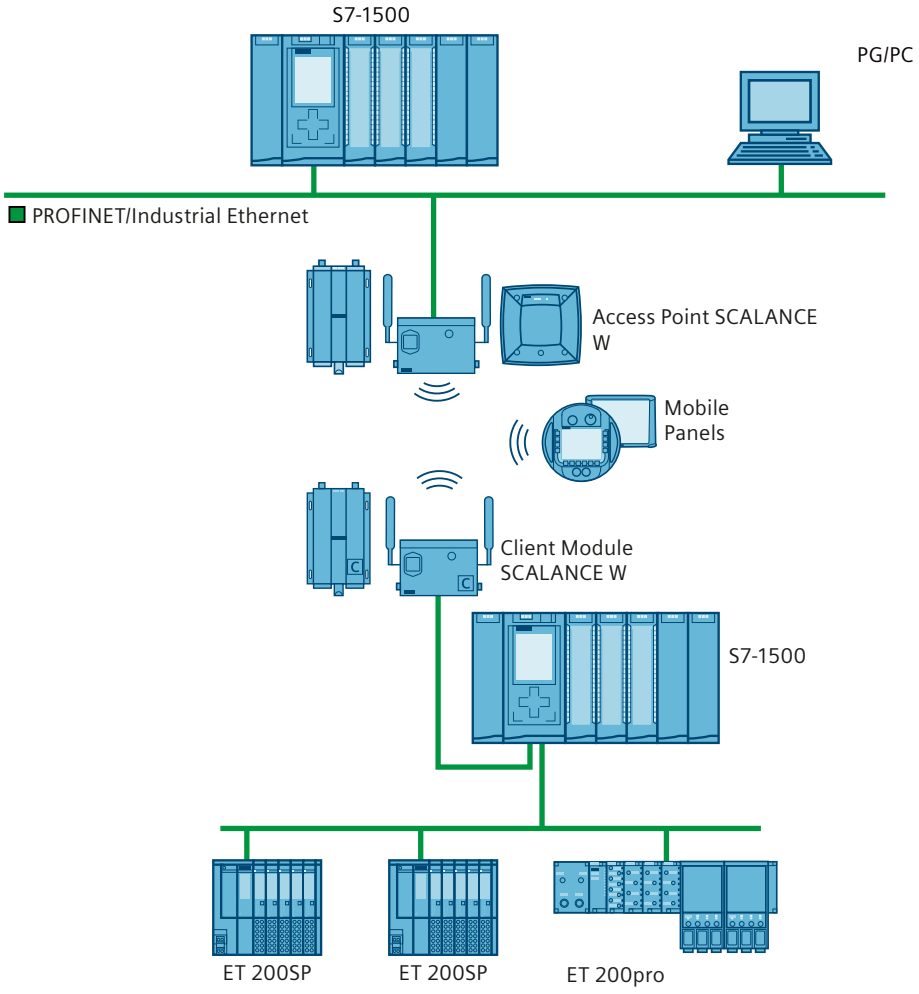


Figure 3-302 Application example for the use of Industrial Wireless LAN

Data transmission rate

In Industrial Wireless LAN, gross data transmission rates of 11 Mbps or 54 Mbps without full duplex are permitted.

Range

With SCALANCE W (access points), wireless networks can be set up indoors and outdoors. Multiple access points can be installed to create large wireless networks in which mobile subscribers are transferred seamlessly from one access point to another (roaming).

As an alternative to a wireless network, point-to-point connections of Industrial Ethernet segments can also be set up over large distances (several hundred meters). In this case, the range and characteristics of the RF field are determined by the antennas used.

NOTE

Range

The range can be considerably less, depending on spatial factors, the wireless standard used, the data rate, and the antennas on the send and receive sides.

4.3.3.2 Tips on assembly

Wireless networks, SCALANCE device family

With PROFINET, you can also set up wireless networks with Industrial Wireless Local Area Network (IWLAN) technology. We recommend implementing the SCALANCE W device line for this.

Update time in STEP 7

If you set up PROFINET with Industrial Wireless LAN, you may have to increase the update time for the wireless devices. The IWLAN interface provides lower performance than the wired data network: Several communication stations have to share the limited transmission bandwidth. For wired solutions, 100 Mbps is available for each communication device.

The Update time parameter can be found in the "Realtime settings" section in the Inspector window of IO devices in STEP 7.

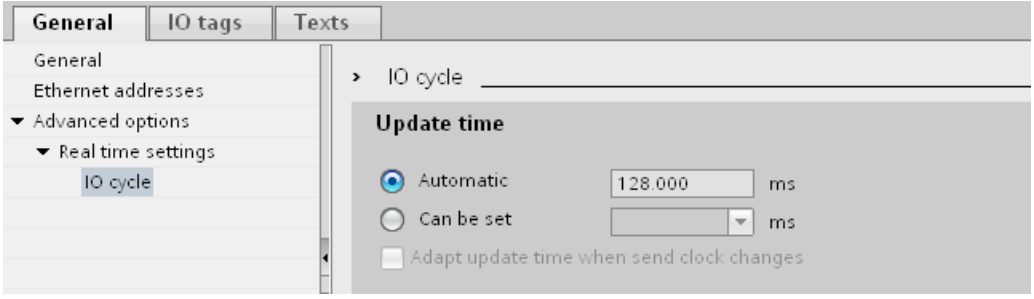


Figure 3-303 Update time in STEP 7

Additional information

More information about SCALANCE W Industrial Wireless LAN components can be found in the manual SIMATIC NET SCALANCE W-700 (http://support.automation.siemens.com/WW/view/en/42784493).

More information about wired data transmission can be found in the manual SIMATIC NET Twisted Pair and Fiber Optic Networks (http://support.automation.siemens.com/WW/view/en/8763736).

More information about wireless data transmission can be found in the manual Basics for configuring an industrial wireless LAN (http://support.automation.siemens.com/WW/view/en/9975764).

You should also read the PROFINET installation guideline of the PROFIBUS User Organization on the Internet (http://www.profibus.com/nc/download/installation-guide/downloads/profinet-installation-guide/display/). Various documents that assist with the setting up of your PROFINET automation solution are available here:

- PROFINET planning guideline
- PROFINET installation guideline
- PROFINET commissioning guideline
- Additional documents for setup of PROFINET

4.3.4 Network security

4.3.4.1 Basics

Introduction

The topic of data security and access protection (Security) has become increasingly important in the industrial environment. The increased networking of entire industrial systems, vertical integration and networking of levels within a company and new techniques such as remote maintenance all result in higher requirements for protecting the industrial plant.

Data security solutions for office environments cannot simply be transferred one-to-one to industrial applications to protect against manipulation in sensitive systems and production networks.

Requirements

Additional security requirements arise from the specific communication requirements in the industrial environment (real-time communication, for example):

- Protection against interaction between automated cells
- Protection of network segments
- Protection against faulty and unauthorized access
- Scalability of network security
- Must not influence the network structure

Definition of security

Generic term for all the measures taken to protect against:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability due to destruction of data, for example, through faulty configuration and denial-of-service attacks

Threats

Threats can arise from external and internal manipulation. The loss of data security is not always caused by intentional actions.

Internal threats can arise due to:

- Technical errors
- Operator errors
- Defective programs

Added to these internal threats there are also external ones. The external threats are not really any different to the known threats in the office environment:

- Software viruses and worms
- Trojans
- Man-in-the-middle attacks
- Password Phishing
- Denial of Service

Protective measures

The most important precautions to prevent manipulation and loss of data security in the industrial environment are:

- Physical access protection to the devices
- Filtering and control of data traffic by means of firewall
- A virtual private network (VPN) is used to exchange private data on a public network (Internet, for example).

  The most common VPN technology is IPsec. IPsec (Internet Protocol Security) is a collection of security protocols that are used as the basis for the IP protocol at the mediation level and allow a secured communication via potentially unsecure IP networks.
- Segmenting in protected automation cells

  This concept has the aim of protecting the lower-level network devices by means of security modules. A group of protected devices forms a protected automation cell.
- Authentication (identification) of the devices

  The security modules identify each other over a safe (encrypted) channel using authentication procedures. It is therefore impossible for unauthorized parties to access a protected segment.
- Encrypting the data traffic

  The confidentiality of data is ensured by encrypting the data traffic. Each security module is given a VPN certificate which includes the encryption key.

4.3.4.2 Network components and software

Protection against unauthorized access

The following solutions may be used to connect industrial networks to the intranet and Internet to protect against internal and external threats:

- Communication processors, such as the SIMATIC CP 1543-1
- SCALANCE X-300 and SCALANCE S - the data security components of the SIMATIC NET product family
- SOFTNET security client for use on PCs

Features

Both of these products have a wide variety of features, such as:

- Easy integration of existing networks without configuration, with integrated firewall.
- Segmenting in protected automation cells
- Authentication (identification) of the devices
- Encrypting the data traffic

4.3.4.3 Application example

Data security at the office and production levels

The following graphic contains an application example with protected areas at different levels of the company created using SCALANCE S and the security client. The protected areas are highlighted in light gray.

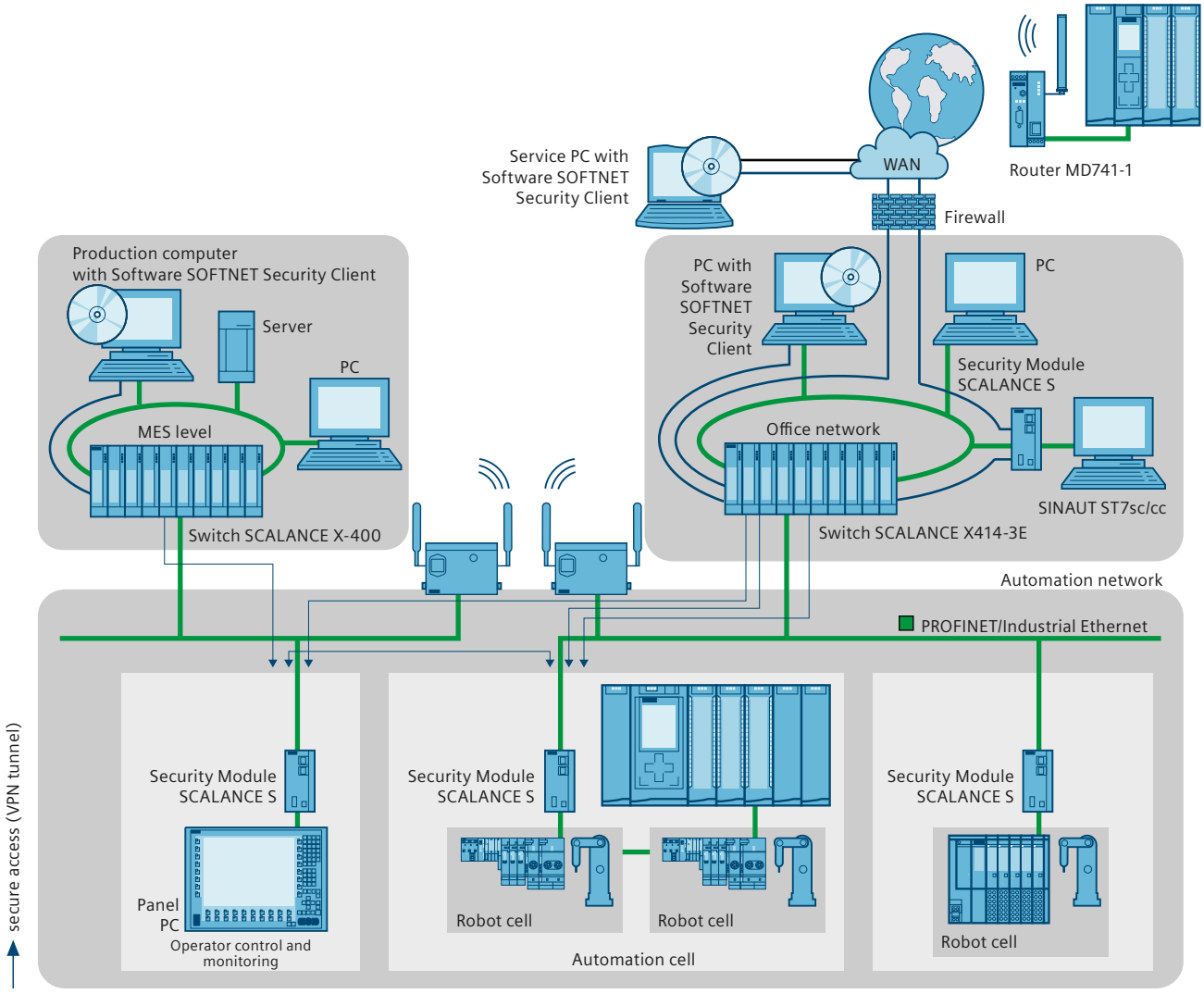


Figure 3-304 Network configuration with the SCALANCE S security module and the SOFTNET security client

Additional information

Additional information on the configuration of a security standard in PROFINET, is available:

- In the PROFINET security guideline. These guidelines can be found on the homepage of the PROFIBUS user organization on the Internet (http://www.profinet.com).
- In the Industrial Ethernet Security (https://support.industry.siemens.com/cs/ww/en/view/109742946) manual
- In the SCALANCE S and SOFTNET Security Client (http://support.automation.siemens.com/WW/view/en/21718449) manual

You can find general information on industrial security concepts, functions and news on the Industrial Security website (http://www.siemens.com/industrialsecurity).

Parameter assignment/addressing

5

To set up an automation system, you will need to configure, assign parameters and interlink the individual hardware components. In STEP 7, the work needed for this is undertaken in the device, topology and network view.

Configuring

"Configuring" is understood to mean arranging, setting and networking devices and modules within the device, topology or network view.

An I/O address is automatically assigned to each module. The I/O addresses can be subsequently modified.

The CPU compares the configuration preset in STEP 7 with the actual current configuration of the system. In this way, potential errors can be detected and reported straight away.

The exact procedure for configuring devices is described in detail in the STEP 7 online help.

Assigning parameters

"Assigning parameters" is understood to mean setting the properties of the components used. The settings for the hardware components and for data communication are configured at the same time.

In STEP 7, you can "assign parameters" for the following settings PROFINET:

- Device name and IP address parameters
- Port parameters
- Module properties / parameters

The parameters are loaded into the CPU and transferred to the corresponding modules when the CPU starts up. Modules are easy to replace from spare parts, as the parameters assigned for the SIMATIC CPUs are automatically loaded into the new module at each startup.

Adjusting the hardware to the project requirements

You need to configure hardware if you want to set up, expand or change an automation project. To do this, add hardware components to your structure, link these with existing components, and adapt the hardware properties to the tasks.

The properties of the automation systems and modules are preset such that in many cases they do not have to be assigned parameters again.

Parameter assignment is however needed in the following cases:

- You want to change the default parameter settings of a module.
- You want to use special functions.
- You want to configure communication connections.

5.1 Assigning an IO device to an IO controller

PROFINET IO System

A PROFINET IO system is comprised of a PROFINET IO controller and its assigned PROFINET IO devices. After these devices have been placed in the network or topology view, STEP 7 assigns default values for them. Initially, you only have to worry about the assignment of IO devices to an IO controller.

Requirement

- You are in the network view of STEP 7.
- A CPU has been placed (e.g., CPU 1516-3 PN/DP).
- An IO device has been placed (e.g., IM 155-6 PN ST).

Procedure

To assign IO devices to an IO controller, proceed as follows:

1. Place the pointer of the mouse over the interface of the IO device.
2. Press and hold down the left mouse button.
3. Move the pointer.

   The pointer now uses the networking symbol to indicate "Networking" mode. At the same time, you see the lock symbol on the pointer. The lock symbol disappears only when the pointer is over a valid target position.
4. Now move the pointer onto the interface of the IO controller. You can keep the left mouse button pressed or release it when performing this action.
5. Now release the left mouse button or press it again (depending on your previous action).

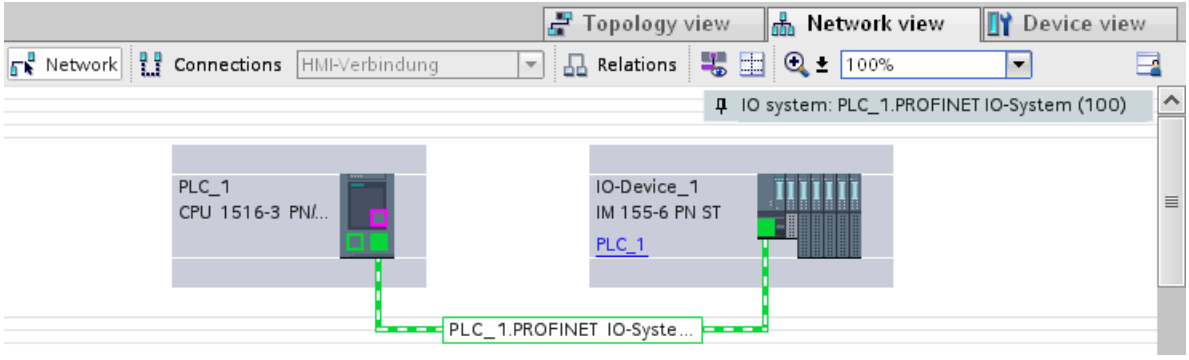


Figure 3-305 Assigning an IO device to an IO controller in the network view of STEP 7

Result

You have assigned an IO device to an IO controller.

Checking the assignment

You can find an overview of the communication relationships in the "IO communication" tab in the tabular area of the network view. This table is context-sensitive for selection in the graphic area:

- Selection of the interface shows the I/O communication of the respective interface.
- Selection of the CPU shows all I/O communication of the CPU (including PROFIBUS).
- Selection of the station (as in the above figure) interface shows the I/O communication of the complete station.

Information on S7-1500R/H

You can find the procedure for assigning an IO device with system redundancy S2 to the redundant S7-1500R/H system in section Assigning IO device to the redundant S7-1500R/H system (Page 337).

5.2 Device name and IP address

Introduction

In order that the PROFINET device can be addressed as node on PROFINET, the following are required:

- A unique PROFINET device name
- A unique IP address in the relevant IP subnet

STEP 7 assigns a device name during the arrangement of a PROFINET device in the hardware and network editor. The IP addresses are typically assigned automatically by STEP 7 and assigned to the devices based on the device name.

You can change the name and IP address manually.

In STEP 7

You can find the device name and the IP address under "Ethernet addresses" in the properties of the PROFINET interface in the Inspector window.

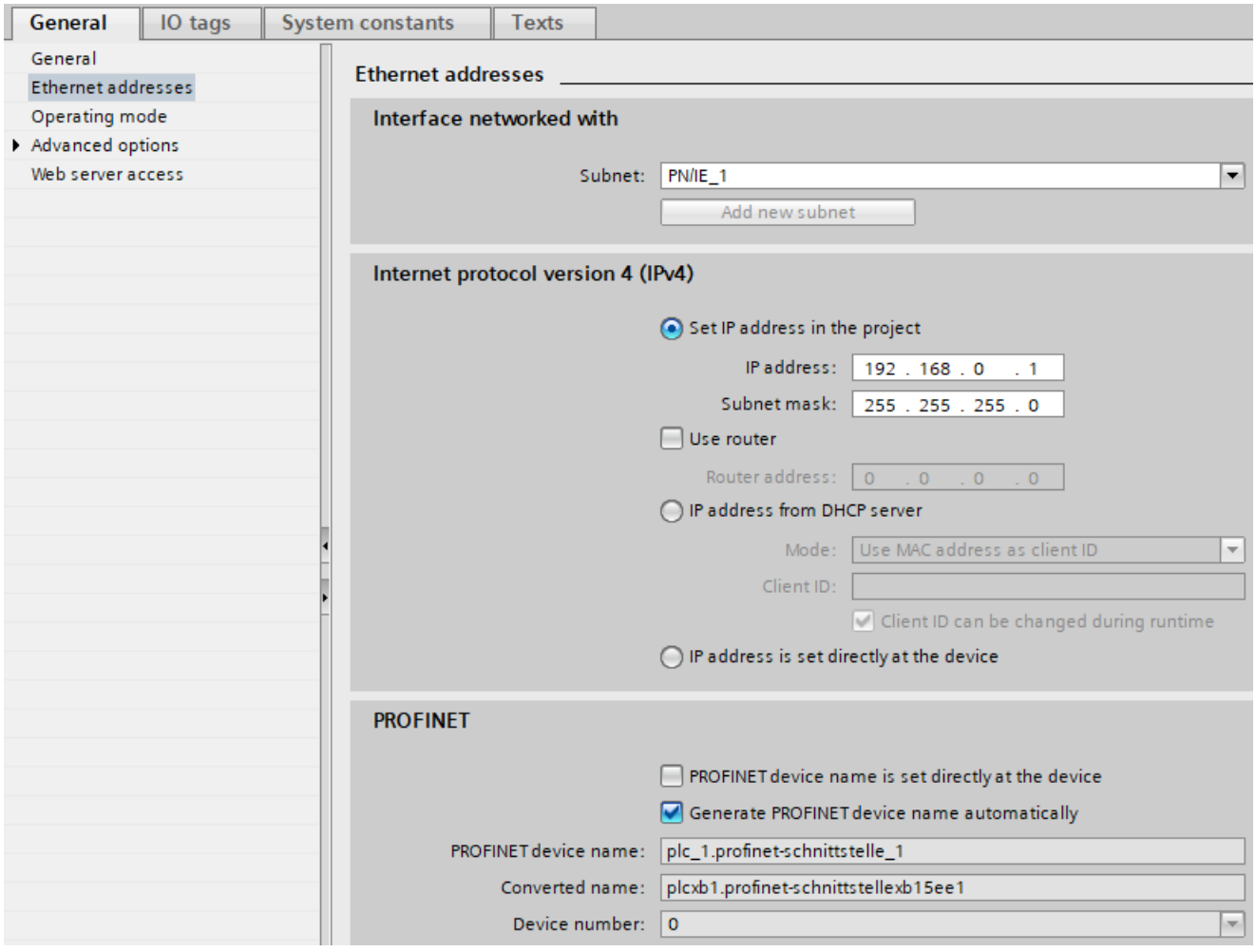


Figure 3-306 Device name and IP address in STEP 7

The function, the assignment and the changing of the device name and the IP address are described in the following sections.

5.2.1 Device name

Device names

Before an IO device can be addressed by an IO controller, it must have a device name. In PROFINET, this method was selected because it is simpler to work with names than with complex IP addresses.

In delivery state, an IO device does not have a device name. A device name must first be assigned before an IO device can be addressed by an IO controller, for example, for transferring configuration data during startup or for exchanging user data in cyclic mode. You assign the device names to the IO device, for example, with the programming device/PC.

With IO devices, the device name is stored directly by the IO devices, e.g. on removable media, the BusAdapter or directly in the interface module.

When a device is replaced by a device without removable medium, the IO controller assigns the device name based on topological configuration (see section Configuring topology (Page 74)).

Structured device names

The device name is automatically assigned by default for PROFINET devices when configured in STEP 7. The device names are formed from the name of the CPU or the name of the interface module. For devices with several PROFINET interfaces, the name of the interface is enhanced, for example, "plc_1.profinet-interface_2" or "io-device_1".

You can structure the device names using DNS conventions.

These conventions are defined by "Internationalizing Domain Names in Applications (IDNA). According to this, device names are written in lower case.

The "Domain Name System" (DNS) is a distributed database (http://iana.org), which manages the name space on the Internet. To structure the names, you use the dot ("."). The hierarchy is shown in ascending order from left to right.

...<Subdomain name>.<Domain name>.<Top-level domain name>

If the name is not DNS-compliant, the name will be converted by STEP 7, for example, to "plcxb1.profinet-schnittstellexb2022c" or "io-devicexb15b32".

Device number

In addition to the device name, STEP 7 also assigns a device number beginning with "1" when an IO device is allocated.

The device number is located in the Inspector window in the properties of the PROFINET interface, under "Ethernet addresses" in the area PROFINET.

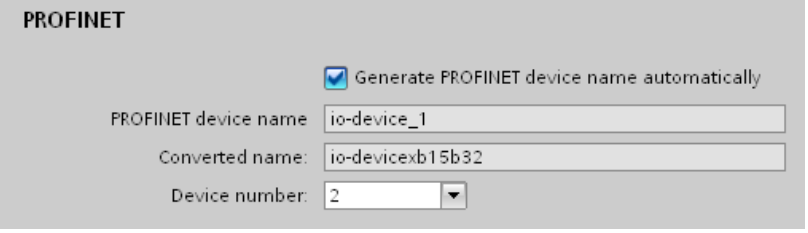


Figure 3-307 Device number

This device number can be used to identify an IO device in the user program (for example, with the instruction "LOG2GEO").

5.2.2 IP address

IP address

To allow a PROFINET device to be addressed as a device on Industrial Ethernet, this device also requires an IP address that is unique within the network. This applies to PROFINET devices that do not support PROFINET communication without an IP address.
For PROFINET devices that support PROFINET communication without an IP address, assigning an IP address is optional. Depending on whether other connections to this device require an IP address.

The IP addresses are typically assigned automatically by STEP 7 and assigned to the devices based on the device name. If it is a standalone network, you can apply the IP address and subnet mask suggested by STEP 7. If the network is part of an existing Ethernet company network, obtain the information from your network administrator.

Configuration of the IP address

In accordance with Internet Protocol version 4 (IPv4), the IP address is made up of four decimal numbers with a range of values from 0 through 255. The decimal numbers are separated by periods (for example, 192.162.0.0).

The IP address consists of the following:

- Address of the network
- Address of the device (PROFINET interface of the IO controller/IO device)

Generating IP addresses

You assign the IP addresses of the IO devices in STEP 7. The IO devices receive their IP addresses during parameter assignment by the IO controller.

In addition, for some IO devices (e.g., SCALANCE X, S7-300 CPs), it is possible not to obtain the IP address during startup of the IO controller, but rather to set it beforehand on the device (see Permitting changes to the device name and IP address directly on the device (Page 68)).

The IP addresses of the IO devices always have the same subnet mask as the IO controller and are assigned from the IP address of the IO controller in ascending order. The IP address can be changed manually, if necessary.

For devices with several PROFINET interfaces (e.g., CPU 1516-3 PN/DP), the IP addresses must be located in different subnets.

NOTE

Assignment of the IP address by a DHCP server

As of STEP 7 V17, you can select the option "IP address from DHCP server" for the PROFINET interface. With this option, the PROFINET interface is assigned an IP address by an DHCP server.

When you configure the option "IP address from DHCP server" for a PROFINET interface, this interface does no longer support the PROFINET IO functionality.

For more information on addressing by a DHCP server, please refer to the Communication (http://support.automation.siemens.com/WW/view/en/59192925) function manual.

Default router

The default router is used when data has to be forwarded via TCP/IP or UDP to a partner located outside the local network.

In STEP 7, the default router is named Router. For a CPU, activate the use of a router in the properties of a PROFINET interface. In the "Internet protocol version 4 (IPv4)" area, select the "Use router" check box. The check box is available for all PROFINET interfaces of the CPU in the respective properties. You can only configure one router for each CPU.
STEP 7 assigns the default router the IP address that was assigned to the PROFINET interface X1 of the CPU.

The router address that is set on the PROFINET interface of the IO controller is automatically transferred for the configured IO devices.

Subnet mask

The bits set in the subnet mask decide the part of the IP address that contains the address of the network.

In general, the following applies:

- The network address is obtained from the AND operation of the IP address and subnet mask.
- The device address is obtained from the AND NOT operation of the IP address and subnet mask.

Example of the subnet mask

Subnet mask: 255.255.0.0 (decimal) = 11111111.11111111.00000000.00000000 (binary)

IP address: 192.168.0.2 (decimal) = 11000000.10101000.00000000.00000010 (binary)

Meaning: The first 2 bytes of the IP address determine the network - i.e., 192.168. The last two bytes address the device, i.e. 0.2.

Relation between IP address and default subnet mask

An agreement exists relating to the assignment of IP address ranges and so-called "Default subnet masks". The first decimal number (from the left) in the IP address determines the structure of the default subnet mask with respect to the number of "1" values (binary) as follows:

IP address (decimal)	IP address (binary)	Address class	Default subnet mask
0 to 126	0xxxxxxx.xxxxxxxx....	A	255.0.0.0
128 to 191	10xxxxxx.xxxxxxxx...	B	255.255.0.0
192 to 223	110xxxxx.xxxxxxxx...	C	255.255.255.0

NOTE

Range of values for the first decimal point
A value between 224 and 255 is also possible for the first decimal number of the IP address (address class D etc.). However, this is not recommended because there is no address check for these values.

Masking other subnets

You can use the subnet mask to add further structures and form "private" subnets for a subnet that is assigned one of the address classes A, B or C. This is done by setting other, less significant bits of the subnet mask to "1". For each bit set to "1", the number of "private" networks doubles and the number of devices they contain is halved. Externally, the network continues to function as an individual network.

Example:

You have a subnet of address class B (for example, IP address 129.80.xxx.xxx) and change the default subnet mask as follows:

Masks	Decimal	Binary
Default subnet mask	255.255.0.0	11111111.11111111.00000000-.00000000
Subnet mask	255.255.128.0	11111111.11111111.10000000-.00000000

Result:

All devices with addresses from 129.80.001.000 to 129.80.127.254 are located in a subnet, all devices with addresses from 129.80.128.000 to 129.80.255.254 in a different subnet.

Reading out an IP address in the user program

You can read out the IP address of a PROFINET device in the user program of a S7-1500 CPU. You can find information in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/82947835).

5.2.3 Assigning a device name and IP address

Assigning an IP address and subnet mask for an IO controller for the first time

You have the following options:

- **Using a programming device or PC:**
  Connect your programming device/PC to the same network as the relevant PROFINET device. The interface of the programming device/PC must be set to TCP/IP mode. During the download, first of all display all available devices via the "Accessible devices" download dialog box. Select the target device via its MAC address and then assign its IP address before you download the hardware configuration including the configured IP address (IP address is saved retentively).
- **Using the display of a S7-1500 CPU:**
  The S7-1500 CPUs have a front cover with a display and operating keys. You can use this display to assign or change the IP address. To set the IP address, navigate on the display via the menu items "Settings" > "Addresses" > "X1 (IE/PN)" > "Parameters".
- **Using a memory card:**
  If your PROFINET device is equipped for a memory card (Micro Memory Card/SIMATIC memory card), plug this into your programming device/PC and save the hardware configuration together with the configured IP address on this memory card. Then plug the memory card into the PROFINET device. Once inserted, the PROFINET device automatically applies the IP address.
  If you have saved a configuration to the memory card with the "IP address is set directly at the device" option, you must assign the IP address using a different method after inserting the memory card (see section Permitting changes to the device name and IP address directly on the device (Page 68)).

Assigning device names and IP address for "Device replacement without exchangeable medium/programming device"

All PROFINET IO devices are assigned the device name via the topology. To do this, the IO device must be in the delivery state or reset to the factory settings. The IO controller can identify the device without a name from the neighborhood relationships specified by the target topology and the actual neighborhood relationships determined by the real PROFINET devices. The IO controller then assigns the PROFINET device the configured name and incorporates the PROFINET device in the user data traffic. (See also Device replacement without exchangeable medium (Page 257)).

IP address assignment when replacing IO devices with exchangeable mediumPG

The following is contained on the memory card of the programmable logic controller:

- On the IO controller: Device name and IP address
- On the IO device: Device name

When you remove the memory card from a PROFINET device and insert it in another PROFINET device with exchangeable medium (e.g., ET 200S), device-specific information and the device name are loaded to the device.

If an IO device has to be replaced in its entirety due to a device or module defect, the IO controller automatically assigns parameters and configures the replaced device or module.

The cyclic exchange of user data is then restarted. In addition to this, before the power ON of the IO device, the memory card with the valid name must be removed from the faulty IO device and added to the replaced device.

In the event of an error in the PROFINET device, the memory card allows you to replace a module without a programming device/PC. You can also transfer the device data directly from the programming device/PC to the memory card.

Procedure: Changing the device name using properties of the PROFINET interface

You can change the PROFINET name via the properties of the PROFINET interface. This is useful when the PROFINET device has not received its previous name from the automatic generation, for example, in the case of a migration.

1. In the network or device view of the STEP 7 hardware and network editor, select the PROFINET interface of a PROFINET device.
2. In the Inspector window, go to "Ethernet addresses" in the PROFINET area.
3. Clear the "Generate PROFINET device name automatically" check box.
4. Enter the new PROFINET device name in the relevant field.

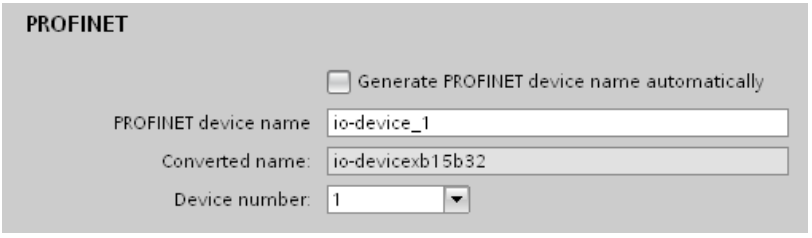


Figure 3-308 Changing the device name of a PROFINET device in the properties

Alternative procedure: Changing the device name of a PROFINET device in the network view

Requirement: The "Generate PROFINET device name automatically" check box is selected.

1. In STEP 7, select the "Network overview" tab in the tabular area of the network view.
2. In the "Device" column, overwrite the name in the row of the relevant PROFINET device.

The name is also changed accordingly in the graphic area of the network view.

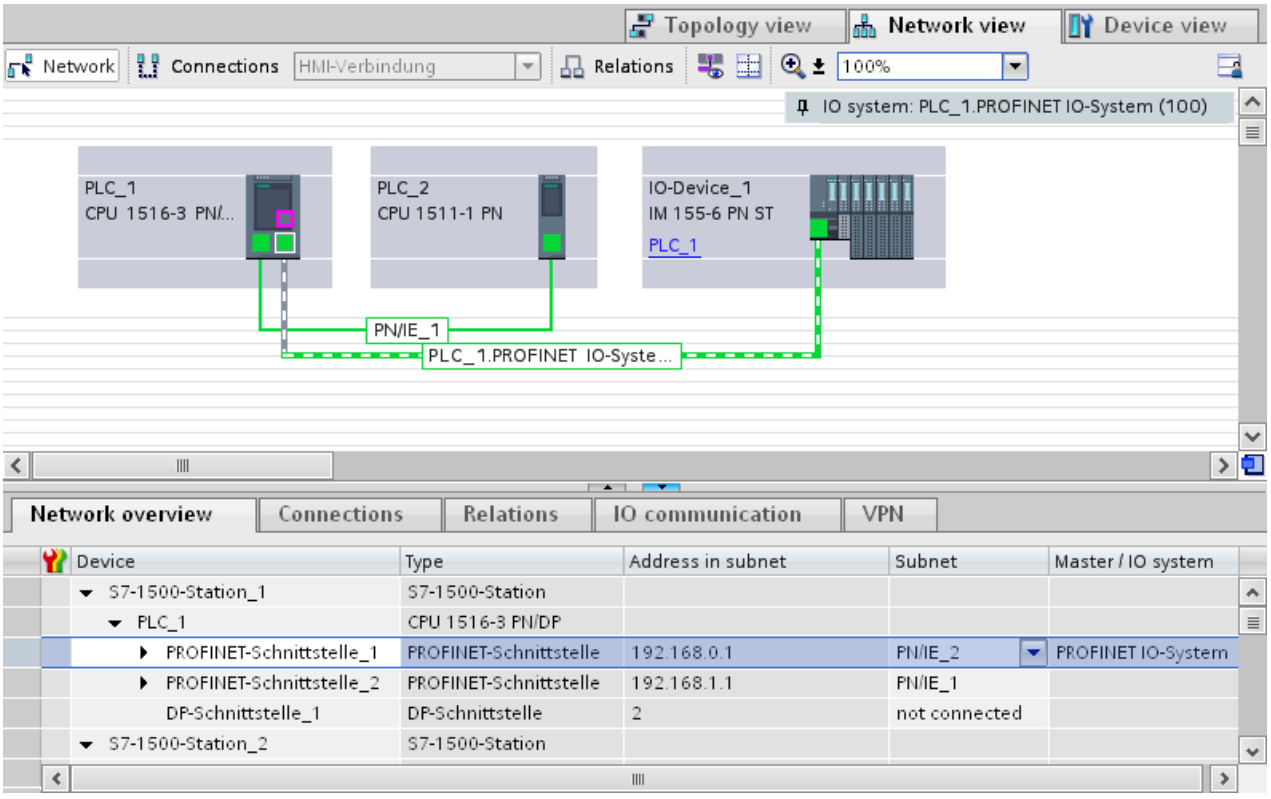


Figure 3-309 Changing the device name of a PROFINET device in STEP 7

Procedure: Changing the IP address

To change the IP address, follow these steps:

1. In the network or device view of the STEP 7 hardware and network editor, select the PROFINET interface of a PROFINET device.
2. In the Inspector window, go to "Ethernet addresses" in the "IP protocol" area.
3. Check that the option "Set IP address in the project" is selected.

4. Enter the new IP address in the relevant field.

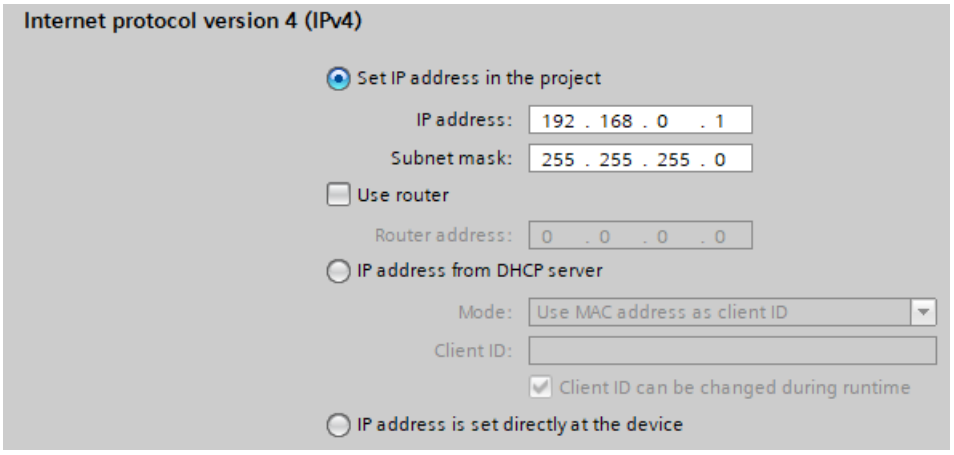


Figure 3-310 Changing the IP address of a PROFINET device in STEP 7

Downloading configured device name to IO device

To load the configured device names to the IO device, follow these steps:

1. Connect your programming device/PC to the same network as the relevant IO device. The interface of the programming device/PC must be set to TCP/IP mode.
2. In STEP 7, select the relevant IO device in the "Accessible devices" dialog based on the MAC address.
3. Click "Assign name" to download the configured device name to the IO device.
   The IO controller recognizes the IO device automatically by its device name and automatically assigns the configured IP address to it.

Identification of the PROFINET device

To clearly identify a device from several identical devices in a control cabinet, for example, you can flash the link LED of the PROFINET device.

To do this, select the menu command **Online > Accessible devices...** in STEP 7. In the "Accessible devices" dialog, set the "PG/PC" interface by means of which you are connected to the devices. STEP 7 now automatically searches for the accessible devices and displays them in the "Accessible devices in target subnet" table. Select the desired PROFINET device and click on the "Flash LED" button. The PROFINET device is identified based on its MAC address.

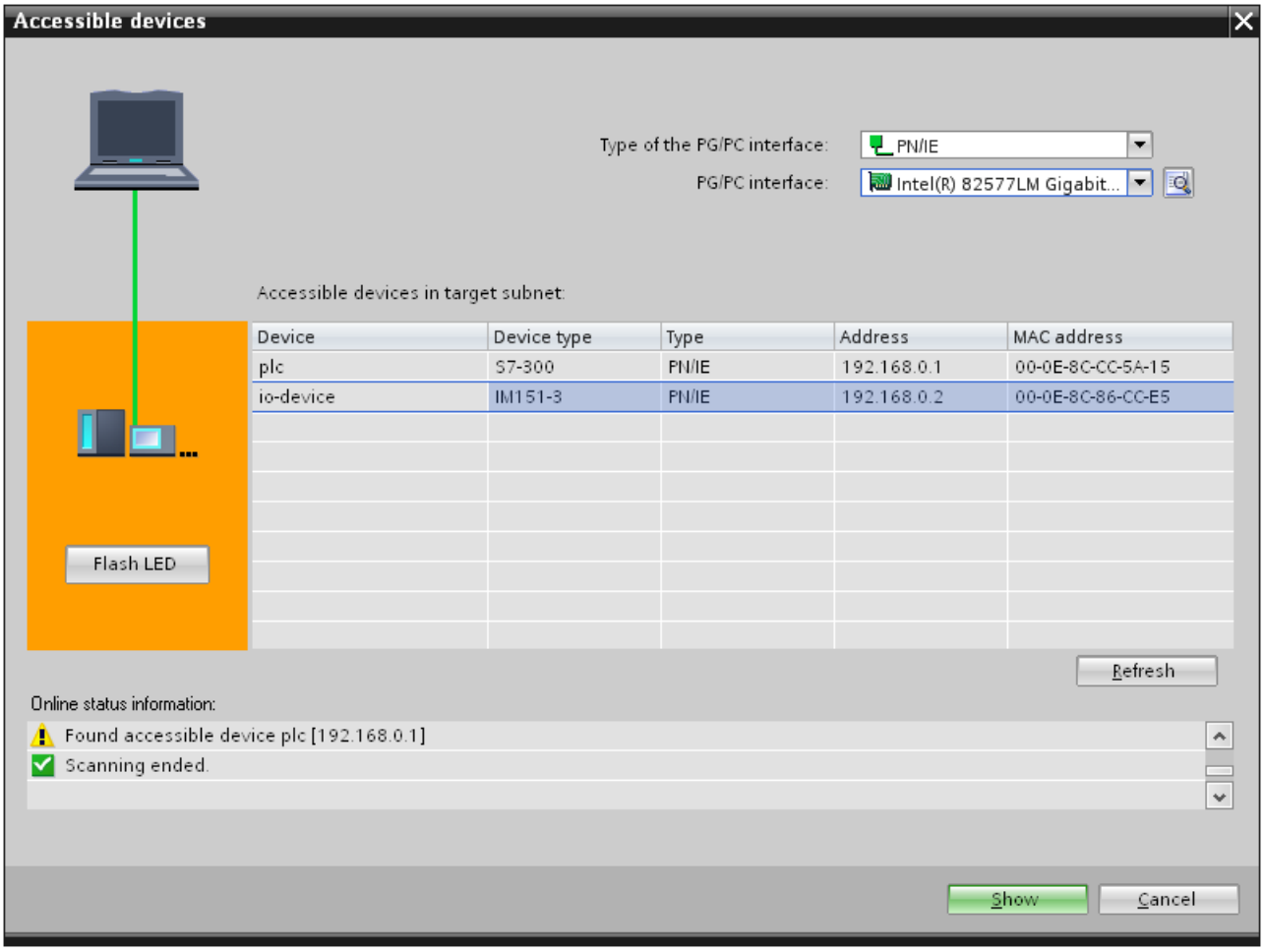


Figure 3-311 "Accessible devices" dialog

Using an different way to assign IP addresses for IO devices

Various IO devices, for example, SCALANCE X,S7-300 CPs, support the option of not having the IP addresses assigned by the IO controller during startup. In this case, the IP address is assigned in a different way. For additional information, refer to the manual of the respective PROFINET device of the SIMATIC device family.

More information

You can find a detailed description of the operation and functions of the display of the S7-1500 CPUs in the system manual S7-1500, ET 200MP (http://support.automation.siemens.com/WW/view/en/59191792).

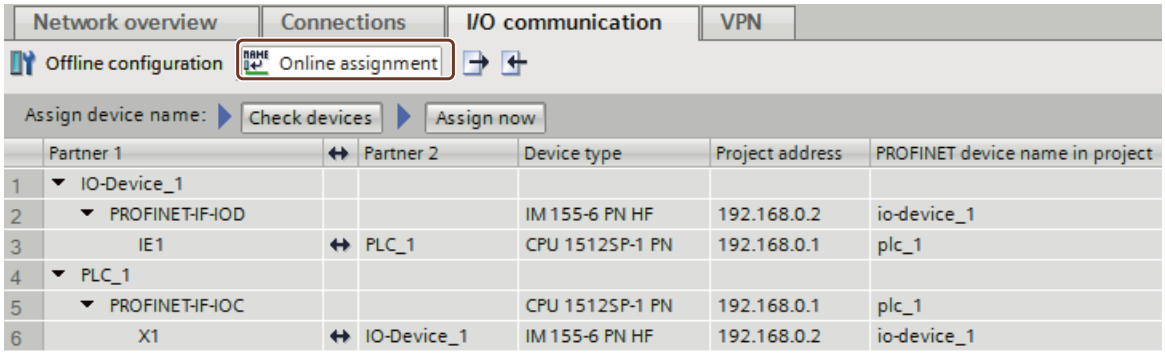
5.2.4 Assign device name via communication table

Introduction

You can assign the device names of PROFINET IO devices configured offline to the devices online. You can do this in the table area of the network view in the table "I/O communication". You can also assign the device names to several devices at the same time.

"Online assignment" tab

In the I/O communication table, you will find the tabs "Offline configuration" and "Online assignment". In the "Online assignment" tab, you can assign the PROFINET device names that were assigned offline to the corresponding IO devices online. To do this, use the buttons "Check devices" and "Assign now".



	Partner 1		Partner 2	Device type	Project address	PROFINET device name in project
1	IO-Device_1					
2	PROFINET-IF-IOD			IM 155-6 PN HF	192.168.0.2	io-device_1
3	IE1	↔	PLC_1	CPU 1512SP-1 PN	192.168.0.1	plc_1
4	PLC_1					
5	PROFINET-IF-IOC			CPU 1512SP-1 PN	192.168.0.1	plc_1
6	X1	↔	IO-Device_1	IM 155-6 PN HF	192.168.0.2	io-device_1

Figure 3-312 Assign device name via communication table

The objects displayed in the table of the "Online assignment" tab depend on the setting of the filter function. If only selected objects should be displayed, only objects of the corresponding context are displayed depending on the selection in the network view.

- PROFINET subnet: All connected devices and their PROFINET interfaces
- IO system All devices involved and their PROFINET interfaces
- Sync domain: All devices involved and their PROFINET interfaces
- Devices: The device and any existing PROFINET interfaces
- Other subnets or interfaces such as MPI or PROFIBUS are not displayed

If the display is set for all devices using the filter function, all devices are displayed that have a PROFINET interface, regardless of whether they are connected via a PROFINET subnet or are part of an IO system. Devices without a PROFINET interface, for example only with a DP or MPI interface, are not displayed.

General procedure

To assign PROFINET device names, you must first detect the IO devices available online. With this procedure, it matters whether the MAC addresses are known or unknown. This results in a general procedure in two steps:

1. Detecting the IO devices available online
2. Assigning configured PROFINET device names to the IO devices available online

Requirements

- You are in the network view.
- There is an online connection to the devices.

Procedure (step 1)

To detect IO devices available online from the I/O communication table, follow these steps:

1. Optional: Entered known MAC addresses in the "MAC address" column. After every valid entry, the check box under "Assign device" is selected for the relevant row.

   NOTE

   You can enter, insert or import the MAC address in different formats. The correct format is automatically entered in the cell. The following entries are supported and then converted to the required format:

   – "08:00:06:BA:1F:20"
   – "08 00 06 BA 1F 20"
   – "080006BA1F20"

   The formats used in the example are automatically converted to "08-00-06-BA-1F-20".

2. Click "Check devices" to start the check of the IO devices available online.
3. Set the PG/PC interface in the dialog window and click "Start".

Intermediate result

After the check, the result is displayed for every device in the table. Online data found is automatically entered in the table and the check box "Assign device" is set to "checked" in the rows in which a MAC address was entered or found online. The result of the check is shown as an icon in the "Status" column.

Status	Meaning
	Matching device and compatible type
	Matching device and incompatible type
	Non-matching device
	Device cannot be reached (with a known MAC address)
	Ready for assignment (with known MAC address)

NOTE

The icon "Ready for assignment" appears when a MAC address exists and matching device data was found, but no PROFINET device name was found online.

You can update the data of the detected devices again via their MAC addresses at any time. To do this, you specify the MAC address and the status of the device is displayed immediately without having to re-detect the device.

Procedure (step 2)

All PROFINET device names configured offline will be assigned to the devices available online in a bulk operation.

1. Click the "Assign now" button.

   NOTE

   The bulk operation cannot be reversed. A message to this effect appears in a dialog window.

2. Click "Start" in the dialog window to start the assignment of the PROFINET device names.

Result

The PROFINET device names configured offline will be assigned to the devices available online. This relates to devices in whose row the check box under "Assign device" is selected, that have a MAC address and have the status "Ready for assignment".

Importing and exporting data

Using the import and export button, you can import or export the data of the I/O communication table for the online assignment:

- When you export, the currently displayed data of the table is exported to a CSV file. Using the filter function of the table, you can select which data will be exported.
- When you import, the data of the CSV file is written to the table. If there are conflicts with values already existing in the table, you can decide whether the data should be overwritten or whether the import needs to be stopped.

5.2.5 Permitting changes to the device name and IP address directly on the device

Introduction

Machines are frequently commissioned on site or integrated into the existing infrastructure without STEP 7. You can find typical applications in all areas of the series machine building. Alternative means for assigning the IP address are available for this.

Procedure

1. In the network or device view of the STEP 7 Hardware and Network editor, select the PROFINET interface of an IO controller.
2. Navigate in the Inspector window to "Ethernet addresses".
3. Select the "IP address is set directly at the device" option in the "IP protocol" area.

4. In the "PROFINET" area, select the " PROFINET device name is set directly at the device" check box.

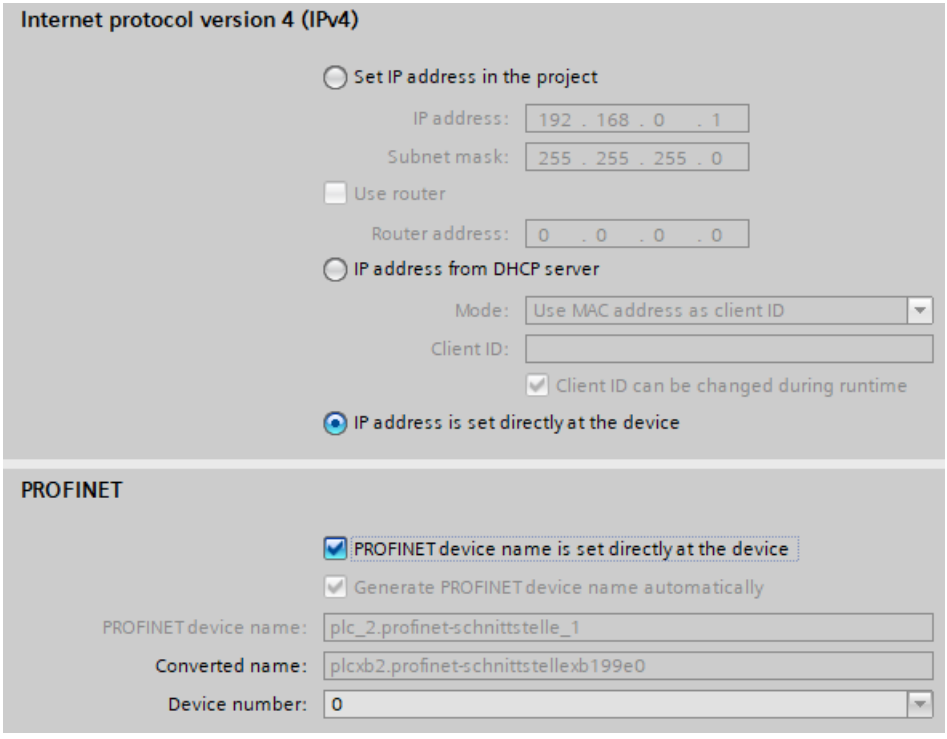


Figure 3-313 Setting the device name and IP address on the device

NOTE

Gateway

When you operate a PROFINET device with the option "Allow adaption of the device name/IP address directly on device", you cannot use this PROFINET device as gateway for S7 routing.

Options for assigning IP addresses and device names

Apart from the known address and device name assignment in the "Ethernet addresses" section of the Inspector window, there are other ways in which the IP address and name can be assigned:

- Assigning by means of the user program with the instruction "T_CONFIG"
- Assignment when downloading the configuration to the target system via the "Extended download to device" dialog box.
- Assignment via the Primary Setup Tool (PST)
- Assignment via the PRONETA ("PROFINET network analysis") commissioning and diagnostics tool
- Assignment via the SIMATIC Automation Tool

Additional information

For information on the "T_CONFIG" instruction and on downloading to the target system, refer to the STEP 7 online help.

A free Download (https://support.industry.siemens.com/cs/ww/en/view/109776941) of the Primary Setup Tool (PST) can be found on the Internet. On this Internet page, you will also find a list of devices for which the PST is approved.

5.3 Configuring an IO device through hardware detection

Introduction

As of STEP 7 V15, you have the possibility to detect a real existing IO device and to import it into your project.

You find the IO device in STEP 7 through the "Hardware detection" function. A detected device can be imported into your project. STEP 7 inserts the IO device with all the modules and submodules.

Requirements

- STEP 7 (TIA Portal) as of V15
- It must be possible to technically access the IO device via IP

Procedure

To detect one or more existing IO devices in STEP 7 and add them to the project, follow these steps:

1. In STEP 7, navigate to "Online" > "Hardware detection".
2. Click "PROFINET devices from network...".
   STEP 7 opens the "Hardware detection of PROFINET devices" window.
3. Select the interface of your programming device at "PG/PC interface:".
4. Click "Start search".
   STEP 7 begins with the hardware detection. When the hardware detection is completed, STEP 7 displays the detected IO devices.
5. Select the IO devices that you want to add to the project by clicking the corresponding check box before the IO device.
6. Click "Add devices".
   After a brief moment, a window is opens to report about the success or failure of the hardware detection.

Result of the hardware detection

If the hardware detection is successful, STEP 7 inserts the IO device with all the modules and submodules into the project.

An IO device configured via hardware detection responds as follows:

- Modules configured through the "Hardware detection" are configured as if they have been inserted from the catalog.
- MAC address: STEP 7 imports the MAC address of the detected IO device into the project.
- IP settings:
  - If the detected IO device already has an IP address, STEP 7 imports the IP address into the project.
  - If the detected IO device does not have an IP address, STEP 7 automatically assigns an IP address in the project.

  PROFINET device name:
  - If the detected IO device already has a PROFINET device name, STEP 7 imports the PROFINET device name into the project.
  - If the detected IO device does not have a PROFINET device name, STEP 7 automatically assigns a PROFINET device name in the project.
- IO devices configured through "Hardware detection" have neither an IP subnet nor an IO controller assigned.

5.4 Specifying the router for a PROFINET IO device

Introduction

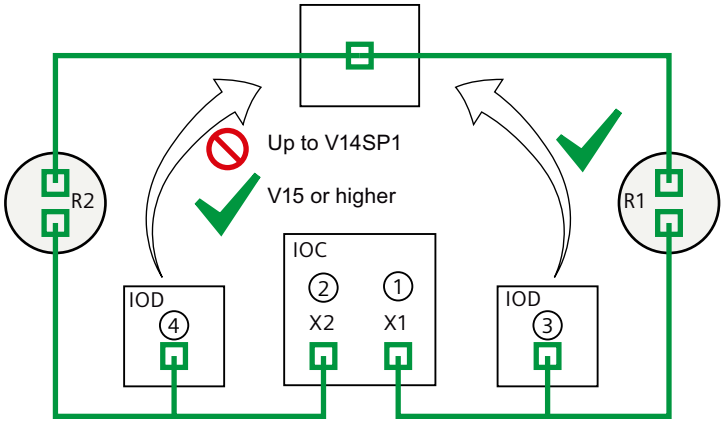
You always require a router (also referred to as a "Standard Gateway") when the PROFINET device has to communicate with a node whose IP addresses lie outside the own IP subnet. If the PROFINET device sends an IP packet to an IP address outside its own IP subnet, the IP packet first goes to the configured router. The router in turn checks the IP address. If this lies outside its own subnet, the router passes the IP packet on to the next router. The IP packet is routed to the next router until it has reached the target address.

Like all S7-1500 CPUs, S7-1500 CPUs with several PROFINET interfaces provide the possibility to configure the IP address of a router. However, there is the restriction that you can only enter the IP address of a router at a PROFINET interface.

You cannot configure an IP address of a router for the other PROFINET interfaces of the CPU. IO devices that are connected to this PROFINET interface adopt this setting. Up to and including STEP 7 V14 SP1, these IO devices did not have any possibility to reach devices in a different IP subnet.

As of STEP 7 V15, you have the possibility to assign the address of a router for an IO device independent of the setting of the IO controller. You can now, for example, set a router address at the IO device in the following cases as well:

- You have not set an IP address of a router for the interface of the associated IO controller.
- You have already set a router address for a different interface in the CPU.



① Router R1 configured at PROFINET X1

② If a router is configured at X1, you cannot configure a router at X2.

③ Because a router is configured at X1, the IO device adopts the IP address of the router R1. The IO device can be reached from a different IP subnet.

④ As of STEP 7 V15, you set the IP address of the router R2 at the IO device irrespective of the setting at the interface X2. The IO device can be reached from a different IP subnet.

Figure 3-314 Specifying the router for an IO device

Further information about the "User router" setting

You have the possibility to configure the use of a router including IP address of the router in the "IP protocol" section of the settings for the PROFINET interface (Ethernet addresses).

Rules

Observe the following rules if you want to configure a router for the PROFINET interface of an IO controller:

- A PROFINET IO device supports exactly one router, irrespective of the number of interfaces.
- You can configure a router for exactly one PROFINET interface. All IO devices that are assigned to the PROFINET interface adopt the configured router from the IO controller.
- You cannot configure a router for the further PROFINET interfaces of the CPU. The further PROFINET interfaces take on the IP address "0.0.0.0" as the router and pass it on to their IO devices.

As of STEP 7 V15, you can configure the use of a router for an IO device. This allows the IO device to communicate with a node outside its own IP subnet, irrespective of the setting of the PROFINET interface of the IO controller.

Configuration example: Configuring a router for an IO device

The following example shows a configuration in which you configure a router at the IO device so that the IO device reaches IP addresses in the higher-level network.

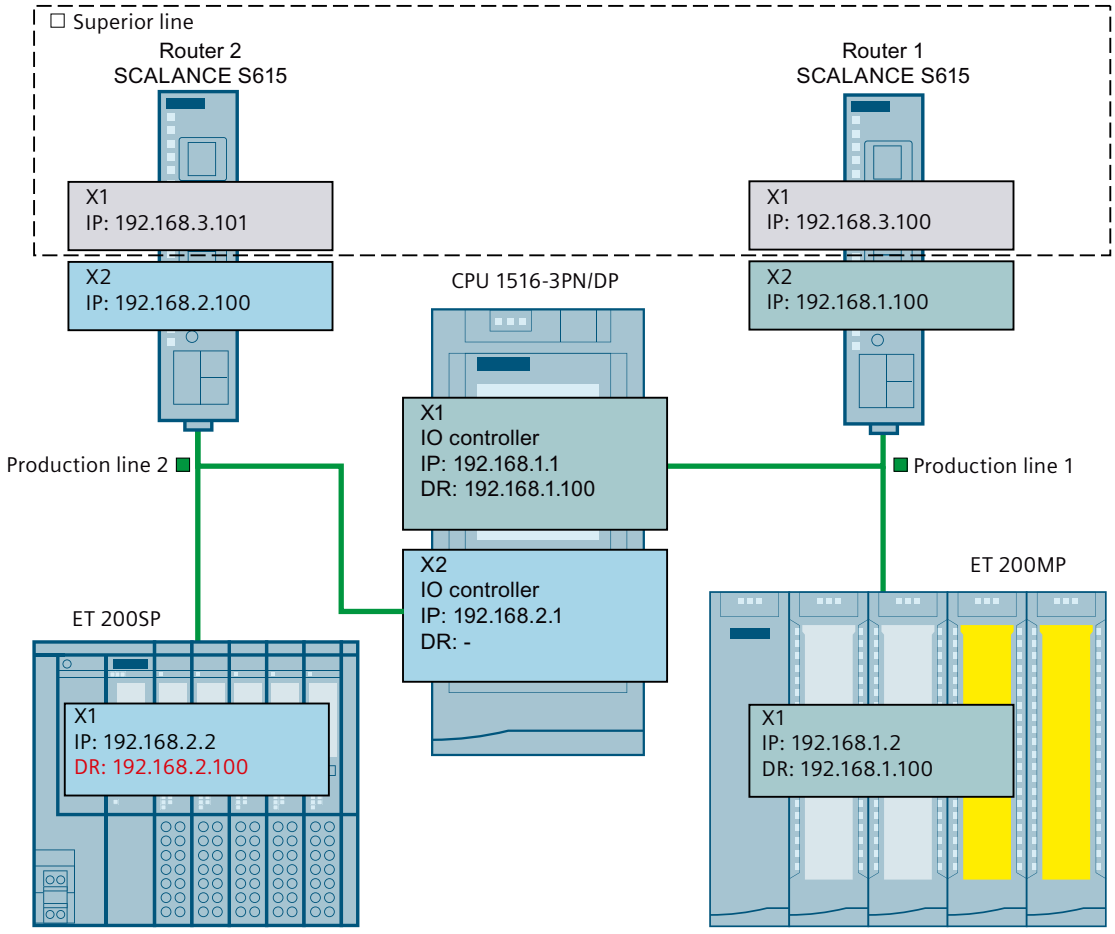


Figure 3-315 Configuration example: Configuring a router for an IO device

You have a CPU 1516-3PN/DP. The two PROFINET interfaces X1 and X2 of the CPU work in the "IO controller" operating mode. The PROFINET interface X1 is connected with the subnet "Production line 1". PROFINET interface X2 is connected with the subnet "Production line 2". The two subnets "Production line 1" and "Production line 2" are each connected via a router with the higher-level network "Superior line".

For PROFINET X1, you configure the router "Router 1" with the IP address 192.168.1.100.

The IO device (ET 200SP) in the "Production line 1" subnet adopts the router from the IO controller.

You cannot configure a router for the PROFINET interface X2 because you have already configured a router for the PROFINET interface X1 of the CPU.

No router is transferred by the PROFINET interface X2 to the IO device in the subnet "Production line 2".

In order for the IO device in the subnet "Production line 2" to reach nodes in the higher-level "Superior line", configure the router "Router 2" with the IP address 192.168.2.100 for the IO device.

Configuring the router for the IO controller

Requirements: You use the "Set IP address in the project" option for the PROFINET interface.

Follow these steps to configure a router for the IO controller in STEP 7:

1. In the network view of STEP 7, select the PROFINET interface of the IO controller.
2. In the Inspector window, navigate to "Properties" > "General" > "Ethernet addresses".
3. Select the "Use router" check box in the "IP protocol" field.
4. Enter the IP address of the router at "Router address".

Configuring a router for an IO device

Requirements:

- STEP 7 as of V15
- CPU 1500 as of firmware version V2.5
- IO device is assigned to the PROFINET interface of an IO controller. The PROFINET interface of the IO controller uses the "Set IP address in the project" option.

Follow these steps to configure a router for the IO device in STEP 7:

1. In the network view of STEP 7, select the PROFINET interface of the IO device.
2. In the Inspector window, navigate to "Properties" > "General" > "Ethernet addresses".
3. Clear the "Synchronize router settings with IO controller" check box.
4. Select the "Use router" check box.
5. Enter the IP address of the router at "Router address".

5.5 Configuring topology

Introduction

If an IO device is assigned to an IO controller, this does not yet specify how the ports are connected to each other.

A port interconnection is not required to use RT, but it provides the following advantages:

- A set topology is assigned with the port interconnection. Based on an online-offline comparison, it is possible to conduct a set-actual comparison with all devices that support this function.
- The "Device replacement without exchangeable medium" function can be used.

A port interconnection is an essential requirement for using IRT.

An overview of various options for setting up a PROFINET network is given below.

Line



All the communication devices are connected in a linear bus topology.

In PROFINET, the linear bus topology is implemented with switches that are already integrated into the PROFINET devices. Therefore, the linear bus topology at PROFINET is merely a special form of tree / star topology.

If a link element (switch, for example) fails, communication across the failed link element is no longer possible. The network is then divided into 2 subsegments.

Linear bus topology structures require the least cabling.

Star



If you connect communication devices to a switch with more than two PROFINET ports, you automatically create a star network topology.

If an individual PROFINET device fails, this does not automatically lead to failure of the entire network, in contrast to other structures. It is only if a switch fails that part of the communication network will fail as well

Tree



If you interconnect several star structures, you obtain a tree network topology.

Ring



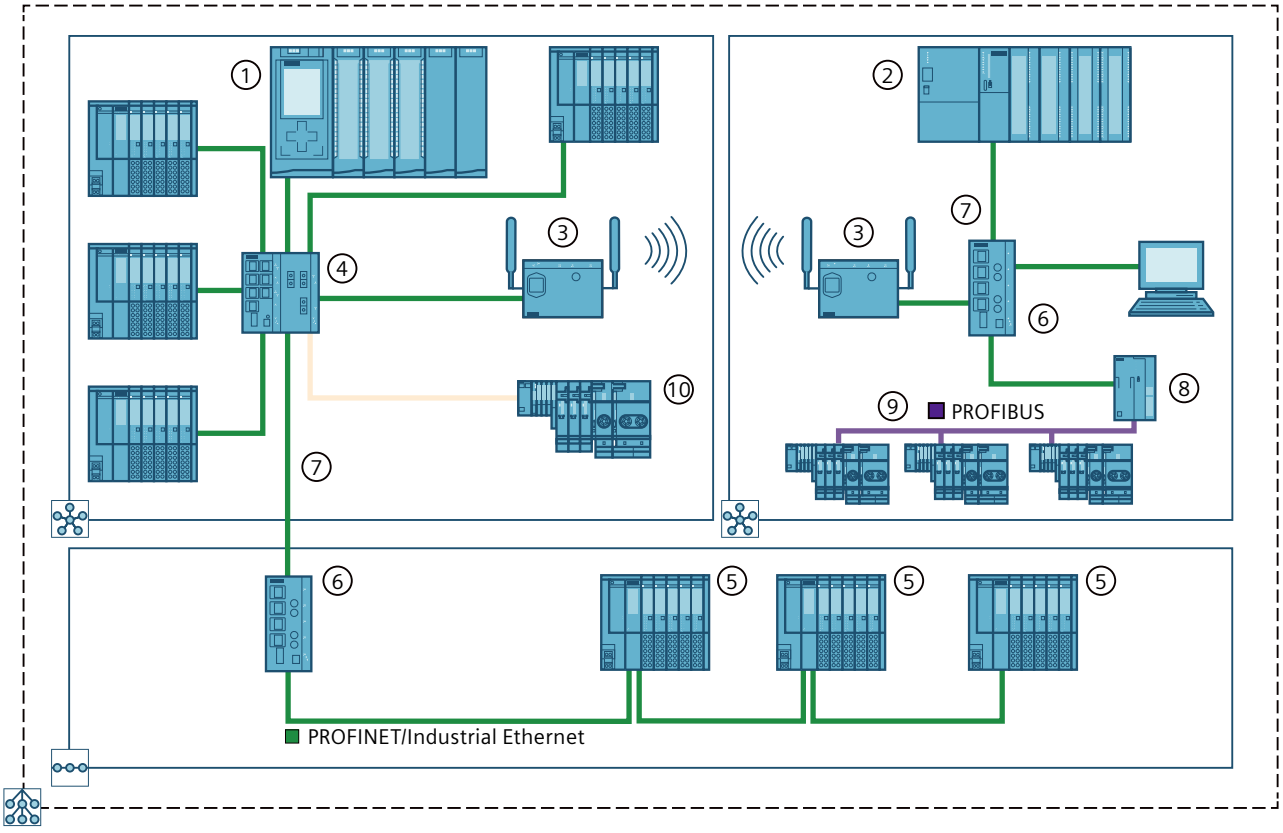
In order to increase the availability of a network, use ring structures. In principle, a linear bus topology is connected to a ring through a so-called redundancy manager.

The task of the redundancy manager is managed by an external switch SCALANCE X, a CPU that supports the Media Redundancy Protocol MRP (e.g., CPU 1516-3 PN/DP) or a CP (e.g., CP 343-1 Lean).

If there is a break in the network, the redundancy manager ensures that the data is redirected over an alternative network connection in the ring.

Example for topology

The following example shows a combination of different topologies.



Number	Meaning
①	S7-1500 as IO controller
②	S7-300 as IO controller
③	Industrial WLAN with SCALANCE W
④	SCALANCE X 307-3 with seven electrical and three optical ports
⑤	ET 200SP with integrated 2-port switch
⑥	SCALANCE X 204 with four electrical ports
⑦	PROFINET/Industrial Ethernet
⑧	IE/PB-Link PN IO
⑨	PROFIBUS DP
⑩	ET 200S with two optical ports
	Star topology
	Linear bus topology
	The combination of topology forms results in a tree topology.

Figure 3-316 Combined topology

Additional information

Observe the PROFINET Installation Guideline (http://www.profibus.com/nc/download/installation-guide/downloads/profinet-installation-guide/display/) of the PROFIBUS User Organization when planning your PROFINET topology.

For more detailed information, see the SIMATIC NET Twisted Pair and Fiber Optic Networks (http://support.automation.siemens.com/WW/view/en/8763736) manual.

You can find basic information in the Communication with SIMATIC (http://support.automation.siemens.com/WW/view/en/1254686) manual.

5.5.1 Topology view in STEP 7

Introduction

The topology view is one of three working areas of the hardware and network editor. You undertake the following tasks here:

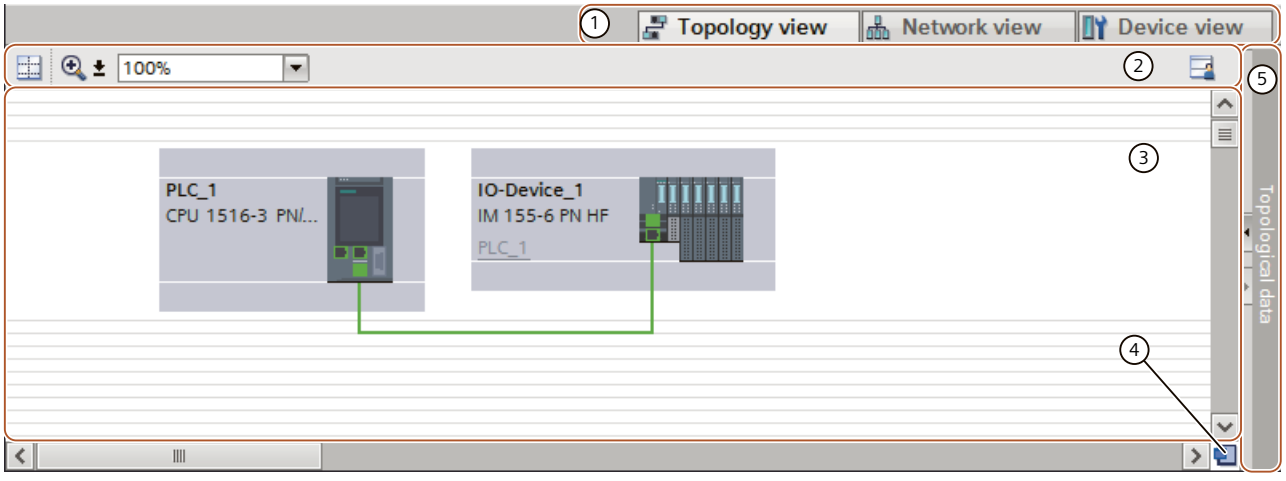
- Displaying the Ethernet topology
- Configuring the Ethernet topology
- Identify and minimize differences between the set and actual topology (online)

The topology view in STEP 7 consists of a graphic area and a table area.

Graphic area

The graphic area of the topology view displays PROFINET devices with their appropriate ports and port connections. Here you can add more PROFINET devices.

The following figure shows the graphic area of the topology view.



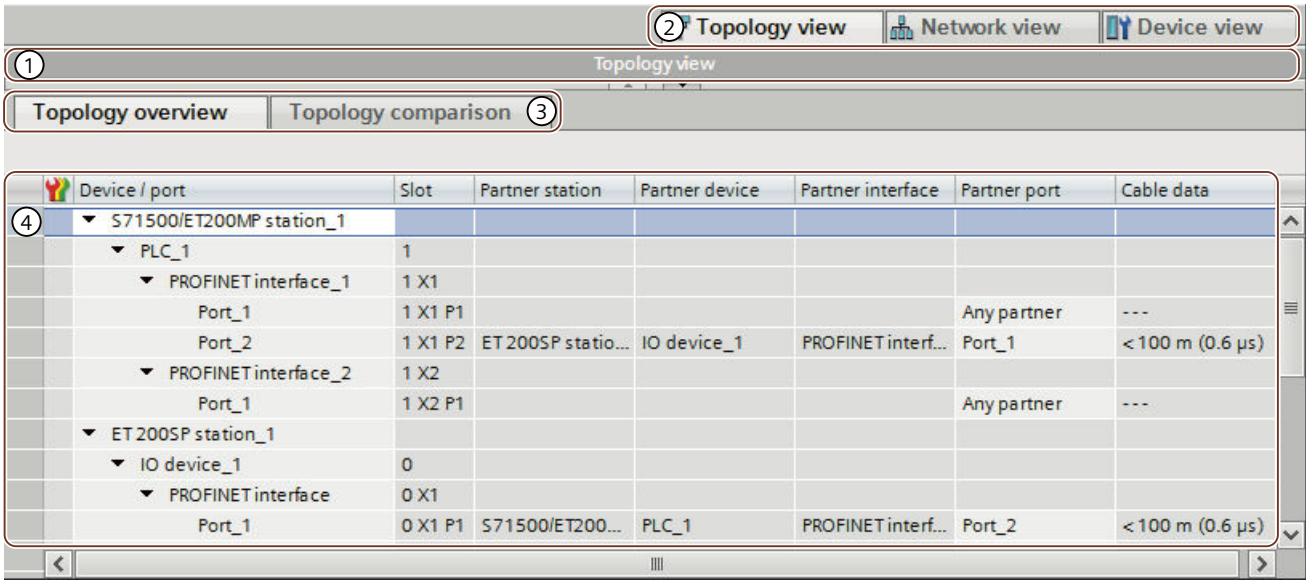
① Selector: Device view/Network view/Topology view
② Toolbar
③ Graphic area of the topology view
④ Overview navigation
⑤ Selector for the table area of the topology view

Figure 3-317 Graphic area of the topology view

Overview navigation
Click in the overview navigation to obtain an overview of the created objects in the graphic area. By holding down the mouse button, you can quickly navigate to the desired objects and display them in the graphic area.

Table area

- Topology overview: This displays the Ethernet or PROFINET devices with their appropriate ports and port connections in a table. This table corresponds to the network overview table in the network view.
- Topology comparison: Here you can import devices and port interconnections automatically through offline/online comparison or extended Offline/Online comparison into STEP 7.



① Selector for the graphic area of the topology view
② Selector: Device view/Network view/Topology view
③ Selector: Topology overview/Topology comparison
④ Table area of the topology view

Figure 3-318 Table area of the topology view

5.5.2 Interconnecting ports in the topology view

Requirement

You are in the graphic view of the topology view.

Procedure

To interconnect ports in the topology view, follow these steps:

1. Place the pointer of the mouse on the port you want to interconnect.
2. Press and hold down the left mouse button.
3. Move the pointer.
   The pointer now uses the networking symbol to indicate "Interconnecting" mode. At the same time, you see the lock symbol on the pointer. The lock symbol disappears only when the pointer is over a valid target position.
4. Now drag the pointer to the target port. You can keep the left mouse button pressed or release it when performing this action.
5. Now release the left mouse button or press it again (depending on your previous action).

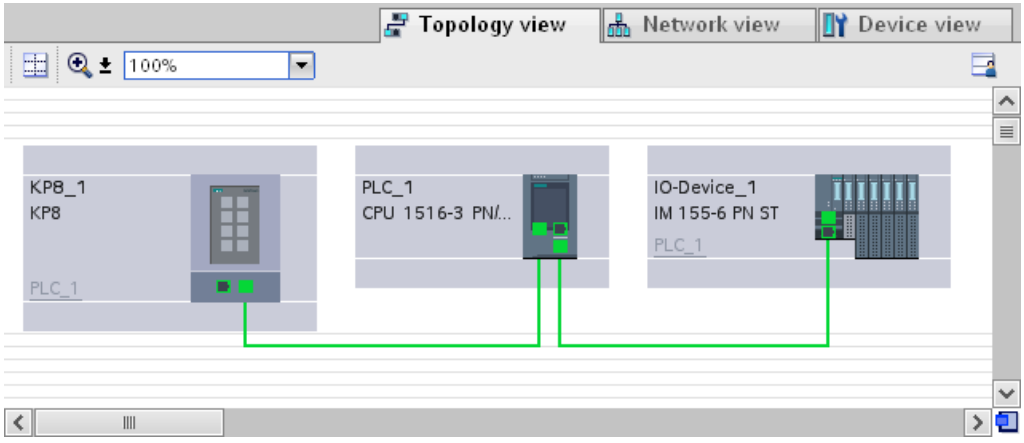


Figure 3-319 Interconnecting ports in the topology view

Result

You have created a port interconnection.

5.5.3 Interconnecting ports - Inspector window

Interconnecting ports in the Inspector window

To interconnect ports, follow these steps:

1. In the device or network view, select the PROFINET device or PROFINET interface.
2. In the Inspector window, navigate to the port property "Port interconnection".
   When the PROFINET interface is selected, you can find this setting in the Inspector window as follows: "Properties > General > Advanced Options > Port [...] > Port Interconnection."
3. In the "Local port" section, you can find the settings at the local port. In the case of fiber-optic cable you can, for example, set the cable names here.
   In the "Partner port" area, select the drop-down list for "Partner port" in order to display the available partner ports and make a selection.

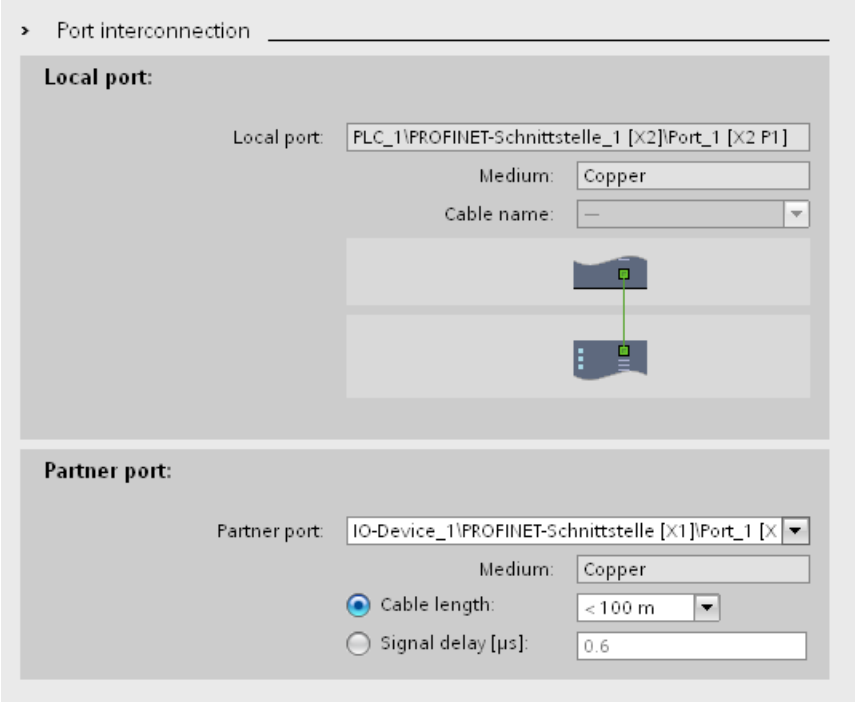


Figure 3-320 Interconnecting ports in the Inspector window in STEP 7

If the PROFINET interface was disconnected, it is automatically connected by this action. In the properties of the subnet you can set whether this subnet should or should not be used for the networking.

5.5.4 Automatic assignment of devices by offline/online comparison

Overview

During the offline/online comparison, the configured topology is compared with the actual existing topology. Devices identified online are automatically assigned to configured devices as far as this is possible.

Start of availability detection

You start the availability detection the first time by clicking the "Compare offline/online" button in the toolbar of the "Topology comparison" tab.

You restart availability detection by clicking the "Update" button.

NOTE

The availability detection can take several seconds. During this time, no user input is possible.

Automatic assignment of a PNIO device

A PNIO device identified online is automatically assigned to a configured device if the following properties of the two devices match up:

- Article no.
- Type
- PROFINET device name

No automatic assignment

In the following situations, no automatic assignment is possible:

- No device can be identified online to match a configured device. (This means that the corresponding columns in the "Online topology" area of the topology comparison table are empty.)

  In this case, you should add the already configured device to your system or delete the configured device from the configuration.
- A device identified online can be assigned to a configured device, but there are differences in the port interconnections.

  In this case, you can Apply the port interconnections identified online manually to the project (Page 82).
- A device identified online cannot be assigned to a configured device. (In this case, the corresponding columns in the "Offline topology" area of the topology comparison table are empty.)

  In this case, you can Include the devices identified online manually in the project (Page 83).

5.5.5 Apply the port interconnections identified online manually to the project

Requirements

You have run an offline/online comparison in the topology view. The result of this is that at least one device identified online was automatically assigned to a configured device, but that there are differences relating to the interconnection.

Procedure

To adopt one more port interconnections identified online in the project manually, follow these steps:

1. Select the row belonging to the port interconnection.
2. If applicable, select further roles using multi-selection.
3. Select "Apply" > "Use selected" in the shortcut menu.
   The content of the corresponding table cells in the "Action" column changes to "Apply".
4. If you have mistakenly prepared too many port interconnections to be included in the project:
   Select the rows belonging to the port interconnections you have mistakenly prepared for inclusion in the project using multi-selection.
   Select "Reset" > "Reset selected" in the shortcut menu.
   The content of the corresponding table cells in the "Action" column change to "No action".
5. Click the "Synchronize" button.

Result

The port interconnections identified online for the corresponding devices are included in the project. Successful adoption is indicated by the diagnostics icon "Identical topology information" for each port.

NOTE

If other port interconnections are recognized for a device identified online and these differ from those that exist in the project, adopting these in the project means that the port interconnections that were previously in the project are replaced by those identified online. If no port interconnections are detected for a device identified online, adopting in the project means that all the port interconnections of this device are deleted in the project.

5.5.6 Include the devices identified online manually in the project

Requirements

You have run an offline/online comparison in the topology view. The result of this is that at least one device identified online could not be assigned to any configured device.

Procedure

To adopt one more devices identified online in the project manually, follow these steps:

1. For a configured device without an online partner, move the mouse pointer to the "Device/port" column of the online topology.
2. Select the device you want to assign to the configured device from the drop-down list of this box.
3. Repeat the previous steps if necessary for other configured devices without an online partner.

Result

The selected device that was identified online is moved up from the end of the table. Following this, it is in the row of the configured device to which you have just assigned it.

5.5.7 Automatic assignment of devices by advanced offline/online comparison

Overview

With the advanced offline/online comparison, ICMP is also used alongside DCP to be able to detect devices that do not support DCP.

Automatic assignment of devices detected by ICMP

With devices detected by ICMP, no type is available.

With passive devices, no article number is available. For this reason, passive devices can only be assigned automatically if you have not assigned an article number in the configured data and the offline and online IP addresses match.

With switches, automatic assignment is possible if the offline and online article number, IP address and PROFINET device name match.

Diagnostics and maintenance

6

LEDs for diagnostics on PROFINET

Each port of a PROFINET interface of a SIMATIC device has one LED.

The following table shows a summary of the meaning of these LEDs in the S7-1500, ET 200MP, ET 200SP and ET 200AL systems.

Table 3-40 S7-1500, ET 200MP, ET 200SP, ET 200AL: LEDs for diagnostics on PROFINET

LED image	Meaning	S7-1500	ET 200MP	ET 200SP	ET 200AL
		LINK/TX/RX LED		LK LED	P1 Link LED P2 Link LED
LED off	There is no Ethernet connection between the PROFINET interface of the PROFINET device and the communication partner. No data is currently being sent/received via the PROFINET interface.	X	X	X	X
LED green	There is an Ethernet connection between the PROFINET interface of your PROFINET device and a communication partner.	X	X	X	X
LED flashes green	The "LED flashing test" is being performed.	X	X	X	X
LED flickers yellow	Data is currently being received from or sent to a communications partner on Ethernet via the PROFINET interface of the PROFINET device.	X	X	-	-

Additional information

You can find a detailed description of all LEDs of the module with cause of the error and remedies in the relevant documentation for the module.

6.1 Diagnostics mechanisms of PROFINET IO

Totally Integrated Diagnostics Concept

All SIMATIC products have integrated diagnostics functions that they can use to detect and remedy faults. The components automatically flag a potential fault in the operation and provide detailed information.

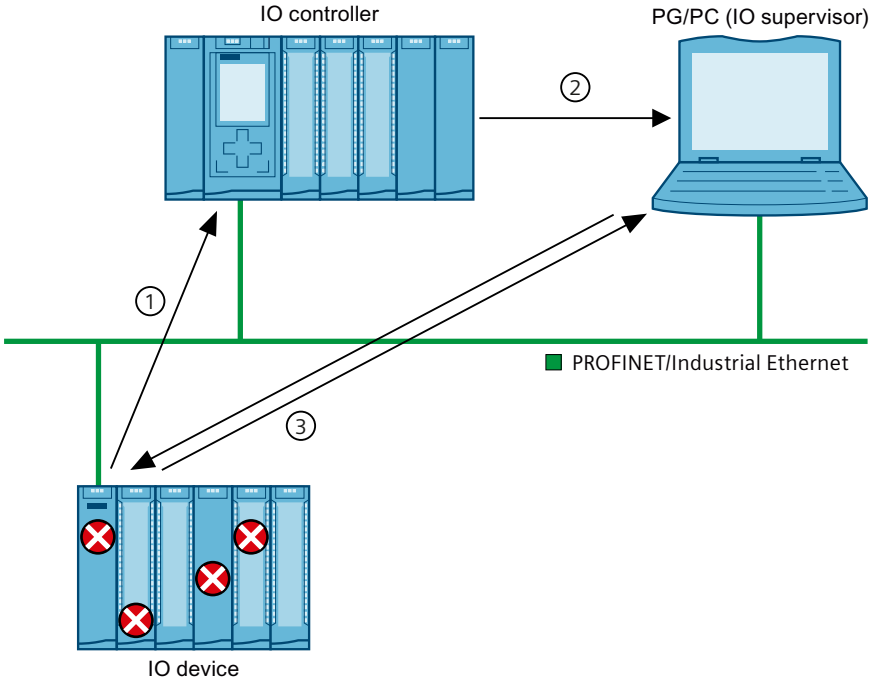
Each individual error or several errors occurring concurrently are transferred from the IO device to the IO controller. If you require the full status of the IO device including any pending errors, you can also read the status directly from the IO device.

The following sections provide basic information on using diagnostics via PROFINET IO. You can find a detailed description of the system diagnostics for S7-1500, ET 200MP, ET 200SP

and ET 200AL in the Diagnostics (http://support.automation.siemens.com/WW/view/en/59192926) function manual.

Accessing the status of an IO device with a PG/PC or an HMI device

If you are connected to the Industrial Ethernet via a PG/PC with STEP 7 or an HMI device, you can also call up diagnostics information online. This is illustrated by the following graphic.



Number	Description
①	The IO device detects an error and sends diagnostics data to the IO controller.
②	The IO controller notifies the programming/HMI device. The display of the system diagnostics is updated.
③	In STEP 7, you can read the station status for "Accessible devices" directly from the IO device regardless of the IO controller. This is only possible if the programming device is connected to Industrial Ethernet. This means that you can access diagnostics information during the commissioning phase or for servicing even if the IO controller is not operational.

Figure 3-321 PROFINET IO diagnostics with PG/PC or HMI device

6.1.1 Diagnostics levels in PROFINET IO

Concept

The IO device sends all error messages that occur to the IO controller. The scope and volume of diagnostics information varies according to the level of diagnostics data evaluation and the PROFINET devices you are using.

Diagnostics levels

You can evaluate diagnostics data at different levels. The number and type of channels is selected, for example, at the diagnostics level 4.

The following figure shows the diagnostics levels with PROFINET IO.

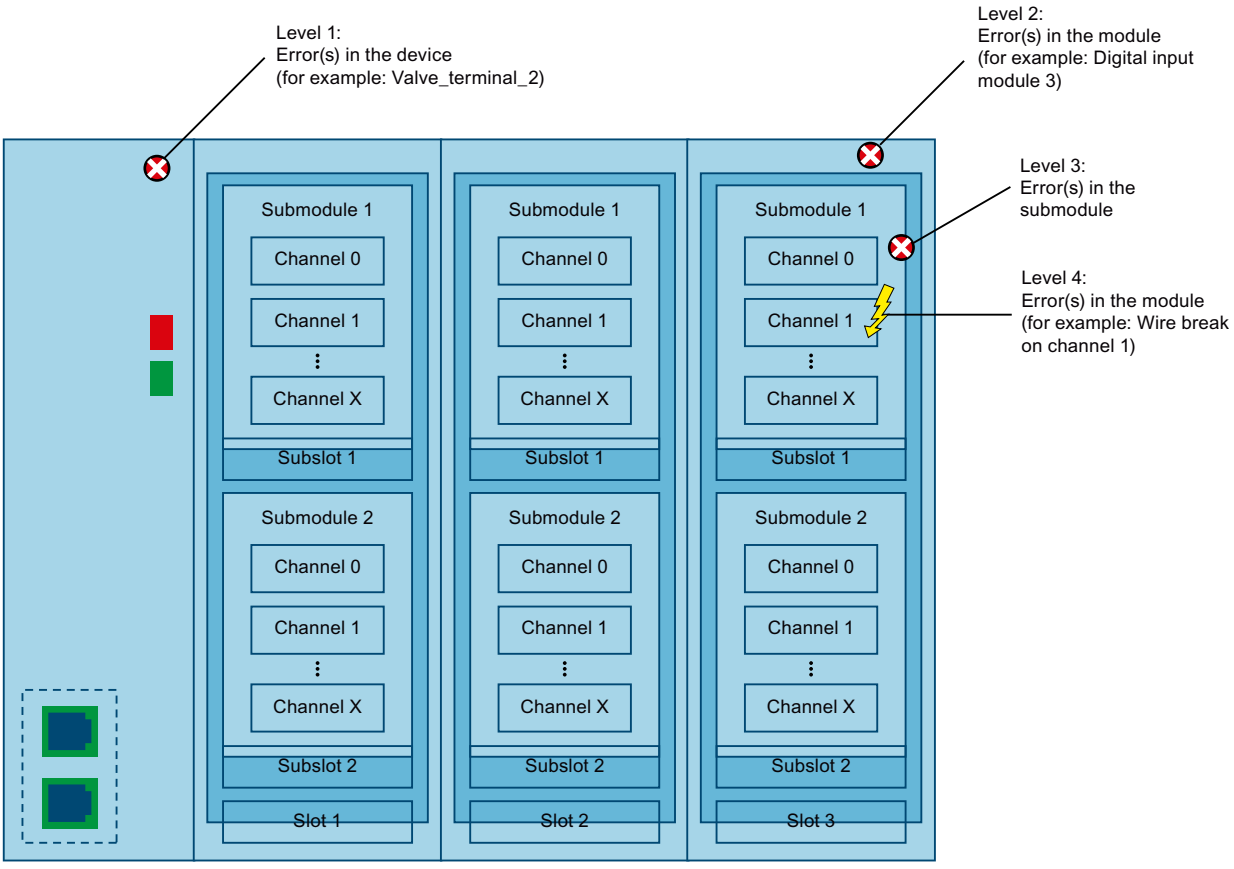


Figure 3-322 Diagnostics levels with PROFINET IO

Representation of diagnostics levels in the device view in STEP 7

The following figure shows the representation of the PROFINET device model in the device view of STEP 7, based on the example of a distributed I/O system ET 200MP:



Number	Description	
①	Level 1:	Error(s) in the device
②	Level 2:	Error(s) in the module

Figure 3-323 Diagnostics levels in the device view of STEP 7

Which PROFINET nodes support the extended PROFINET diagnostics?

An overview of the PROFINET nodes that support extended PROFINET diagnostics and of what you have to configure is provided in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/23678970).

6.2 Diagnostics via the display of the S7-1500 CPUs

Display

The S7-1500 CPU has a display and operating keys. The display of the CPU shows you the control and status information in different menus. You use operating keys to navigate through the menus and make a variety of settings in the process.

Diagnostics via the display

The following indicators can be evaluated for diagnostics purposes on the display:

- Error and alarm texts (system diagnostics, alarm messages)
- Module status for central and distributed modules

In the following example of a display of the CPU 1516-3 PN/DP, you can see a warning on the diagnostics icon and an exclamation mark on the icon for module.

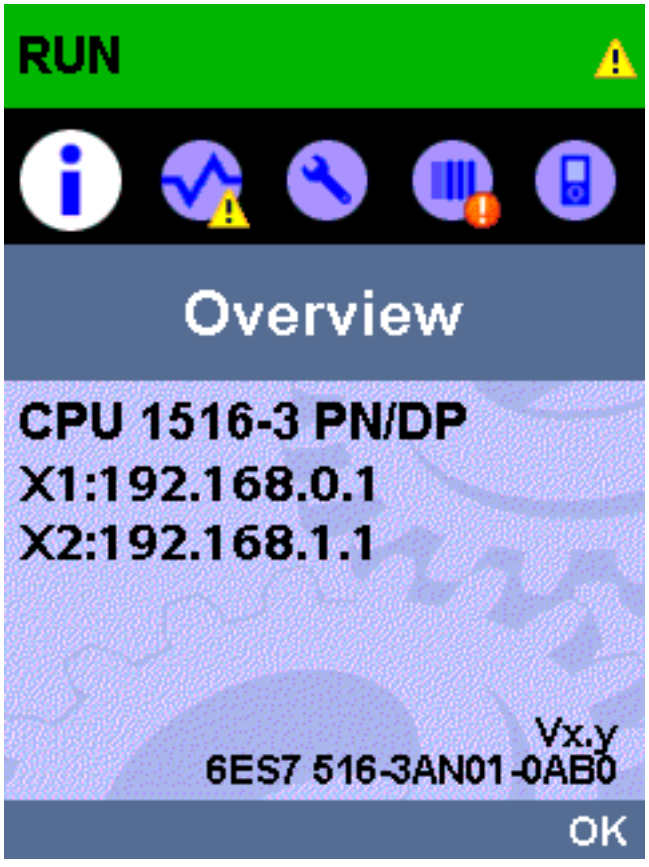


Figure 3-324 Display of overview

Module status

To show the module status, navigate on the display through the menu items "Module" > "PROFINET I/O (X1)" > "Station" > "Slot" > "Status" > "Module status".

The module status indicates that a fault has occurred in the module. The "lower-level status" is the status of the module in the diagnostics level below this. In the example, the status is "good", i.e., the fault is not in the lower diagnostics level submodule or channel, but instead in the module.



Figure 3-325 Display of module status

Error and alarm texts

You can show diagnostics buffer entries and alarm messages for the relevant automation system on the display.

To show the diagnostics buffer entries of the CPU, navigate on the display via the menu items "Diagnostics" > "Diagnostics buffer".



Figure 3-326 Display of diagnostics buffer

To show the alarm messages of the automation system, navigate through the menu items "Diagnostics" > "Alarms" > "Alarm text" on the display.

NOTE

Updating the alarm display

The display shows the currently read status of the CPU in static form, the display is not automatically updated. The alarm display is updated after it has been exited and opened again.

You set the automatic updating of the diagnostics information under: "Display" > "DiagnosticRefresh".



Figure 3-327 Display of alarms



Figure 3-328 Display of alarm message

Additional information

You can find the description of the operation and functions of the display in the SIMATIC S7-1500 Display Simulator (http://www.automation.siemens.com/salesmaterial-as/interactive-manuals/getting-started_simatic-s7-1500/disp_tool/start_de.html).

6.3 Diagnostics via Web server

The CPUs belonging to the S7 family have their own integrated Web server with a wide range of functions.

The following diagnostics options are available to you:

- Start page with general CPU information
- Information on diagnostics
- Contents of the diagnostics buffer
- Module information
- Alarms
- Information about communication
- PROFINET topology
- Motion Control diagnostics
- Trace
- Contents of the diagnostic buffer
- Module status
- Actual topology of the PROFINET system
- Set topology of the PROFINET system (from the configuration)

Set topology and actual topology - graphic view

Requirements for displaying the set and actual topology:

- You have configured the PROFINET ports in the topology editor of the hardware and network editor of STEP 7.
- You have loaded the entire project with STEP 7 in the CPU.

The following shows an example of the graphic view.

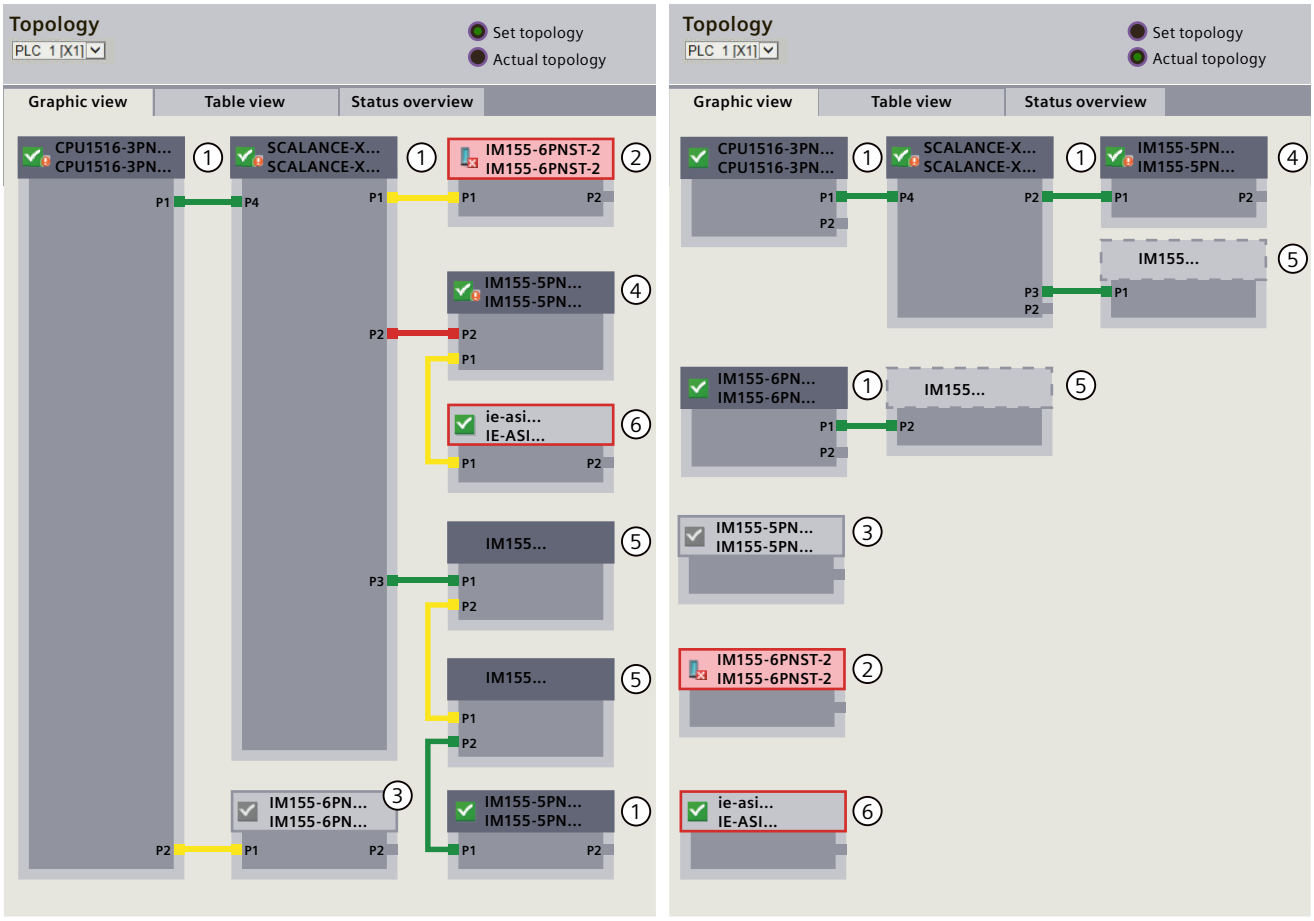


Figure 3-329 Topology - graphic view via the Web server

Meaning of the colored connections in the set/actual topology:

Table 3-41 Meaning of the colored connections in the set/actual topology:

Connection	Meaning	
	Set topology	**Actual topology**
green	The current actual connection matches the configured set connection.	detected connections
red	The current actual connection does not match the configured set connection (e.g., port interchanged).	-
yellow	The connection cannot be diagnosed. Causes: • The communication to an IO device has been disrupted (e.g., cable removed) • Connection to a passive component • Connection to PROFINET devices of another IO controller or PROFINET system	-

① Configured and accessible PROFINET devices

Configured and accessible PROFINET devices are displayed dark-gray. Connections show the ports through which the PROFINET devices of a station are connected.

① Configured but not accessible PROFINET devices

The configured but not accessible PROFINET devices are displayed in pink with red border (e.g., device has failed, cable disconnected).

③ Disabled devices

All disabled, configured PROFINET devices are displayed light-gray.

④ Interchanged ports

Interchanged ports are marked red in the set topology view. The currently connected ports are displayed in the actual topology, the configured set connection in the set topology.

⑤ PROFINET devices of another PROFINET IO system

- In the set topology:

  A PROFINET device of another PROFINET IO system is displayed with a green connection (or red connected if the ports have been interchanged), when it is directly adjoining a configured and accessible PROFINET device ① and it is also accessible. When the PROFINET device of another PROFINET IO system is not accessible, a yellow connection line is displayed.

  The connection between two PROFINET devices that both belong to a different PROFINET IO system, cannot be determined and is always displayed in yellow.
- In the actual topology:

  A PROFINET device of another PROFINET IO system is only displayed if the PROFINET device is in direct proximity to a configured PROFINET device. The PROFINET device is displayed light-gray and with dashed line.

For PROFINET devices of a different PROFINET IO system, **no** status display is shown on the device head.

⑥ Representation of faulty neighbor relations

The devices whose neighbor relations cannot be read out completely or correctly are displayed light-gray with red border.

Additional information

The tabular view of the actual topology and the status overview of the PROFINET devices in the project are possible.

You can find these views, additional topology examples, and detailed information on the operation and the functions of the Web server in the Web server (http://support.automation.siemens.com/WW/view/en/59193560) manual.

6.4 Online diagnostics with STEP 7

For PROFINET, you have the following options to evaluate diagnostics in STEP 7:

- Online & diagnostics - Devices & networks
- Online & diagnostics - diagnostics of PROFINET ports

Online & diagnostics network view

In the hardware and network editor (launched from the "Project tree" by double-clicking "Devices & networks"), you can get an overview of the current state of your system by clicking on the "Go online" button. It also shows the configuration information (for example, non-configured modules). This option is also available in the topology view in similar form.

Schematic drawing of the network view (online):

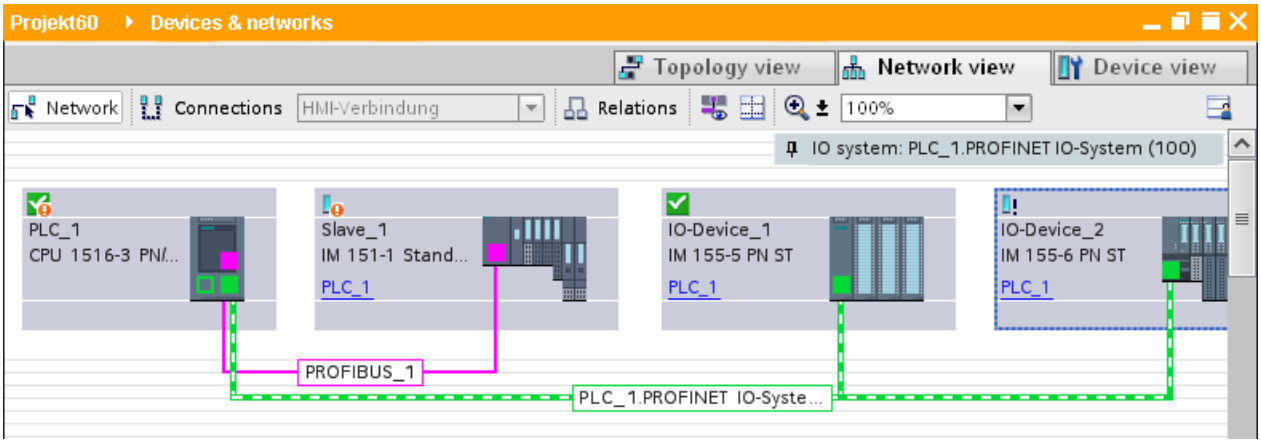


Figure 3-330 Online & diagnostics network view

Online & diagnostics device view

In STEP 7, you can display an overview of the modules in which faults have occurred. To do this, select the menu command "Online > Online & diagnostics". Once you are connected, you can see the status of the accessible devices in the project tree.

Double-click the device which displays an alarm message to access the faulty module directly. The device view is opened in the work area. In the device view of the device that reports the fault you can see directly in which module the fault occurs.

Open the "Diagnostics" tab and the subordinate "Device information" tab in the Inspector window for a more detailed error description.

Schematic drawing of the device view (online):

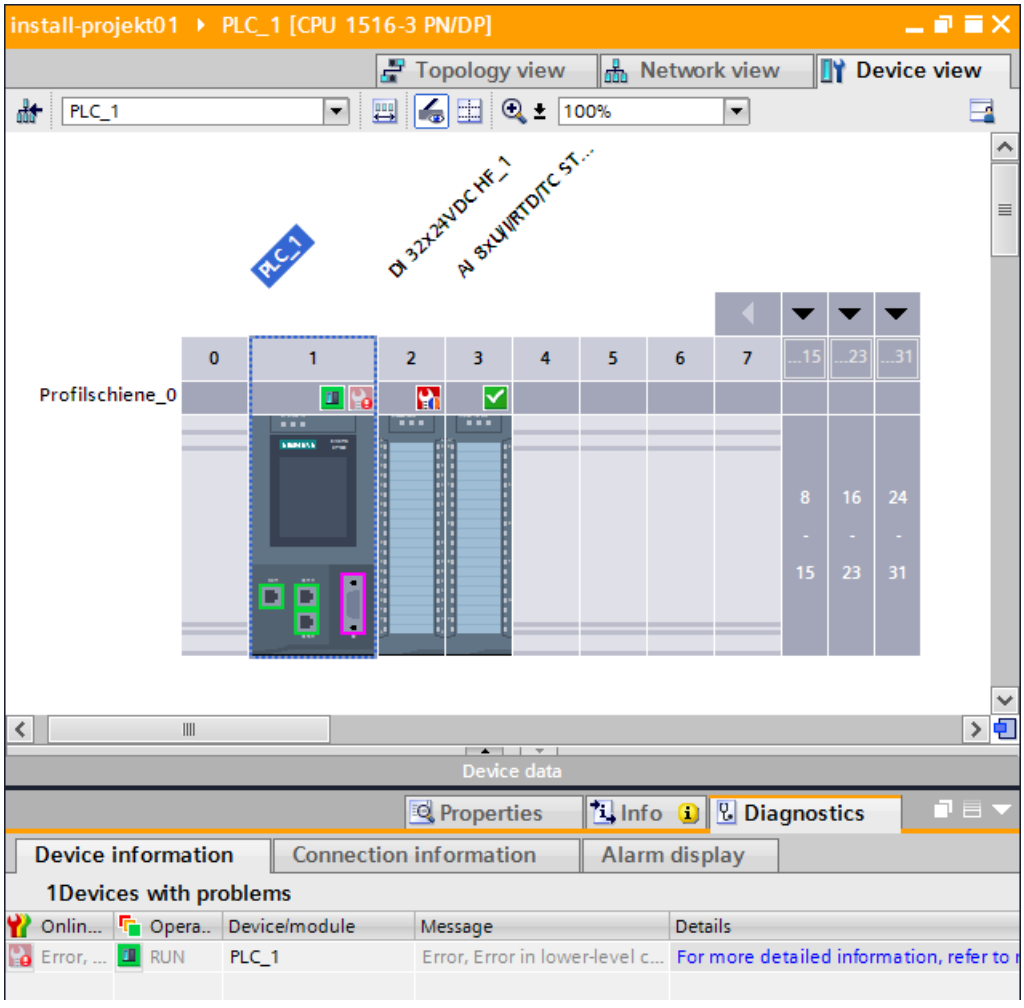


Figure 3-331 Online & diagnostics device view

Diagnostics of PROFINET ports

If you select "PROFINET interface > Ports" in the Diagnostics area in the online & diagnostics device view of a PROFINET device, the ports of the PROFINET interface are listed in a table.

The table provides you with the following information about the ports of the PROFINET interface.

- Name
- Status
- Settings
- Operating mode

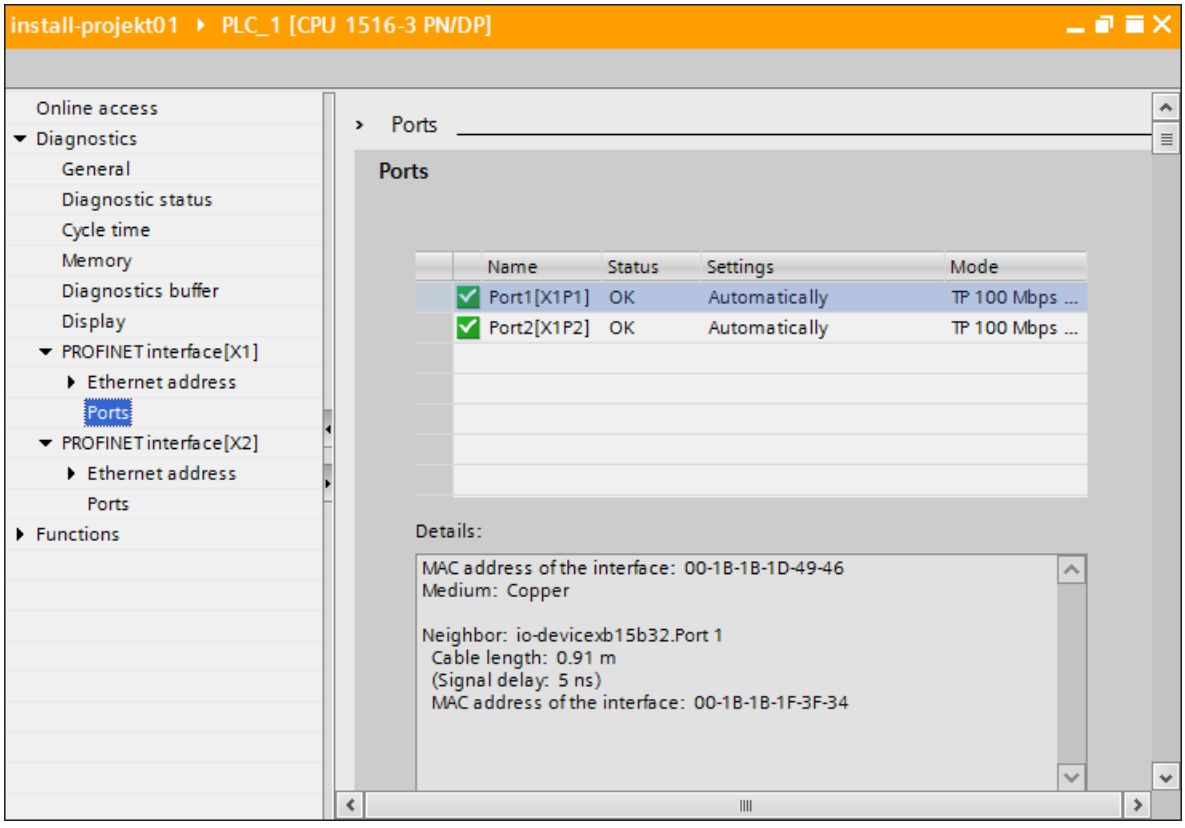


Figure 3-332 Diagnostics of PROFINET ports in STEP 7

Additional information

You can find information on the system diagnostics for S7-1500, ET 200MP, ET 200SP and ET 200AL in the Diagnostics (http://support.automation.siemens.com/WW/view/en/59192926) function manual and online help for STEP 7.

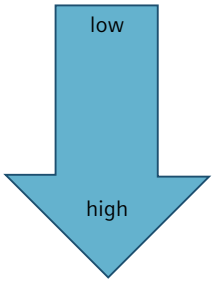
6.5 Extended maintenance concept

Extended maintenance concept

The PROFINET interfaces with integrated switch of the SIMATIC devices support the four-level diagnostics concept in accordance with PROFINET specification Version V2.3 or higher with the following status:

Table 3-42 Classification of the diagnostic status

Diagnostic status	Symbol		Severity of the error
Good	White check mark on a green back-ground		

Diagnostic status	Symbol		Severity of the error
Maintenance required	White wrench on a green background		
Maintenance demanded	White wrench on a yellow background		
Bad	White wrench on a red background		

The aim of the diagnostics concept is the early detection and elimination of potential faults - before they cause a production outage.

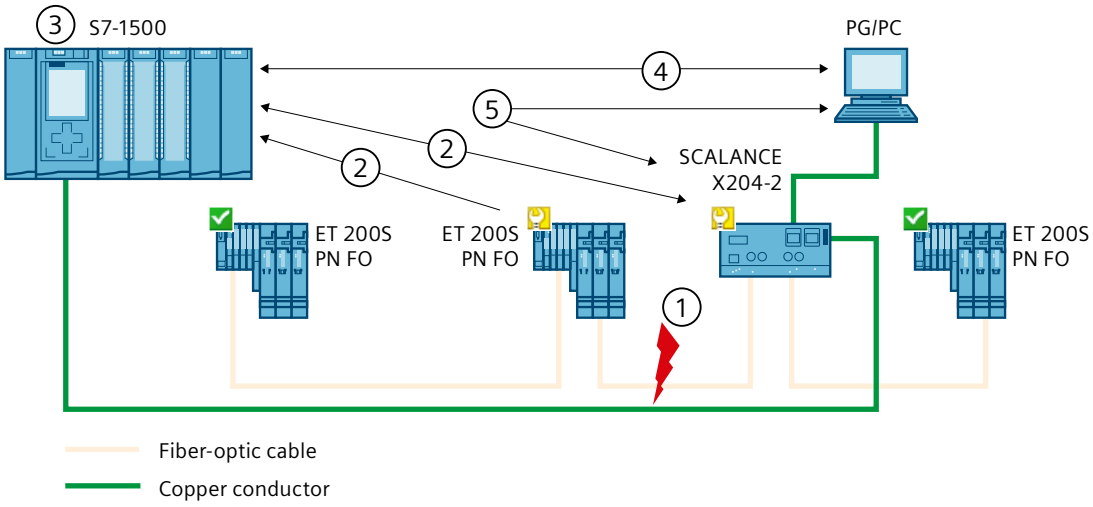
Other status information is defined in addition to the Good (no fault) and Bad (fault) status information for a PROFINET device.

The maintenance information is generated with the maintenance required and maintenance demanded system alarms.

The times at which the two system alarms are generated can be customized for most wear parameters.

Example: Maintenance demanded for a PROFINET cable

The following graphic illustrates how diagnostics information is transmitted when the transmission quality on the optical cable decreases due to aging, for example. In this example, the scenario is considered after a maintenance required has already been diagnosed.



Number	Description
①	The system reserve of the fiber-optic cable drops below 0 dB.
②	Both the ET 200S PN FO and the switch send the maintenance demanded alarm to the IO controller.
③	Based on the interrupts, the IO controller detects the maintenance demanded from the switch and from the IO device. The module information data is updated in the IO controller and the corresponding error OBs are called. Note: To be able to start the error OBs in the IO controller, the "Call the user program if communication errors occur" property must be selected in STEP 7 for the relevant IO controller.
④	In STEP 7 (on the programming device/PC), the IO device and switch indicate maintenance demanded with a white wrench on a yellow background.
⑤	STEP 7 can also read out detailed information directly from the switch.

Figure 3-333 Maintenance demanded for a PROFINET cable

6.6 Diagnostics of the network topology

Availability

As an open standard, you can use any SNMP based systems or software solutions for diagnostics in PROFINET.

Network diagnostics

The network management protocol SNMP (Simple Network Management Protocol) uses the wireless UDP transport protocol. It consists of two network components, similar to the client/server model. The SNMP manager monitors the network nodes and the SNMP clients collect the various network-specific information in the individual network nodes and store it in a structured form in the **MIB** (Management Information Base). This information allows a network management system to run detailed network diagnostics.

MIB

The MIB (Management Information Base) is the database of a device. SNMP clients access this database in the device. The S7 device family supports the following standard MIBs:

- MIB II, standardized in the RFC 1213
- LLDP-MIB, standardized in the international standard IEC 802.1AB
- LLDP-PNIO-MIB, standardized in the international standard IEC 61158-6-10

You will find the MIBs for ET 200 interface modules and couplers with PROFINET interface in this product note (https://support.industry.siemens.com/cs/ww/en/view/109770525).

Detecting the network topology

LLDP (Link Layer Discovery Protocol) is a protocol that is used to detect the closest neighbor. LLDP enables a device to send information about itself and to receive information from its neighbor devices. This information is then saved in the LLDP MIB, for example, and can be queried using SNMP. This information allows a network management system to determine the network topology.

Use of SNMP (Simple Network Management Protocol)

SNMP can be used as follows:

- By users to integrate network diagnostics into a central HMI/SCADA system using the SIMATIC NET OPC server
- By the IT administration of machine and plant operators to monitor their Industrial Ethernet network using standard network management systems.
- By the IT administration, to monitor the automation network, alongside the office network, using standard network management systems.

Use of SNMP in the SIMATIC NET environment

SNMP-compliant devices from the SIMATIC NET family can be monitored and operated via a conventional standard Internet browser. The management system known as web-based management offers a wide range of device-specific information (network statistics, status of redundant supply, for example).

6.7 Diagnostics in the user program

6.7.1 Diagnostics and configuration data records

Diagnostics mechanism

The IO device outputs a diagnostics interrupt to the IO controller when it detects faults such as wire break on an IO module. This interrupt calls a corresponding organization block in the user program (diagnostics interrupt OB82), in order to generate a defined (programmed) response to the fault and passes a diagnostics data record.

Diagnostics data records in PROFINET IO

There are two different types of diagnostics data record:

1. Channel diagnostics data records

   Channel diagnostics data records are generated if a channel is in an error state and / or has triggered an interrupt.

   A diagnostics data record of length 0 is returned if there is no fault.
2. Vendor-specific diagnostics data records

   The structure and size of vendor-specific diagnostics data records depend on the vendor's settings.

   For information about vendor-specific diagnostics data records, refer to the appropriate device manual.

Addressing levels of diagnostics data records

Diagnostics and configuration data is evaluated at the following addressing levels:

- Device level
- AR (Application Relation)
- API (Application Process Identifier)
- Slot
- Subslot

A group of diagnostics and configuration data records are available for each address level (exception: device level always 0xF80c). In HEX representation, the individual groups of data records are distinguished by the first letter of the data record number.

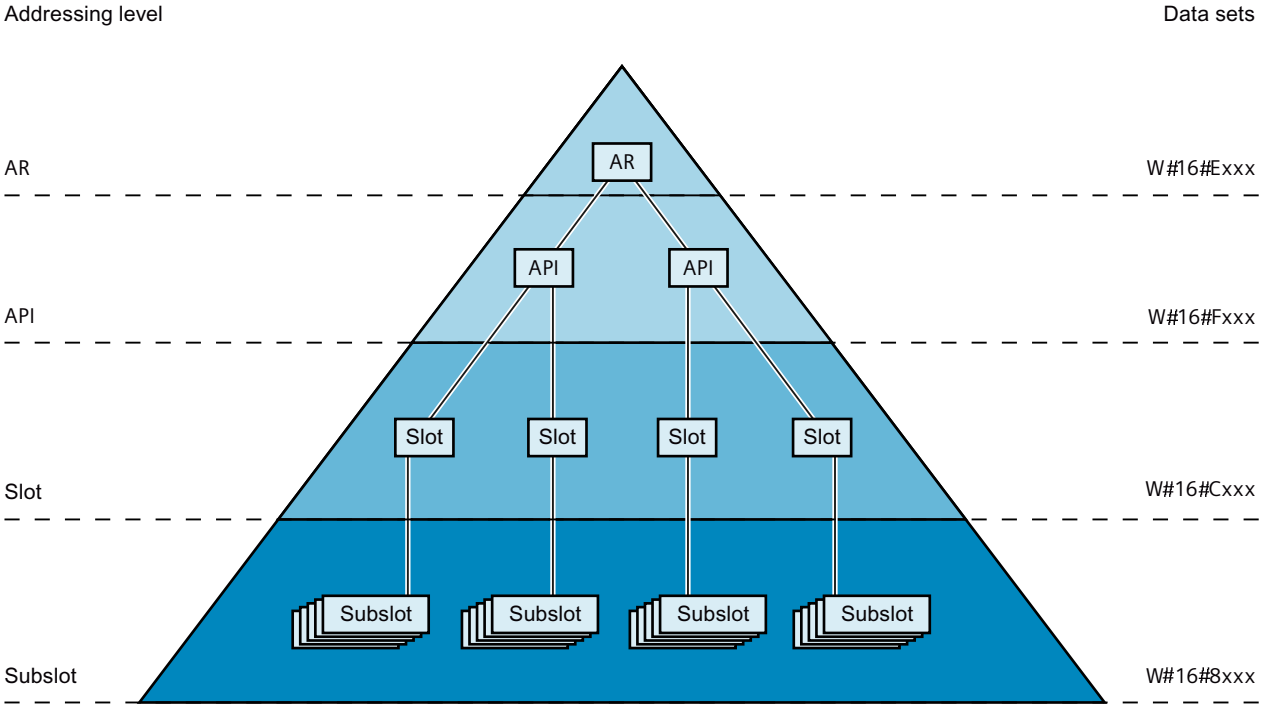


Figure 3-334 Addressing levels of diagnostics data records

The information for each IO device (addressing level AR), module (addressing level slot) or submodule (addressing level subslot) is always transferred in separate diagnostics or configuration data records. The data record returns diagnostics data or configuration data for one or more subslots, slots and APIs, depending on the addressing level.

NOTE
The diagnostics information is only generated for configured modules / submodules / channels.

Library for PROFINET data records

The "LPNDR" block library contains various function blocks. You can use these blocks to read out various device and status information from a PROFINET device and write parameters.

You can execute the following functions using the library blocks:

- Read device information:
  - Information about the interface, e.g. IP and MAC address
  - Information about the device interface, e.g. status, medium, name
  - Information about the link status of the interfaces, e.g. link down, link up
  - Information about the role of the device for MRP, e.g. client, manager
  - Information about the port statistics, e.g. number of received bytes

- Read the MRP status
- Modification of the parameters of analog input module of the ET 200SP in runtime, e.g. in order to disable/enable the channel diagnostics.

The finished functions are freely adaptable and can therefore be used universally.

The "LPNDR" block library with an example project can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109753067).

6.7.2 Evaluate diagnostics in the user program

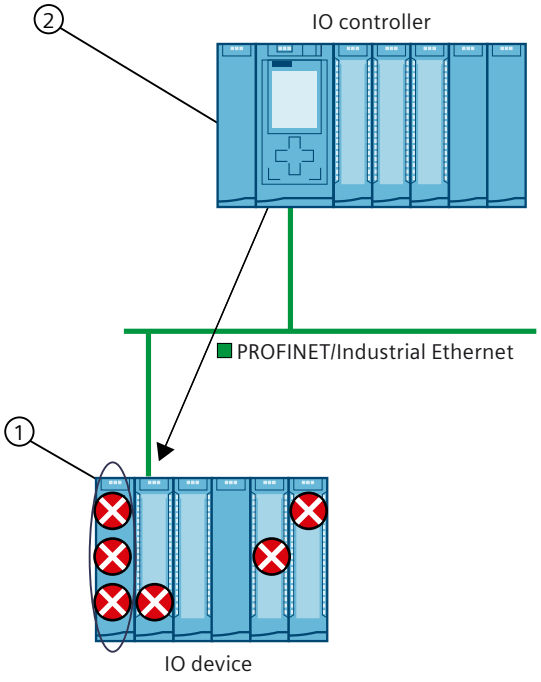
Diagnostics in the user program

For PROFINET IO, a cross-vendor structure of data records with diagnostics information applies. Diagnostics information is created only for channels on which a fault has occurred. With PROFINET, there are two basic ways to obtain diagnostics information.

1. Evaluating the diagnostics status

Read out the diagnostics of your PROFINET IO system using the instructions "DeviceStates" and "ModuleStates" to localize faulty stations / modules or station / modules with maintenance demanded or maintenance required within a PROFINET IO system.

The instruction RDREC (read data record) is then used to read various diagnostics data records directly from the module concerned and thus obtain detailed information about the error.

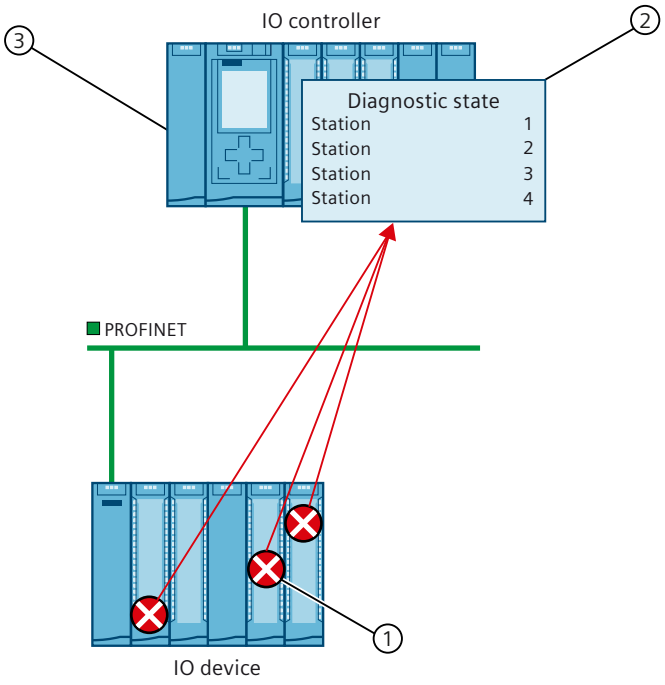


Number	Description
①	All individual errors are collected in a single data record on the interface module.
②	In your user program, the instruction "RDREC" reads the entire station status asynchronously directly from the IO device.

Figure 3-335 Example: Evaluating diagnostics data records with the instruction "RDREC"

2. Evaluation of interrupts

When the error OB (OB 82) is called, the OB's start information provides you with information on the cause and location of the error. Detailed information on the error event can be obtained in the error OB using the instruction "RALRM" (read additional interrupt information).



Number	Description
①	Every error is sent to the IO controller individually as channel diagnostics information in the form of an interrupt.
②	In the IO controller, the module status data is updated automatically and the error OB (OB 82) is started.
③	In your user program in the error OB (OB 82), the instruction "RALRM" reads the error synchronously from the IO controller without addressing the IO device.

Figure 3-336 Diagnostics with OB 82 and the instruction "RALRM"

Instructions and OBs

You will find information on the instructions and OBs in the STEP 7 online help.

6.8 Maintenance

6.8.1 I&M data (identification and maintenance)

Definition and properties

Identification and maintenance data (I&M) is information saved to module memory in order to provide support when:

- Checking the plant configuration
- Locating hardware changes in a plant

Identification data (I data) is module information (some of which may be printed on the module housing) such as the order and serial number. I data is read-only vendor-specific module data.

Maintenance data (M data) is plant-specific information such as the location identifier and installation date. M data is created during configuration.

The modules can be uniquely identified in online mode by means of the I&M data.

Further information

To find out whether and to what extent a PROFINET device supports I&M data, refer to the documentation of the relevant device.

6.8.2 Loading I&M data to PROFINET IO devices and your modules

Which I&M data can be loaded to PROFINET IO devices and your modules?

You can load I&M 1 data (plant designation and location identifier) and/or I&M 2 data (installation date) and/or I&M 3 data (additional information) to the actual hardware.

Requirements

- In the project settings (Options > Settings, Hardware configuration > Compiling and downloading), the option "Download I&M data" must be enabled.
- There is an online connection to the PROFINET IO devices and the modules to which you want to load I&M data.
- You have entered the I&M data you want to download in the properties of the respective PROFINET IO devices and your modules (Inspector window: "Properties" tab > "General" tab, Settings > Identification & Maintenance).

Where do I specify which I&M data is downloaded to which PROFINET IO devices?

You specify which I&M data you want to download to which PROFINET IO devices in the "Load preview" dialog. You will find the following alternatives in the drop-down list of the "Identification and maintenance data (I&M)" row:

- Load nothing

  The check boxes for all PROFINET IO devices as well as the check boxes for the loadable I&M data are cleared.

  No I&M data is transferred to the actual hardware during loading with this setting.
- Load data

  The check boxes for all PROFINET IO devices as well as the check boxes for the loadable I&M data are selected.

  The respective I&M 1, I&M 2 and I&M 3 data is transferred to all PROFINET IO devices during loading with this setting.
- Load selected

  You select the check boxes of those PROFINET IO devices to which you want to load I&M data. You also select the check boxes of the identification data you want to load.

  With this setting, you transfer the selected I&M data to the selected PROFINET IO devices during loading.

NOTE

Language dependency of the I&M data to be loaded
The I&M data are loaded to the real hardware in the form that you specified in the properties of the relevant PROFINET IO devices and your modules. There is no language dependency.

6.8.3 Asset management

6.8.3.1 Further information about asset management at PROFINET

Operation of machines and plants without a detailed knowledge of devices and assets is difficult to imagine.

Maintenance requires data for this – data that is extensive and up-to-date as far as possible.

The requirement of greater transparency with regard to the data made available by plant components has been fulfilled by PROFIBUS & PROFINET International (PI): The identification and maintenance data familiar since PROFIBUS times have been extended.

The current PROFINET fulfills this requirement through the definition of a special data record: the Asset Management Record (AMR).

The aim of this definition is to enable you to acquire **all** the components to be maintained online - and not only those components that can be addressed and accessed through the PROFINET device model (Device / Module / Submodule). PROFINET now also reaches non-PROFINET components!

Assets general and asset management data records

Assets are components (hardware and software / firmware) of a machine, for example a laser welding machine, or a plant.

A large number of these device components can already be identified through tried-and-tested I&M functions or corresponding data records (I&M0 to I&M5) in the PROFINET context: The device itself as well as its modules and submodules. Meaning all components that can be addressed through the PROFINET device model.

Components that **cannot** be addressed via the PROFINET device model, but whose data it should be possible to acquire online for operation and maintenance, can be identified through **asset management** functions. This asset management data (short: AM data) is stored in a defined structure in a special data record, the **asset management record** (AMR) mentioned above.

The PROFINET Guideline "Identification & Maintenance Functions" differentiates here between I&M functions (I&M data) and asset management functions (AM data): The following sections only deal with the AM data.

The components that can be read additionally online through asset management data records include both hardware components, such as backplane bus modules of a device as well as firmware components such as a drive control unit with own versioning.

Application examples

Importing asset management records enables you to read the following information during installation or operation, for example:

- Are only approved devices being used (whitelist check)?
- A firmware update is due. Obtain a fast overview: Which devices or components are affected and have to be upgraded?

Making asset management data available

The concept for the asset management of PROFINET devices stipulates that the manufacturers of PROFINET devices have to ensure that non-PROFINET automation components are made available through an asset management record. This data record is assigned to the PROFINET device.

In contrast to a "standard" IO device, with an I-device the project engineer has to make the asset management record available. In this case, the central modules of the I-device are assets. From the perspective of PROFINET, these central modules are not visible from the point of view of the higher-level IO controller. The higher-level IO controller only "sees" the transfer areas through which it exchanges IO data with the I-device.

The principle of this provision is explained in the section.

Reading asset management data

The asset management record has the index 0xF880 and is read with standard PROFINET mechanisms by the user of the records, for example a tool or program for evaluating these data.

A user program in the S7-1500 IO controller, for example, can read out the AMR of an IO device with the RDREC instruction (Index 0xF880).

It is not possible to write to this data record.

Further information

Whether and to which extent a PROFINET device supports asset management data, meaning whether it makes an AMR available, is specified in the documentation of the respective device.

6.8.3.2 Content and structure of an asset management record

Basic structure of the asset management record

You are first provided with an overview of the general structure of the record. The following table describes the framework within which the asset management data blocks are embedded. Each data block represents an asset, a terminal block for example.

Element of the data structure	Designation according to IEC 61158-6-10	Code	Data type / length in bytes
Header AssetManagementData	BlockType	0x0035	UINT / 2
	BlockLength	Number of bytes without counting the bytes for BlockType and BlockLength	UINT / 2
	BlockVersion	0x0100	UINT / 2
AssetManagementInfo AssetManagementBlocks (n)	NumbersOfEntries	Number of AssetManagementBlocks	UINT / 2
	AssetManagementBlock 1	See the table below	
	AssetManagementBlock 2		
	...		
	AssetManagementBlock n		

Structure of asset management blocks

Each AssetManagementBlock contains identification data and localization information for an asset. An AssetManagementBlock has a substructure with basic characteristics described below.

The header of an AssetManagementBlock contains the coded information about which of the three possible AM data compilations the data record contains. Devices make a suitable BlockType available in accordance with the various device types:

- Complex devices with information about the hardware and firmware (BlockType "AM_FullInformation")
- Complex devices with information about the hardware (BlockType "AM_HardwareOnlyInformation")
- Devices with information about the firmware (BlockType "AM_FirmwareOnlyInformation")

The differentiation provides an efficient data structure below the header. Nevertheless, the data record can have a considerable size (maximum of 64 KB, depending on the number of assets that the IO device supplies).

Table 3-43 Structure of AssetManagementBlock

Element of the data structure	**Designation according to IEC 61158-6-10**	**Code**	**Data type / length in bytes**
Header AssetManagementBlock	BlockType	0x0036 (AM_FullInformation) 0x0037 (AM_HardwareOnlyInformation) 0x0038 (AM_FirmwareOnlyInformation)	UINT / 2
	BlockLength	Number of bytes without counting the bytes for BlockType and BlockLength	UINT / 2
	BlockVersion	0x0100	UINT / 2
	Padding	0x0000 (padding byte)	USINT / 1
	Padding	0x0000 (padding byte)	USINT / 1
AssetManagementBlock (Structure depends on the BlockType. Here it is shown using AM_FullInformation as an example)	IM_UniqueIdentifier	Manufacturer-generated Universal Unique Identifier (UUID) conforming to ISO/IEC 9834-8. Used as a reference key to uniquely identify this asset. Example: 550c5300-d34a-22b4-11d3-5533991111b3	Array of Byte / 16
	AM_Location	Description of the location of the asset: Either slot-oriented ("Slot and SubslotNumber format") or hierarchical ("Twelve level tree format"). See following description	Array of Byte / 16
	IM_Annotation	Manufacturer-specific notation Example: "Terminal block, Type xyz123 ". 64 bytes are always used. Spaces are used for padding if the string is shorter.	Array of Char / 64
	IM_OrderID	Manufacturer-specific article number Example: "6ES7131-6BF00-0BA0 ". 64 bytes are always used. Spaces are used for padding if the string is shorter.	Array of Char / 64
	AM_SoftwareRevision (not at AM_HardwareOnlyInformation)	Manufacturer-specific SW version Example: "V6.3.8 ". 64 bytes are always used. Spaces are used for padding if the string is shorter. If the asset supports IM_Software_Revision, the AM_SoftwareRevision is padded with spaces.	Array of Char / 64
	AM_HardwareRevision (not at AM_FirmwareOnlyInformation)	Manufacturer-specific hardware version Example: "A4 ". 64 bytes are always used. Spaces are used for padding if the string is shorter. If the asset supports IM_Hardware_Revision, the AM_HardwareRevision is padded with spaces.	Array of Char / 64

Element of the data structure	Designation according to IEC 61158-6-10	Code	Data type / length in bytes
AssetManagementBlock (Structure depends on the BlockType. Here it is shown using AM_FullInformation as an example)	IM_Serial_Number	Manufacturer-specific unique production-related number. The characters come from the visible range (0x20 ... 0x7E), no control characters. Example: "A78C-1C82 ". 16 bytes are always used. Spaces are used for padding if the string is shorter.	Array of Char / 16
	IM_Software_Revision (not at AM_HardwareOnlyInformation)	Software version, follows a strict structure (SW version prefix, for example "V", digits for functional extension, digits for BugFix, digits for internal change). Example: 'V' 0x01 0x2 0x3 If AM_SoftwareRevision is padded with spaces, you should evaluate IM_Software_Revision. If the asset does not support any hardware, the coding 'V' 0x00 0x00 0x00.	Array of Byte / 4 Prefix (character "V", "R", "P", "U", or "T"), then 3 digits "0" to "9"
	AM_DeviceIdentification	Identification of the device. The structure is as follows: AM_DeviceIdentification.DeviceSubID (for SIEMENS e.g. 0x0000) AM_DeviceIdentification.DeviceID (Device ID from manufacturer, 0x0000 to 0xFFFF) AM_DeviceIdentification.VendorID (Example for Siemens assets: 0x002A) AM_DeviceIdentification.Organization: Example for Siemens assets: 0x0000 (PROFINET)	Array of Byte / 8
	AM_TypeIdentification	Manufacturer-allocated type identification: 0x0000: Unspecified 0x0001: Controller (PLC) 0x0002: PC-based 0x0003: IO module, IO submodule 0x0004: Communications module / submodule 0x0005: Interface module / submodule 0x0006: Active network component 0c0007: Media attached unit (bus adapter) 0x0100 to 0x7FF: Manufacturer-specific	UINT / 2
	IM_Hardware_Revision (not at AM_FirmwareOnlyInformation)	Version of the hardware (0x0000 to 0xFFFF) Example: 0x0003 If AM_HardwareRevision is padded with spaces, you should evaluate IM_Hardware_Revision.	UINT / 2

AM_Location

Asset management at PROFINET supports two formats for coding the location of an asset:

- Slot-oriented format ("Slot and SubslotNumber format")
- Hierarchical format ("Twelve **L**evel **T**ree format" abbreviated **LT** format)

Assets that are part of the PROFINET device use the slot-oriented format. These assets are bound completely to the PROFINET modules and submodules.

Assets that are located outside the PROFINET device use the hierarchical format (LT format) for coding the location of an asset.

These assets are localized by their tree level. The tree level begins with Level 0. The value of Level 0 provides information about the proximity to the PROFINET device:

- If the asset is connected to a module that can be addressed through the PROFINET device model, Level 0 has the value 0. The subsequent levels (Level 1 to Level 3) then have the meaning of slot address, subslot address and channel number. If further assets are connected to this asset, the next Level 4 is used. The limit is reached at Level 11.
- If the asset belongs to a PROFINET device but is not connected to a module that can be addressed through the PROFINET device model, Level 0 has a value between 1 and 0x1FF. An example of such an asset is a power supply unit in the PROFINET device. If a further asset is connected to this power supply unit, for example a sensor, the next tree level is used to localize this sensor (Level 1).
- If the asset is located outside the PROFINET device, but, for example, belongs to a machine into which the PROFINET device is installed, Level 0 has a value between 0x200 and 0x3FE.

The value 0x3FF for a tree level shows that this tree level is not used. This means that no further asset is connected. In this case, all the lower tree levels down to Level 11 must also have this value.

Example AM_Location slot-oriented

A rack and the terminal blocks located on it each supply AM data. The slot assignments are shown in the figure.

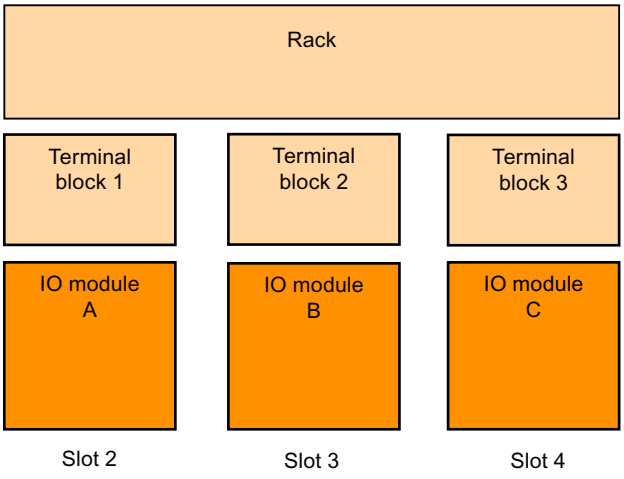


Figure 3-337 Example of assets with slot-oriented AM_Location coding.

Code the AM_Location as an asset for each module as follows:

Bit 0 – 7: AM_Location.Structure = 0x02 (coding "Slot and SubslotNumber format")

Bit 8 – 15: AM_Location.Reserved1 = 0x00 (padding byte)

Bit 16 – 31: AM_Location.BeginSlotNumber = 2 (the "Rack" asset begins from Slot 2 on)

Bit 32 – 47: AM_Location.BeginSubslotNumber = 0xFFFF (the asset encompasses all the subslots of Slot 2. Otherwise you specify the no. of the subslot at which the asset begins)

Bit 48 – 63: AM_Location.EndSlotNumber = 4 (the asset ends at Slot 4)

Bit 64 – 79: AM_Location.EndSubslotNumber = 0xFFFF (the asset encompasses all the subslots of Slot 4. Otherwise you specify the no. of the subslot at which the asset ends)

Bit 80 – 95: AM_Location.Reserved2 = 0x0000 (padding byte)

Bit 96 – 111: AM_Location.Reserved3 = 0x0000

Bit 112 – 127: AM_Location.Reserved4 = 0x0000

Example AM_Location level-oriented

A complex sensor is connected to an IO module (Slot 5, Subslot 1, Channel 1). Two simple sensors, in turn, are connected to the complex sensor. The module can be addressed within the PROFINET device model. Level 0 therefore has the value 0x0000. The next level (Level 1) is specified by the assigned slot. This is followed by the further levels for the subslot and channel and, if appropriate, further subordinate layers.

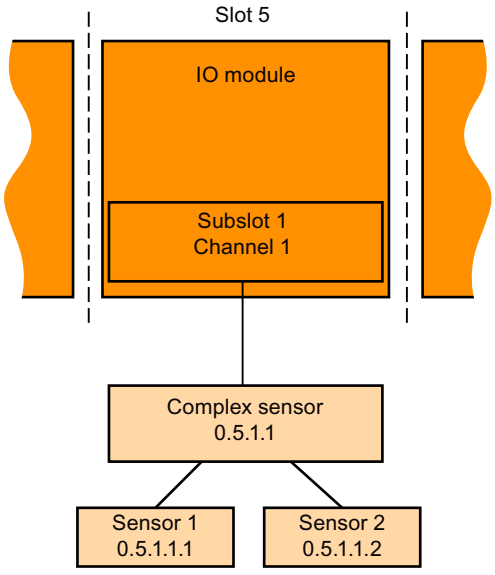


Figure 3-338 Example of assets with hierarchical AM_Location coding.

Detailed coding for the example:

Bit 0 – 7: AM_Location.Structure = 0x01 (LT format)

Bit 8 – 17: AM_Location.Level0 = 0x000 (assets that are assigned to modules always have the Level 0 value 0x000)

Bit 18 – 27: AM_Location.Level1 = 0x005 (Slot 5)

Bit 28 – 37: AM_Location.Level2 = 0x001 (Subslot 1)

Bit 38 – 47: AM_Location.Level3 = 0x001 (Channel 1)

Bit 48 – 57: AM_Location.Level4 = 0x3FF (coding for "Level not used")

Bit 58 – 67: AM_Location.Level5 = 0x3FF (coding for "Level not used")

...

Bit 118 – 127: AM_Location.Level11 = 0x3FF (coding for "Level not used")
Notation used in the screen for the LT coding of complex sensors: 0.5.1.1
The following correspondingly applies for the remaining sensors:
LT coding for simple Sensor 1 at complex sensor: 0.5.1.1.1
LT coding for second simple Sensor 2 at complex sensor: 0.5.1.1.2

6.8.3.3 Asset management data record for I-devices

With STEP 7 (TIA Portal) as of V15 and with S7-1500 CPUs as of firmware V2.5.2, you can compile an asset management data record via a user program. Configured as an I-device, these CPUs then supply the data from centrally plugged modules to a requesting IO controller as assets.

"S7-1500 CPUs" also refers to the CPU variants S7-1500F, S7-1500T, S7-1500C, S7-1500 SW Controller, S7-1500pro CPUs and ET 200SP CPUs.

Asset management records for I-devices

I-devices often represent machines. The PROFINET IO controller to which the I-device is assigned only sees the PROFINET interface (also configured as an IO device) and the transfer areas of the I-device configured by the machine manufacturer. The local modules of the I-device are not visible or cannot be accessed.

The assigned IO controller can read the central modules as assets of the I-device by means of an asset management record that the user program of the I-device compiles.

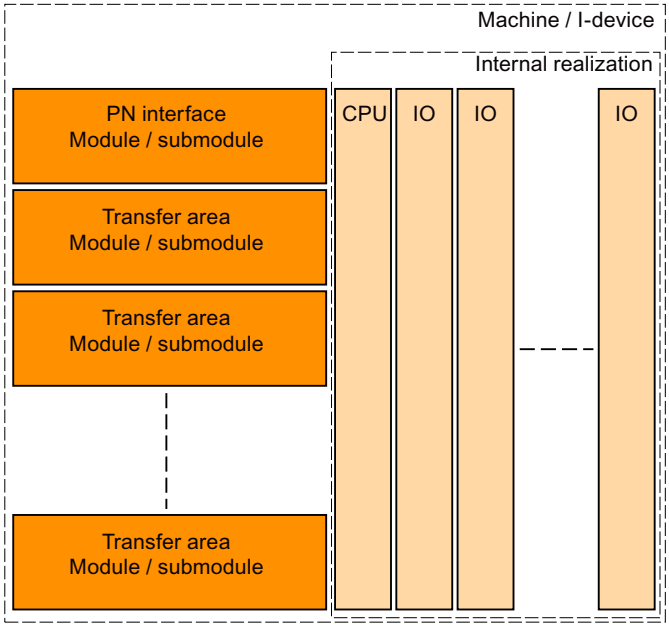


Figure 3-339 Assets of an I-device

Requirement

- S7-1500 CPU as of firmware V2.5.2, configured as I-device
- STEP 7 (TIA Portal) as of V15
- If an IO controller is to read the asset management record:
  The PROFINET IO controller is programmed correspondingly to read an asset management record.
  For a SIMATIC IO controller, for example, you call a read instruction (RDREC) with record index 0xF880. The instruction addresses any submodule of the I-device, for example the first configured transfer area submodule.

Basic procedure

The following steps are fundamentally required to create the requirements so that an I-device can make its local modules available as an asset management record to a requesting IO controller:

1. Make the settings in the properties of the PROFINET interface of the CPU.
   - Activate "IO device" operating mode
   - Activate the "Activate asset management using user program" option
     PROFINET interface forwards a request of an IO controller to the user program of the I-device for reading the asset management record only if the option is selected.

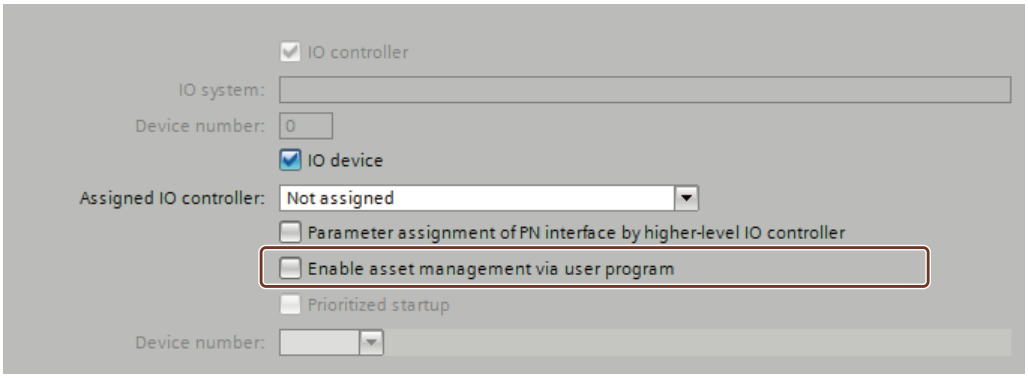


Figure 3-340 Activating asset management using a data record

2. Configure the program routine for compiling the asset management record. The program part collects the required I&M0 data of the plugged central modules and stores them in the corresponding fields of the data record structure of the asset management record.
3. Configure the program part for coordinating the data record provision:
   For this, call the instruction PRVREC (Provide Record) in accordance with the following templates in the corresponding modes:
   - Cyclic calling (for example in the cycle OB) of the PRVREC instruction with Mode 0, in order to recognize the AMR request.
   - When the AM record request is recognized, the PRVREC program has to acknowledge within one second that the request has been recognized. This means that PRVREC must be called with the Mode 2, and with the required AM record. If the I-device does not adhere to the time frame, the I-device acknowledges the record request of the IO controller as negative.

Particular aspect for configuration of the PRVREC call: PRVREC has to be called with **F_ID = 0**. This codes that this is an IO-device-specific data record. The SLOT and SUBSLOT output parameters therefore also return the value 0.

– Within 10 seconds the AM record now has to be completed and PRVREC be called with Mode 3 (positive response to the IO controller with provision of the AM record). If the I-device does not adhere to the time frame, the I-device acknowledges the record request of the IO controller as negative.

A detailed description of the PRVREC instruction and possible error codes for evaluating the function can be found in the online help of STEP 7 (TIA Portal).

Compilation of the asset management record

You have various possibilities for compiling the asset management record for an I-device:

- Recommendation: The Siemens Industry Online Support makes an application available to you that helps you to compile the asset management record.
  The data area of the asset management record is divided in two. The first part consists of an automatically determined area that packages the IM0 data of the slots of the I-device into an asset management block. The second part consists of the user-specific asset management blocks. You configure the user-specific asset management blocks based on pre-configured asset management record structures, fill them with information and make them available to the application.
  The application performs the following:
  – The application determines the required size of all the asset management blocks.
  – The application fills the data block in accordance with the specifications of an asset management record with the automatically determined asset management blocks and your user-specific asset management blocks.
  – The application makes this asset management record available to the higher-level IO controller.

  The application is described in this application example (https://support.industry.siemens.com/cs/ww/en/view/109748894)
- You create the asset management record yourself.
  The following section describes how you can compile an asset management record for an I-device yourself.
  The concept assumes you yourself determine the I&M data for each centrally plugged module and fill the asset management record with this information. The I&M0 data of a module contains basic information about the module such as the manufacturer's code, article number, serial number, hardware and firmware version. These are the data that are also required in the AM record for an asset.

Determine the I&M data of centrally plugged modules

The central structure consists of an optionally plugged power supply unit (Slot 0), followed by the I-device CPU (Slot 1), and then followed by the further modules, such as digital modules, analog modules, etc. (as of Slot 2).

You determine the I&M data with the "Get_IM_Data" instruction for the plugged modules with exception of the CPU:

To assign parameters for the "Get_IM_Data" instruction, you require the hardware identifier (LADDR input parameter). You determine the hardware identifier for each occupied slot with the "GEO2LOG" instruction (Determine hardware identifier from slot).

Summary of the theoretical steps:

1. In a loop, determine the hardware identifiers of the plugged modules with the "GEO2LOG" instruction.
2. For each hardware identifier found, determine the I&M data by using the "Get_IM_Data" instruction and store these data in a data block that you address with the input parameter DATA. Use ARRAY of BYTE for the data storage. This corresponds to the description of the AM record contents in the preceding section.

Forming an AM record with the determined I&M data

The following sections are based on the description of the fundamental structure of the AM record, see the preceding section.

Since each module of an S7-1500 contains hardware and firmware information, select the coding for "AM_FullInformation" for the assigned BlockType.

For the data types used:

- IM_Annotation, IM_OrderID, AM_SoftwareRevision and AM_HardwareRevision: Characters (UTF-8)
- IM_Serial_Number: Characters ("ASCII characters") with the exception of the characters for DEL (0x7F)
- Do not use String data types. They require additional bytes and therefore do not conform to the conventions of the PROFINET standard 61158-6-10 "Application layer protocol specification".

Form the AM_FullInformationBlock for each module as follows:

Table 3-44 AM_FullInformationBlock for modules

Data record element	Description
IM_UniqueIdentifier	Generate a (pseudo) random UUID (hash value) in accordance with ISO 9834-8 as follows: • Generate an 8-byte hash value across the I&M0 data of the module (as of Slot 2). Use the algorithm Fowler-Noll-Vo (in short: FNV); an algorithm for generating variance coefficients (hash values) across data field, see corresponding example code in the Internet or online support. • Generate an 8-byte hash value across the I&M0 data of the CPU. (Use the algorithm Fowler-Noll-Vo (in short: FNV) as described above) • IM_UniqueIdentifier Byte 0 to 7: Hash value of module I&M0 data Bytes 8 to 15: Hash value for CPU-I&M0 data Required customizations to ISO 9834-8: Byte 8, Bit 7 has to be set to 1, and Byte 8, Bit 6 to 0 (result of the AND operator with **00**11 1111, subsequent OR operator with **10**00 0000) Byte 6, Bit 4 to 7 have to be set to 0100 (result of the AND operation with 0000 1111, then OR operation with 0001 0000) Since this algorithm is based on the I&M0 data of the CPU as well as of the modules, it generates a constant IM_UniqueIdentifier for an individual module. When the configuration changes the IM_UniqueIdentifier also changes.
AM_Location	Byte 0 = 0x02 (slot-oriented coding), see description in the preceding section.
IM_Annotation	Example: "S7-1500 module" and pad the remaining bytes of IM_Annotation with spaces (0x20).
IM_OrderID	Copy 20 bytes of the I&M0 data of the module (beginning with offset 2 of the I&M0 data). Pad the remaining 44 bytes with spaces (0x20)

Data record element	Description
AM_SoftwareRevision	Pad the field with 64 spaces (0x20)
AM_HardwareRevision	Pad the field with 64 spaces (0x20)
IM_Serial_Number	Copy 16 bytes of the I&M0 data of the module (beginning with offset 22 of the I&M0 data)
IM_Software_Revision	Copy 4 bytes of the I&M0 data of the module (beginning with offset 40 of the I&M0 data)
AM_DeviceIdentification	Byte 0, 1, 2, 6, 7 = 0x00 Byte 3 = 0x2A (Vendor = Siemens) Byte 4 = 01, Byte 5 = DeviceID (e.g. CPU 15xx = 0x0E)
AM_TypeIdentification	Copy 2 bytes of the I&M0 data of the module (beginning with offset 48 of the I&M0 data)
IM_Hardware_Revision	Copy 2 bytes of the I&M0 data of the module (beginning with offset 38 of the I&M0 data)

Functions

7

Introduction

The following section describes the PROFINET IO functions for field of application, properties and configuration in STEP 7.

Refer to the documentation for the respective device to see to what extent the PROFINET devices support the described functions.

You can find a tabular overview of the PROFINET devices and the functions these support on the Internet (https://support.industry.siemens.com/cs/ww/en/view/102325771).

7.1 Connecting other bus systems

Fieldbus integration

PROFINET allows you to use a proxy-capable PROFINET device to integrate existing fieldbus systems (for example, PROFIBUS, AS interface). The devices of these fieldbus systems are mapped on proxy PROFINET devices. In this way, you can set up any hybrid systems consisting of fieldbus and Ethernet-based subsystems. This allows a continuous exchange of information.

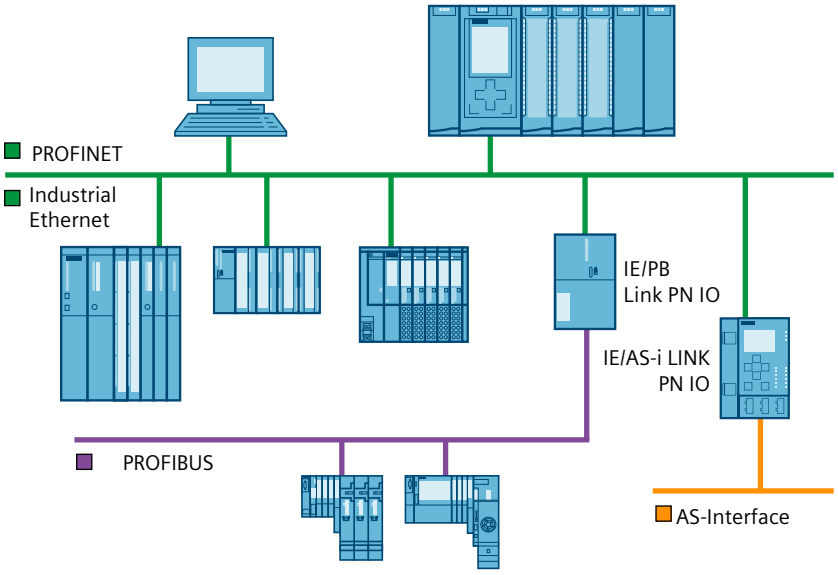


Figure 3-341 Gateways on PROFINET IO

Gateways of an S7-1500 CPU

An overview of the gateways at an S7-1500 CPU is provided in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/88778900).

Connecting to building busses

- BACnet: You can find the procedure for configuring communication between a SIMATIC PLC and a BACnet network with a gateway in this application example (https://support.industry.siemens.com/cs/ww/en/view/109476182).
- M-bus: You can find the procedure for configuring communication between a SIMATIC PLC and an M-bus network with a gateway in this application example (https://support.industry.siemens.com/cs/ww/en/view/109478527).
- DALI: You can find the procedure for configuring communication between a SIMATIC PLC and a DALI network with a gateway in this application example (https://support.industry.siemens.com/cs/ww/en/view/109740160).
- KNX: You can find the procedure for configuring communication between a SIMATIC PLC and a KNX network with a gateway in this application example (https://support.industry.siemens.com/cs/ww/en/view/109739689).

7.1.1 Linking PROFINET and PROFIBUS

Linking PROFINET and PROFIBUS

With a proxy-capable PROFINET device which is equipped with a PROFINET interface in addition to a PROFIBUS interface (for example, IE/PB Link PN IO), you can integrate existing PROFIBUS configurations into the PROFINET configuration.

The following figures shows how a PROFIBUS system is connected via IE/PB Link to a CPU S7-1500 (as of firmware version 1.7).

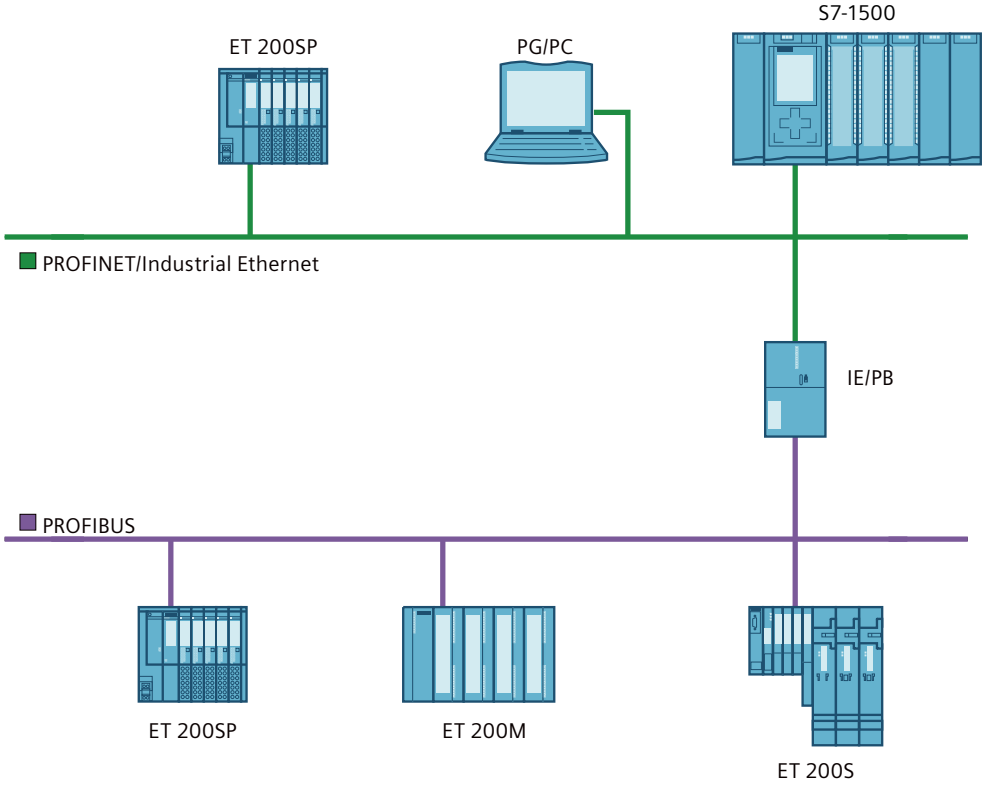


Figure 3-342 Gateway from PROFINET and PROFIBUS via IE/PB link

PROFINET device with proxy functionality

The PROFINET device with proxy functionality is the substitute for a PROFIBUS device on Ethernet. The proxy functionality allows a PROFIBUS device to communicate not only with its master but also with all devices on PROFINET.

With PROFINET you can connect an existing PROFIBUS system to an IO controller, for example with the help of an IE/PB Link PN IO.

From the IO controller perspective, the PROFIBUS DP slaves are connected to the same network as the IE/PB Link PN IO. These slaves have the same device name and IP address as the IE/PB Link PN IO, but different device numbers. Furthermore, each also has a specific PROFIBUS address.

In this way, you can link both DPV0 and DPV1 slaves to PROFINET.

For information on how to connect a DP slave to a PROFINET IO system, refer to section Connect the DP slave via the IE/PB Link to a PROFINET IO system (Page 119).

Diagnostic options with a CPU S7-1500 as IO controller

The CPU S7-1500 (as of firmware version 1.7) as IO controller detects disrupted DP slaves behind the IP/PB link.

7.1.2 Connect the DP slave via the IE/PB Link to a PROFINET IO system

Requirements

- STEP 7 as of V13 SP1
- CPU supports IE/PB link, e.g.:
  - S7-1500 CPU as of firmware version 1.7
  - S7-1500 Software Controller as of firmware version 1.7
  - S7-300/400 CPU

Procedure for connecting a DP slave via an IE/PB Link

To connect a DP slave to a PROFINET IO system via an IE/PB Link in STEP 7, follow these steps:

1. Drag-and-drop a PROFINET CPU, for example CPU 1513-1 PN, from the hardware catalog into the network view of STEP 7.
2. Drag-and-drop an IE/PB Link PN IO from the hardware catalog into the network view of STEP 7. The IE/PB Link PN IO is located under Network components > Gateways > IE/PB Link PN IO.
3. Assign the IE/PB Link PN IO to the CPU.
4. Drag a PROFIBUS interface module e.g. IM155-6 DP HF, from the hardware catalog to the network view.

5. Assign the interface module to the IE/PB Link.

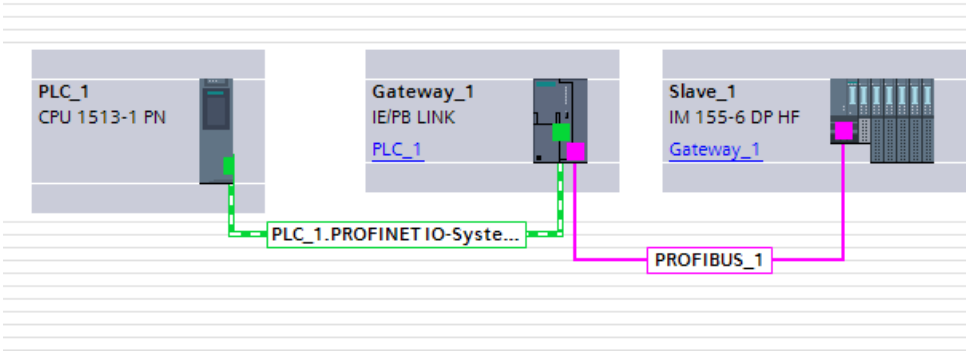


Figure 3-343 Configuring an IE/PB link

6. Select the IE/PB Link PN IO in the network view of STEP 7.
7. In the Inspector window, go to the "Gateway" area and select the "Network gateway as PROFINET IO proxy" option.

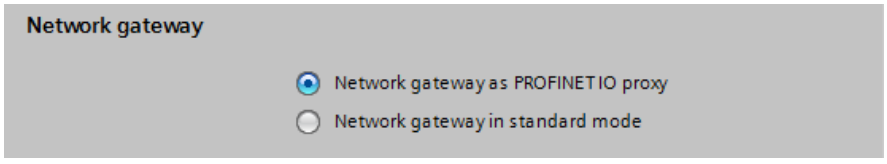


Figure 3-344 Setting a gateway

8. In the PROFINET device number area, you can assign a PROFINET device number for the DP slave.
   If you have selected the "Device number = PB address" check box (default), STEP 7 automatically assigns the device number according to the PROFIBUS address of the slave. In addition, you no longer need to update the device number if the PROFIBUS address changes.

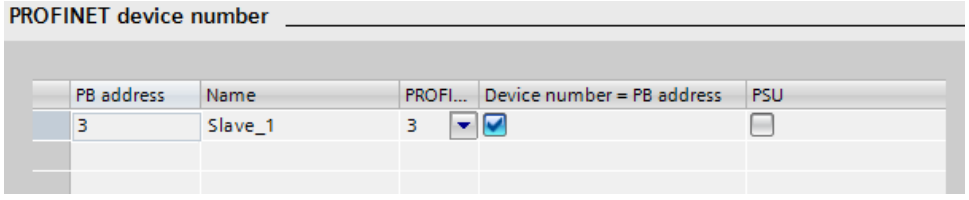


Figure 3-345 Assigning PN device numbers for IE/PB link

Result

You have connected the DP slave to the PROFINET IO system.

Reference

Additional information on the IE/PB link is available in the manual Gateway IE/PB Link PN IO (http://support.automation.siemens.com/WW/view/en/19299692).

7.2 Intelligent IO devices (I-devices)

7.2.1 I-device functionality

I-device functionality

The "I-device" (intelligent IO device) functionality of a CPU facilitates data exchange with an IO controller and operation of the CPU as intelligent preprocessing unit of sub processes, for example. The I-device is linked as an IO device to a "higher-level" IO controller.

The preprocessing is handled by the user program in the I-device. The process values acquired in the centralized or distributed (PROFINET IO or PROFIBUS DP) I/O are preprocessed by the user program and made available to the IO controller.

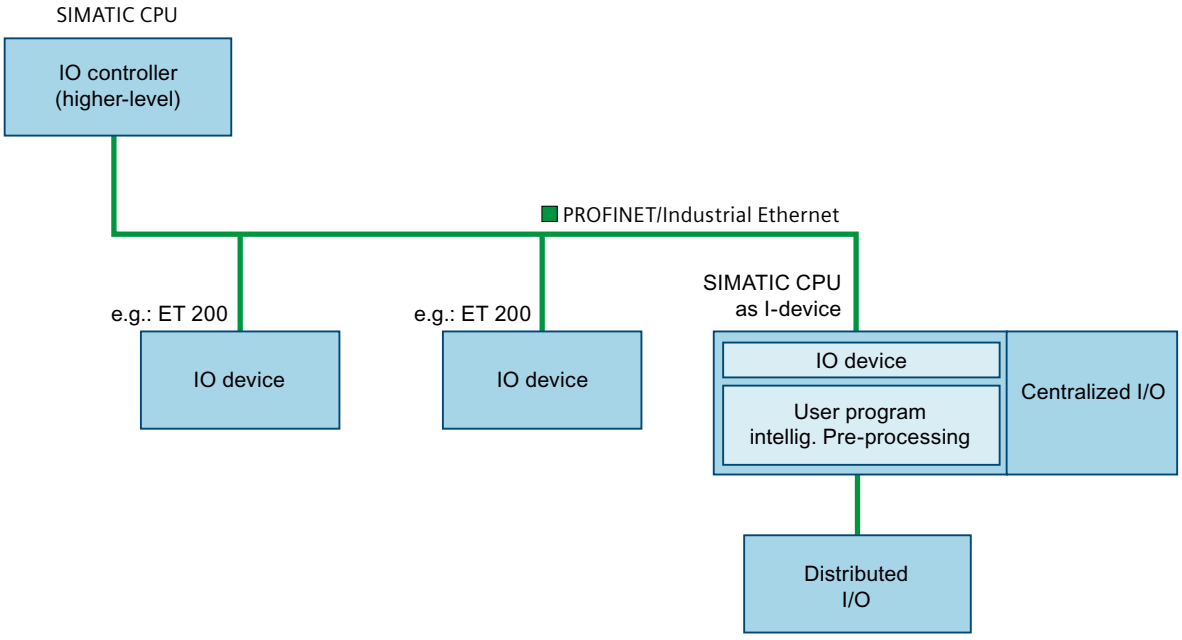


Figure 3-346 I-device

"I-device" naming conventions

In the remainder of this description, a CPU or a CP with I-device functionality is simply called an "I-device".

Application example: Configuration and application of the PROFINET I-device function

A detailed application example is available here (https://support.industry.siemens.com/cs/ww/en/view/109478798).

7.2.2 Properties and Advantages of the I-Device

Fields of application

Fields of application of the I-device:

- Distributed processing

  A complex automation task can be divided into smaller units/subprocesses. This results in manageable processes which lead to simplified subtasks.
- Separating subprocesses

  Complicated, widely distributed and extensive processes can be subdivided into several subprocesses with manageable interfaces by using I-devices. These subprocesses can be stored in individual STEP 7 projects if necessary, which can later be merged to form one master project.
- Know-how protection

  Components can only be delivered with a GSD file for the I-device interface description instead of with a STEP 7 project. The know-how of the user program may no longer be published.

Properties

Properties of the I-device:

- Unlinking STEP 7 projects

  Creators and users of an I-device can have completely separated STEP 7 automation projects. The GSD file forms the interface between the STEP 7 projects. This allows a link to standard IO controllers via a standardized interface.
- Real-time communication

  The I-device is provided with a deterministic PROFINET IO system via a PROFINET IO interface and therefore supports RT (real-time communication) and IRT (isochronous real time).

Advantages

The I-device has the following advantages:

- Simple linking of IO controllers
- Real-time communication between IO controllers
- Relieving the IO controller by distributing the computing capacity to I-devices.
- Lower communication load by processing process data locally.
- Manageable, due to processing of subtasks in separate STEP 7 projects

7.2.3 Characteristics of an I-Device

Principle

An I-device is included in an IO system like a standard IO device.

I-device without lower-level PROFINET IO system

The I-device does not have its own distributed I/O. The configuration and parameter assignment of the I-devices in the role of an IO device is the same as for a distributed I/O system (for example ET 200).

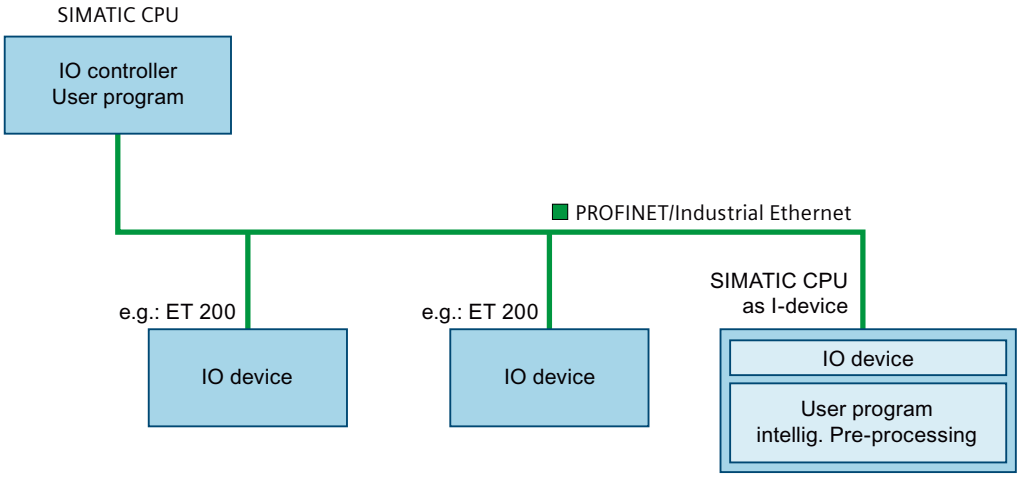


Figure 3-347 I-device without lower-level PROFINET IO system

I-device with lower-level PROFINET IO system

Depending on the configuration, an I-device can also be an IO controller on a PROFINET interface in addition to having the role of an IO device.

This means that the I-device can be part of a higher-level IO system via its PROFINET interface and as an IO controller can support its own lower-level IO system.

The lower-level IO system can, in turn, contain I-devices (see figure below). This makes hierarchically structured IO systems possible.

In addition to its role as IO controller, an I-device can also be used via a PROFIBUS interface as DP master for a lower-level PROFIBUS system.

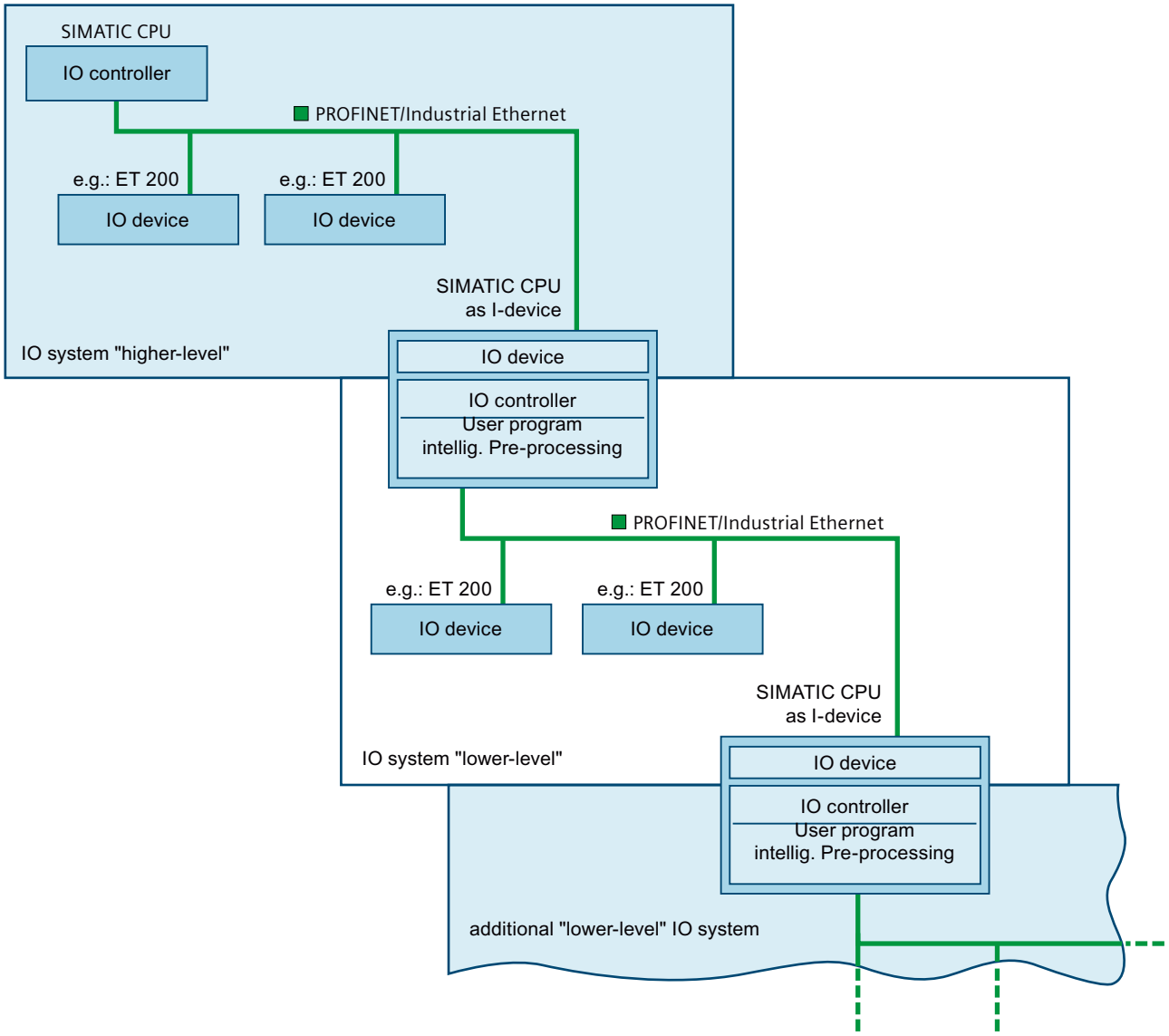


Figure 3-348 I-device with lower-level IO system

Example - the I-device as IO device and IO controller

The I-device as IO device and IO controller is explained based on the example of a print process. The I-device controls a unit (a subprocess). One unit is used, for example, to insert additional sheets such as flyers or brochures in a package of printed material.

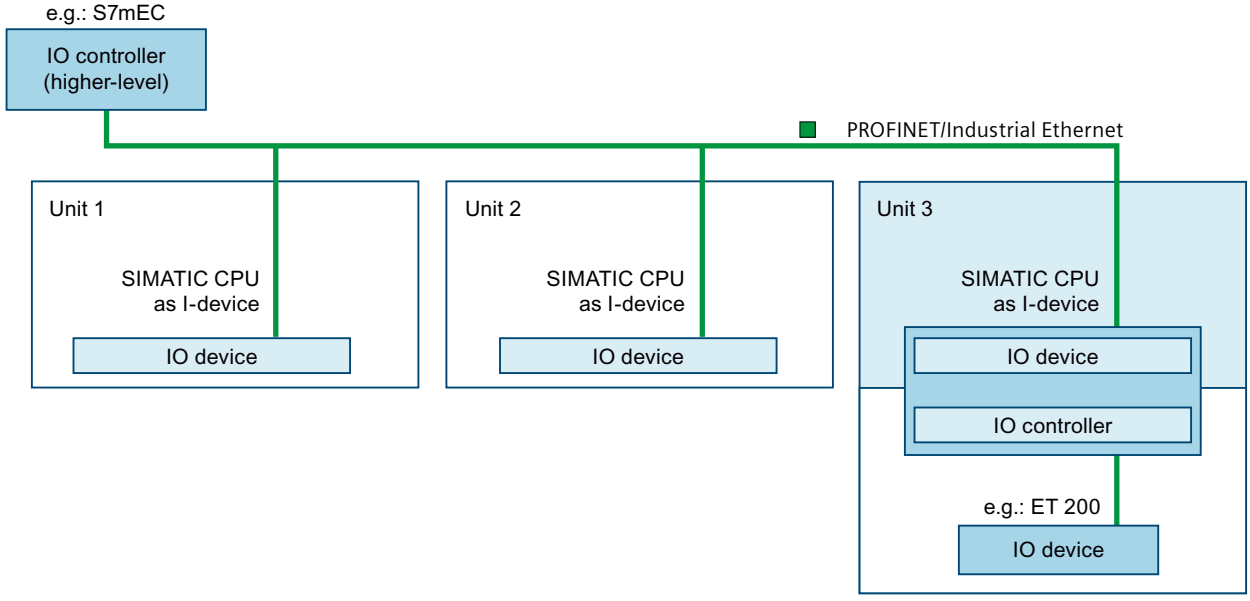


Figure 3-349 Example - the I-device as IO device and IO controller

Unit 1 and unit 2 each consist of an I-device with centralized I/O. The I-device along with the distributed I/O system (for example ET 200) forms unit 3.

The user program on the I-device is responsible for preprocessing the process data. For this task, the user program of the I-device requires default settings (for example control data) from the higher-level IO controller. The I-device provides the higher-level IO controller with the results (for example status of its subtask).

I-device as a shared device

An I-device can also be used simultaneously by multiple IO controllers as a shared device.

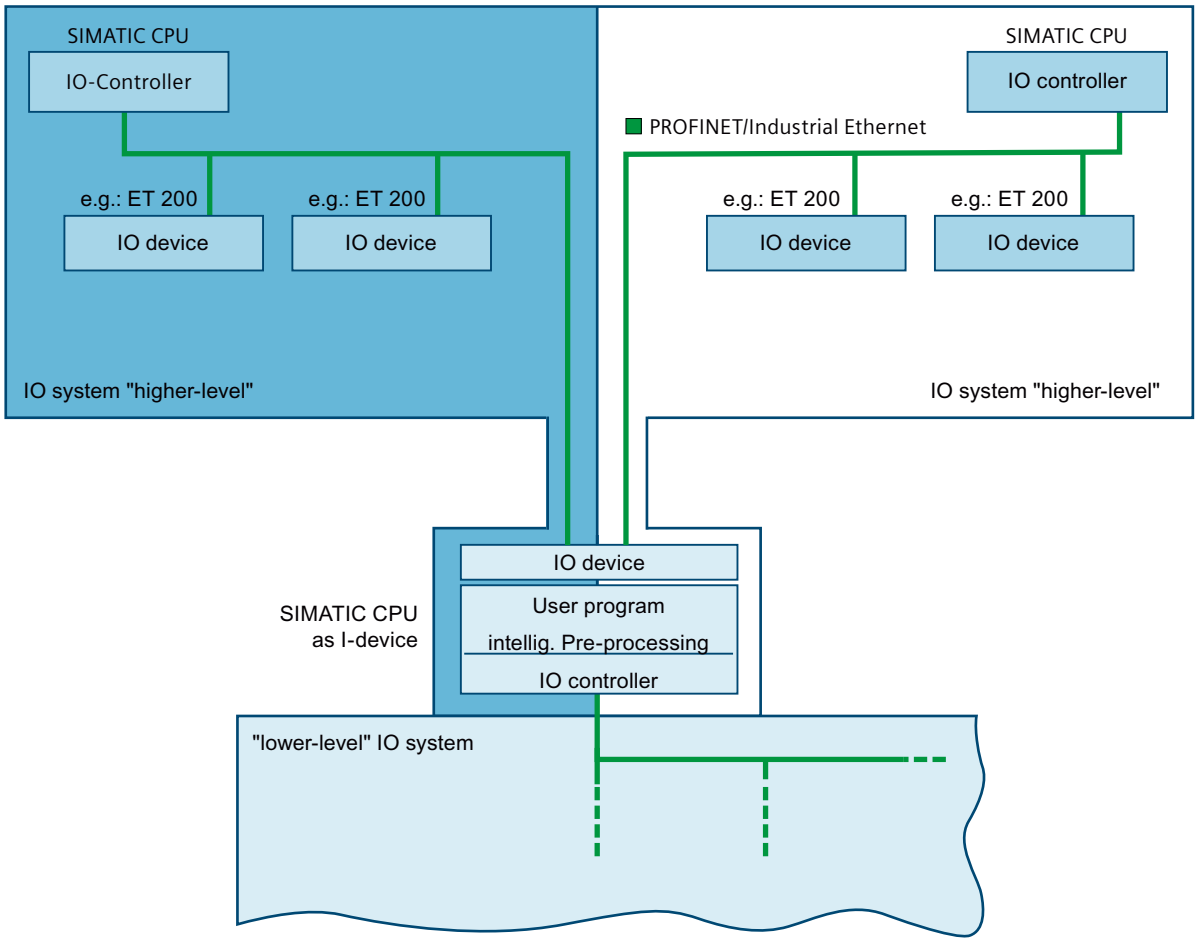


Figure 3-350 I-device as a shared device

Information about configuring an I-device as a shared device is available in the section Configuring a shared I-device in different projects (Page 167).

7.2.4 Data Exchange between higher- and lower-level IO system

Introduction

The next chapter shows the data exchange between the higher- and lower-level IO system.

Transfer areas

Transfer areas are an interface to the user program of the I-device CPU. Inputs are processed in the user program and outputs are the result of the processing in the user program.

The data for communication between IO controller and I-device is made available in the transfer areas. A transfer area contains an information unit that is exchanged consistently between IO controller and I-device. You can find more information on configuration and use of transfer areas in the section Configuring the I-device (Page 129).

The next figure shows the data exchange between the higher- and lower-level IO system. The individual communication relations are explained below based on the numbers.

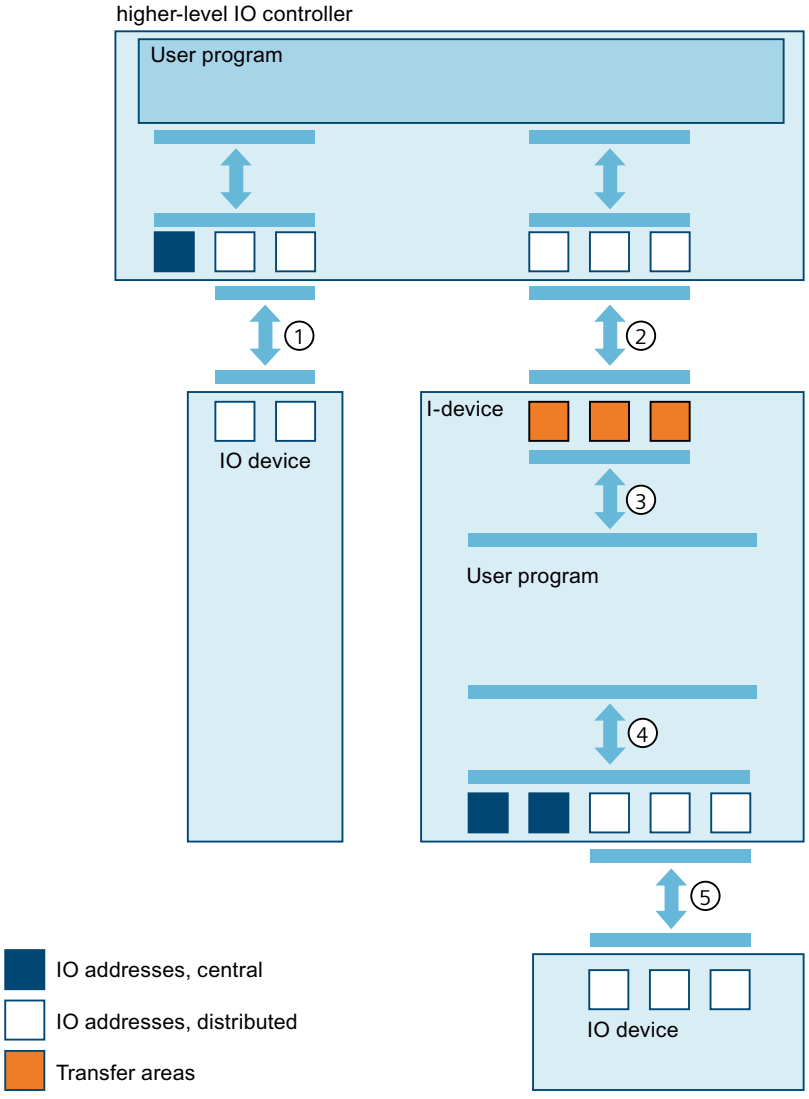


Figure 3-351 Data exchange between higher- and lower-level IO system

① Data exchange between higher-level IO controller and normal IO-device
In this way, the IO controller and IO devices exchange data through PROFINET.

② Data exchange between higher-level IO controller and I-device
In this way, the IO controller and the I-device exchange data through PROFINET.

The data exchange between a higher-level IO controller and an I-device is based on the conventional IO controller / IO device relationship.

For the higher-level IO controller, the transfer areas of the I-devices represent submodules of a preconfigured station.

The output data of the IO controller is the input data of the I-device. Analogously, the input data of the IO controller is the output data of the I-device.

③ **Transfer relationship between the user program and the transfer area**
In this way, the user program and the transfer area exchange input and output data.

④ **Data exchange between the user program and the I/O of the I-device**
In this way, the user program and the centralized / distributed I/O exchange input and output data.

⑤ **Data exchange between the I-device and a lower-level IO device**
In this way, the I-device and its IO devices exchange data. The data transfer is via PROFINET.

7.2.5 Configuring the I-device

Introduction

There are basically two possibilities for configuration:

- Configuration of an I-device within a project
- Configuration of an I-device that is used in another project or in another engineering system.

STEP 7 allows you to configure an I-device for another project or for another engineering system by exporting a configured I-device to a GSD file. You import the GSD file in other projects or engineering systems as with other GSD files. The transfer areas for the data exchange, among other data, are stored in this GSD file.

Configuration of an I-device within a project

1. Drag-and-drop a PROFINET CPU from the hardware catalog into the network view.
2. Drag-and-drop a PROFINET CPU, which can also be configured as an IO device, from the hardware catalog into the network view. This device is configured as I-device (e.g., CPU 1516-3 PN/DP).
3. Select the PROFINET interface for the I-device.
4. In the Inspector window in the area navigation choose "Operating mode" and select the check box "IO device".

5. Assign the I-device to an IO controller as follows:
   – For CPUs as of FW version V3.1:
   Click "Assign to new IO controller" in the "Assigned IO controllers" table.
   In the drop-down menu, select the PROFINET interface of the IO controller to which you want to assign the I-device.

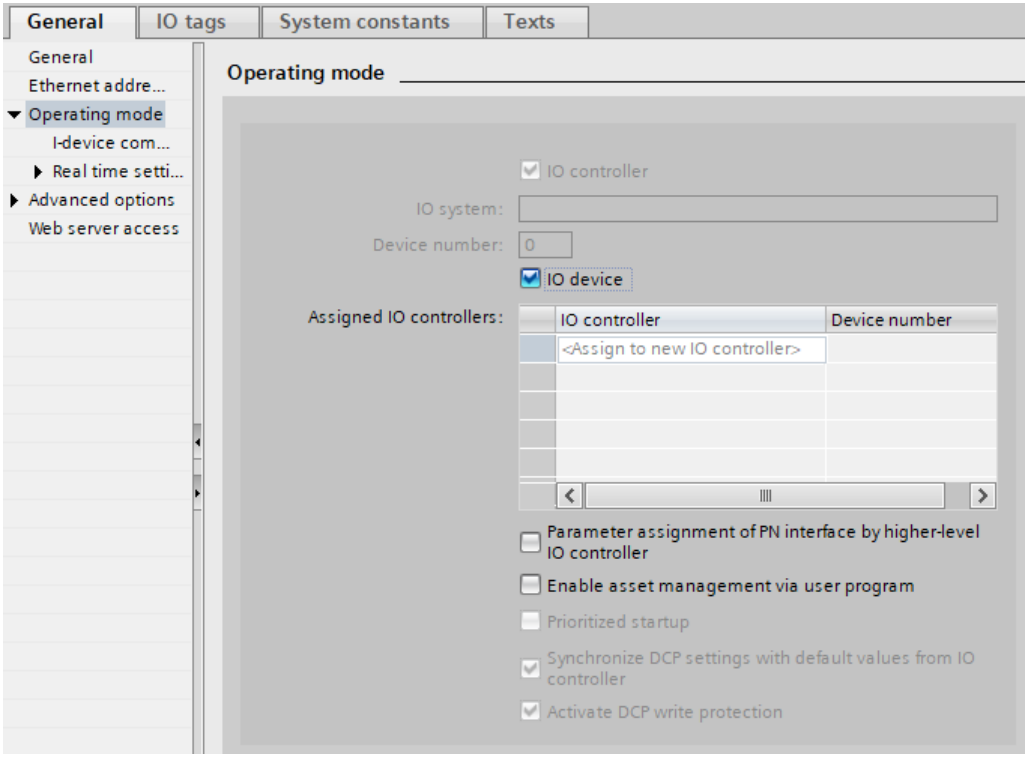


Figure 3-352 Configuring I-device with CPUs as of FW version V3.1

   – For CPUs up to FW version V3.0:
   In the "Assigned IO controller" drop-down menu, select the PROFINET interface of the IO controller to which you want to assign the I-device.

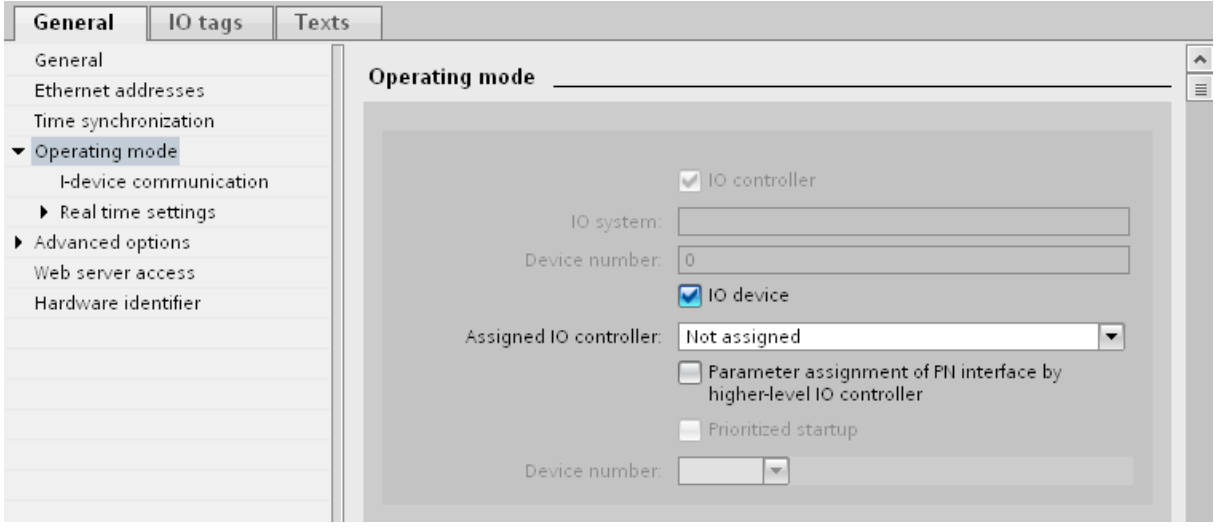


Figure 3-353 Configuring I-device for CPUs up to FW version V3.0

Once you have chosen the IO controller, the networking and the IO system between both devices are displayed in the network view.

6. Use the "Parameter assignment of the PN interface by higher-level IO controller" check box to determine whether the interface is configured by the I-device itself or by the higher-level IO controller.

   If you operate the I-device with a lower-level IO system, then the parameters of the I-device PROFINET interface (for example, port parameter) cannot be assigned with the higher-level IO controller.

7. Configure the transfer areas. The transfer areas are found in the area navigation section "I-device communication".
   - Click in the first field of the "Transfer area" column. STEP 7 assigns a default name that you can change.
   - Select the type of communication relation: you can currently only select CD or F-CD for "Controller-device communication relation".
   - Addresses are automatically preset; you can correct addresses if necessary, and determine the length of the transfer area which is to be consistently transferred.

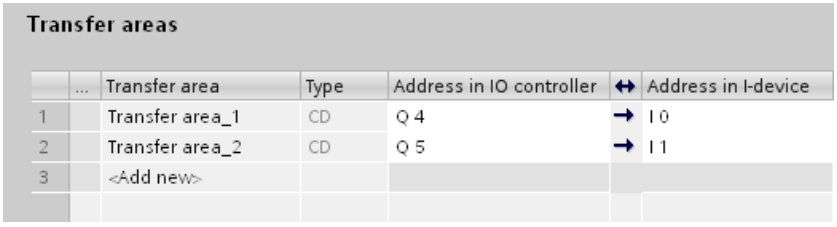


Figure 3-354 Configuring the transfer areas

8. A separate entry is created in the area navigation for each transfer area. If you select one of these entries, you can adjust the details of the transfer area, or correct them and comment on them.

NOTE

Device replacement in the configuration

If you want to exchange a configured CPU (I-device) with FW version < V3.1 for a CPU with FW version V3.1, the new I-device cannot be used as a shared I-device within the project.

To use the new I-device as a shared I-device within the project, you must deselect the "IO device" option at the relevant PROFINET interface of the current device before changing the module.

Configuring an I-device and exporting as a GSD file

If you use an I-device in another project, or if the I-device is used in another Engineering System, then configure the I-device as described above.

Once you have configured the I-device, you must export the I-device as a GSD file. This GSD file serves as a substitute for the configured I-device in other projects. If required, you can export an I-device that was created from a CPU as of FW version V4.1 as a GSD file for a signable GSDX file. This fulfills one of the requirements for PROFINET Security Class 1. You can find information on the use of GSD files in GSDX files in the section PROFINET Security Class 1 (Page 36).

To export a configured I-device as GSD file, proceed as follows:

1. In the Inspector window, navigate to the "Operating mode > I-device communication" area in the "Export generic station description file (GSD)" field.
2. Optional when using the GSD file in a GSDX file:
   – Select the "Use Distributor ID in the exported file" check box
   The text box for the distributor ID becomes editable.
   – Enter your distributor ID in the box.
   If the text box is empty or more than 40 characters have been entered, STEP 7 displays the text box in red.

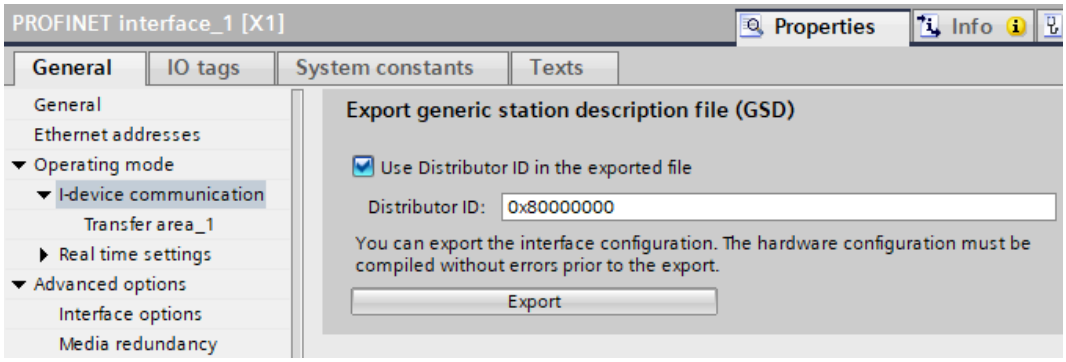


Figure 3-355 Export generic station description file (GSD)

3. Compile the CPU configured as an I-device.
   The export as GSD file only works immediately after the compiling process. If you change the configuration, you need to compile the CPU configured as an I-device again.
   The "Export" button in the "Operating mode > I-device communication > Export device description file (GSD)" area can be selected.
4. Click the "Export" button
   The export dialog opens.
5. Assign a name for the I-device proxy as well as a description and a storage location (path) in the fields provided. Click the "Export" button to complete the process.

Result: You have exported the configured I-device as a GSD file. You can then import the exported GSD file into other projects, for example, or make it available together with the I-device for integration into customer projects.

7.2.6 Program examples

Introduction

This simple program example shows how you use the transfer areas of an I-device.

Requirements

You have configured an I-device.

Task

The result of an "AND logic operation" of two inputs (preprocessing) in the I-device is to be provided to the higher-level IO controller. This result is to be assigned to a local output in the IO master (further processing).
Use a transfer area with the following addresses for this purpose:

- Address in the I-device: Q568
- Address in the IO controller: I68

Required steps

The following steps to solve the task:

1. Configuring the transfer area
2. Programming I-device
3. Programming IO controller

Configuring the transfer area

Configure a transfer area with the following properties in the I-device:

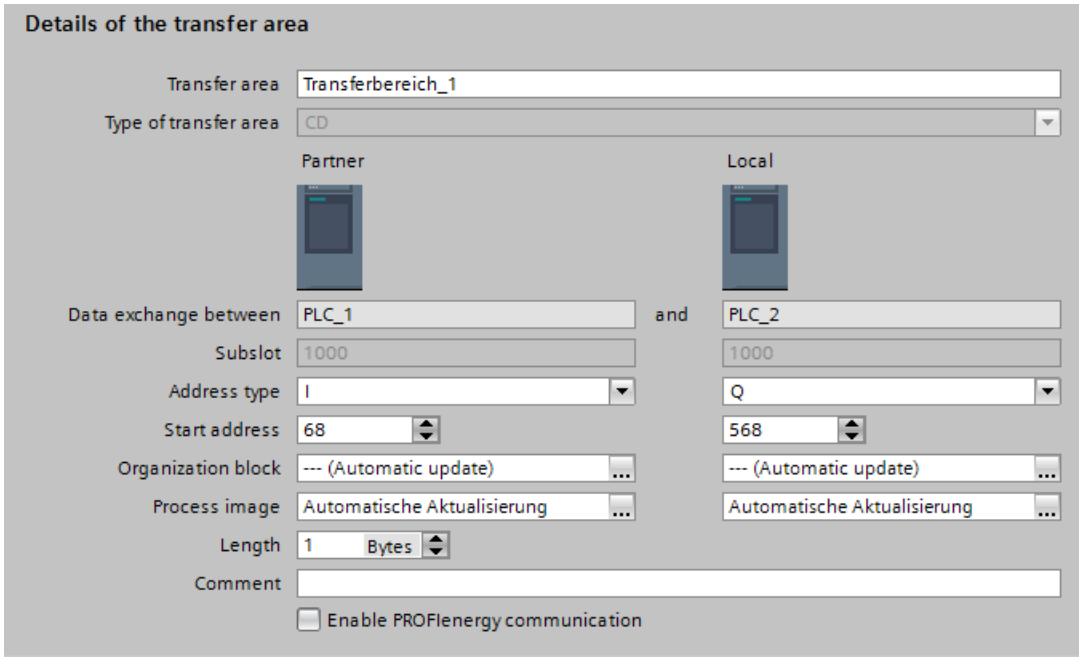


Figure 3-356 I-device transfer area, sample program

Programming I-device

To program the sample program for the I-device, follow these steps:

1. Using the SCL programming language, create a new function with the name "preprocessing" in the project tree in "Program blocks" > "Add new block". Open the function.
2. In the interface of the function "preprocessing", create the following tags:

Name	Data type	Input / output type
input 1	bool	Input
input 2	bool	Input
result	bool	Output

3. In the instruction window of the function "preprocessing", write the following program code:
   #result:=#input 1&#input 2;
4. Call the function "preprocessing" in a program cycle OB, for example, in OB1.
5. Wire the function "preprocessing" in the program cycle OB as follows:

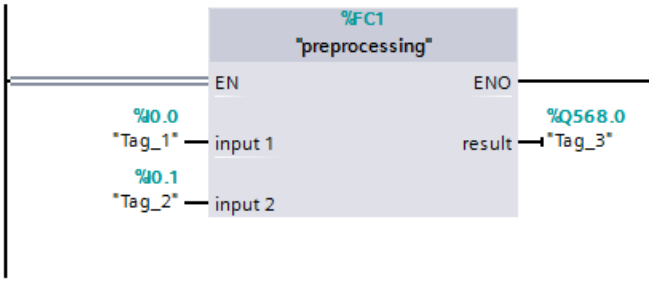


Figure 3-357 I-device sample program

Programming IO controller

To program the sample program for the IO controller, follow these steps:

1. Using the SCL programming language, create a new function with the name "further processing" in the project tree in "Program blocks" > "Add new block". Open the function.
2. In the interface of the function "further processing", create the following tags:

Name	Data type	Input / output type
result	bool	Input
output	bool	Output

3. In the instruction window of the function "further processing", write the following program code:
   #output:=#result;
4. Call the function "further processing" in a program cycle OB, for example, in OB1.

5. Wire the function "further processing" in the program cycle OB as follows:

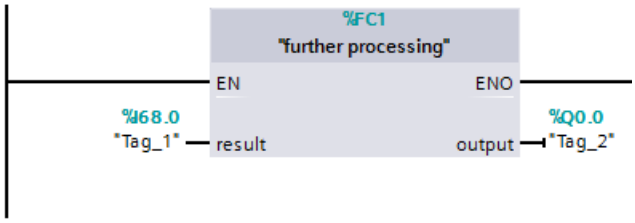


Figure 3-358 IO controller sample program

Result

The IO controller and the I-device can exchange data with each other through the input/output transfer areas.

7.2.7 Diagnostics and interrupt characteristics

Diagnostics and interrupt characteristics

S7 CPUs have numerous diagnostics and interrupt functions that can, for example, report errors or failures of lower-level IO systems. These diagnostics messages reduce down times and simplify localization and elimination of problems.

Diagnostics options in the higher-level IO controller and in the I-device

The following diagnostics functions are available to the higher-level IO controller and the I-device CPU:

- OB 83 (pull/plug)
- OB 86 (rack failure)
- OB 122 (I/O access error)

NOTE

The diagnostics messages of the I/O can be processed in the user program of the I-device CPU and passed on from there to the higher-level IO controller via transfer areas.

Operating state changes and station failure / station return

In the following table, you can see which consequences an operating state change or the failure of an IO controller / I-device of the SIMATIC family has on the respective other(s):

Table 3-45 Operating state changes and station failure / station return

Initial status	Event	I-device response	Higher-level IO controller
I-device CPU is in RUN, higher-level IO controller is in RUN	The I-device CPU changes to STOP	-	During the updating of the process image with the instructions "UPDAT_PI" and "UPDAT_PO" an error report is returned at the parameter RET_VAL. With direct IO access to all transfer areas to the I-device: depending on the type of error handling, e.g., call of OB 122 (IO access error).
I-device CPU is in STOP higher-level IO controller is in RUN	The I-device CPU is starting up	Call of OB 100 (startup). Call of OB 83 (pull/plug) for input transfer areas to the higher-level IO controller. Until call of OB 83 in the case of direct access to the input transfer areas to the higher-level IO controller: depending on the type of error handling, e.g., call of OB 122 (IO access error).	Call of OB 83 (pull/plug) for all transfer areas to the I-device. Until call of OB 83 in the case of direct access to the transfer areas to the I-device: depending on the type of error handling, e.g., call of OB 122 (IO access error).
I-device CPU is in RUN, higher-level IO controller is in RUN	The higher-level IO controller changes to STOP	During the updating of the process image with the instructions "UPDAT_PI" and "UPDAT_PO" an error report is returned at the parameter RET_VAL. With direct IO access to the input transfer areas to the higher-level IO controller: depending on the type of error handling, e.g., call of OB 122 (IO access error). Note: Output transfer areas can still be accessed.	-
Higher-level IO controller is in STOP, I-device CPU in RUN	The higher-level IO controller starts up	Call of OB 83 (pull/plug) for input transfer areas to the higher-level IO controller. Until call of OB 83 in the case of direct access to the input transfer areas to the higher-level IO controller: depending on the type of error handling, e.g., call of OB 122 (IO access error).	Call of OB 100 (startup).
I-device CPU is in RUN, higher-level IO controller is in RUN	Station failure I-device, for example, through bus interruption	If the I-device continues to run without a bus connection: Call of OB 86 (rack failure). During the updating of the process image with the instructions "UPDAT_PI" and "UPDAT_PO" an error report is returned at the parameter RET_VAL. With direct IO access to all transfer areas to the higher-level IO controller: depending on the type of error handling, e.g., call of OB 122 (IO access error).	Call of OB 86 (rack failure). During the updating of the process image with the instructions "UPDAT_PI" and "UPDAT_PO" an error report is returned at the parameter RET_VAL. With direct IO access to all transfer areas to the I-device: depending on the type of error handling, e.g., call of OB 122 (IO access error).

Initial status	Event	I-device response	Higher-level IO controller
I-device CPU is in RUN, higher-level IO controller is in RUN, communication connection between IO controller and I-device is interrupted (bus interruption).	The bus connection between the IO controller and I-device has been reestablished and the I-device is again included in the user data traffic.	Call of OB 86 (rack failure). Call of OB 83 (pull/plug) for input transfer areas to the higher-level IO controller. Until call of OB 83 in the case of direct access to the input transfer areas to the higher-level IO controller: depending on the type of error handling, e.g., call of OB 122 (IO access error).	Call of OB 86 (rack failure). Until reporting of station re-integration by OB 86 with direct IO access to all transfer areas to the I-device: depending on the type of error handling, e.g., call of OB 122 (IO access error)

NOTE

Special characteristic during startup of the higher-level IO controller

In contrast to the station return message from IO devices in the IO controller, which are covered completely by the call of the OB 86, the station return message of a higher-level IO controller in the I-device is separated into 2 parts:

1. Call of the OB 86: The initial values for the outputs of the I-device are set. However, the input values are not yet valid. These values will first be valid with the opening of OB 86 in the higher-level IO controller.
2. Call of OB 83 for each input transfer area; with this call, the validity of an input transfer area is displayed. The starting up of the I device is first complete when the OB 83 has been called for the input transfer areas. This step can be delayed or not occur at all in the following situations:
   - Higher-level IO controller is in STOP: OB 83 is first called at the STOP-RUN transition of the higher-level IO controller.
   - The IRT communication has been disrupted (sync-master failure, topology error, ...). OB 83 is opened only after the IRT communication has taken place.

Reference

For more information on error handling in the case of direct I/O access, refer to "Error handling" in the STEP 7 online help.

7.2.8 Rules for the Topology of a PROFINET IO System with I-Device

Introduction

The following recommendations for the structure and configuration of an IO system when using I-devices will help you to keep the bandwidths required for keeping communication small.

The following communication paths should not overlap:

- Communication paths between the IO controller and the IO device of its IO system.
- Communication paths of the I-device CPU and the IO devices of your IO system.

I-device with one port

Connect an I-device with only one port to a PROFINET switch that is uncoupled from the higher-level IO system. Connect the lower-level IO system to another port of the switch as shown in the following figure.

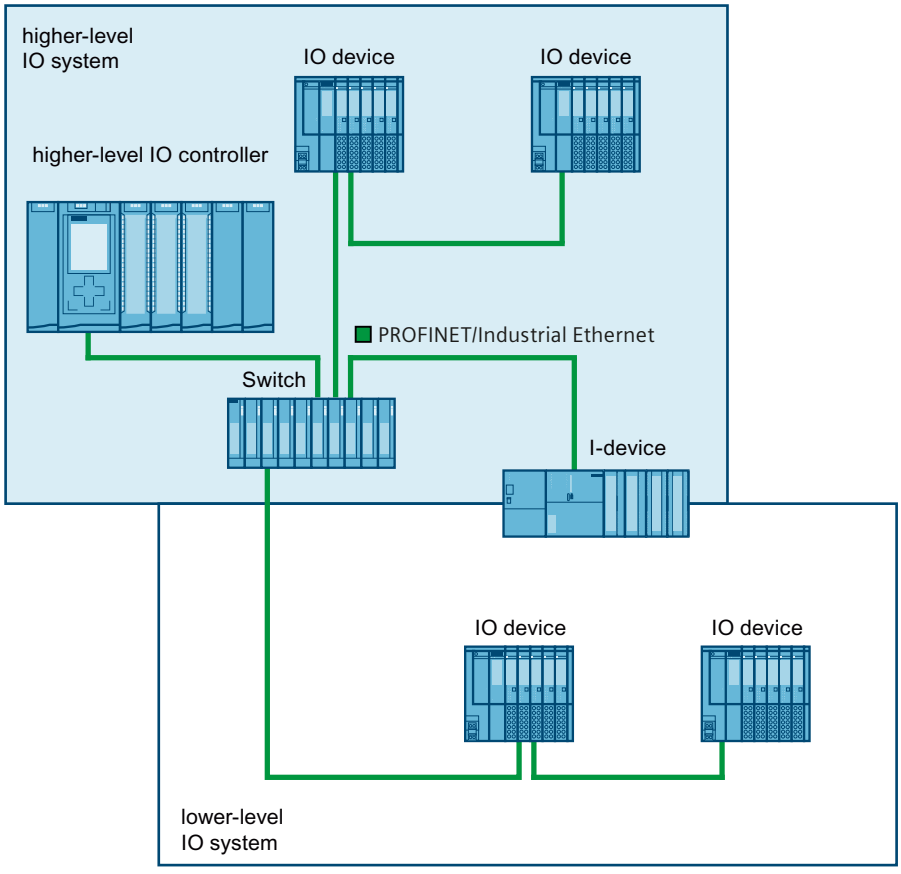


Figure 3-359 I-device with one port

I-device with two ports

With an I-device with two ports, connect one port, uncoupled from the higher-level IO system, to the port of the PROFINET switch. Use the second port for the lower-level IO system as shown in the following figure.

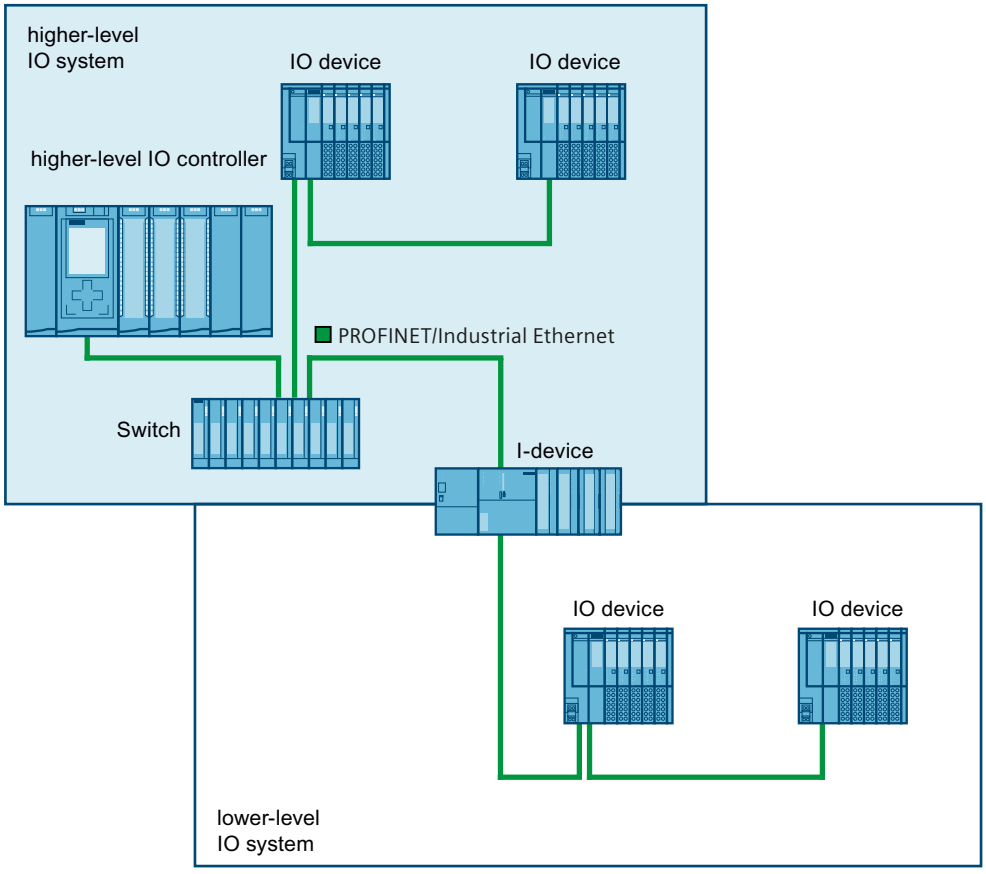


Figure 3-360 I-device with two ports

I-device with three or more ports

If you have an I-device with three or more ports, connect the I-device to one or both ports to the higher-level IO system in a linear bus topology. Connect the third port to the lower-level IO system uncoupled from the linear bus topology as shown in the following figure.

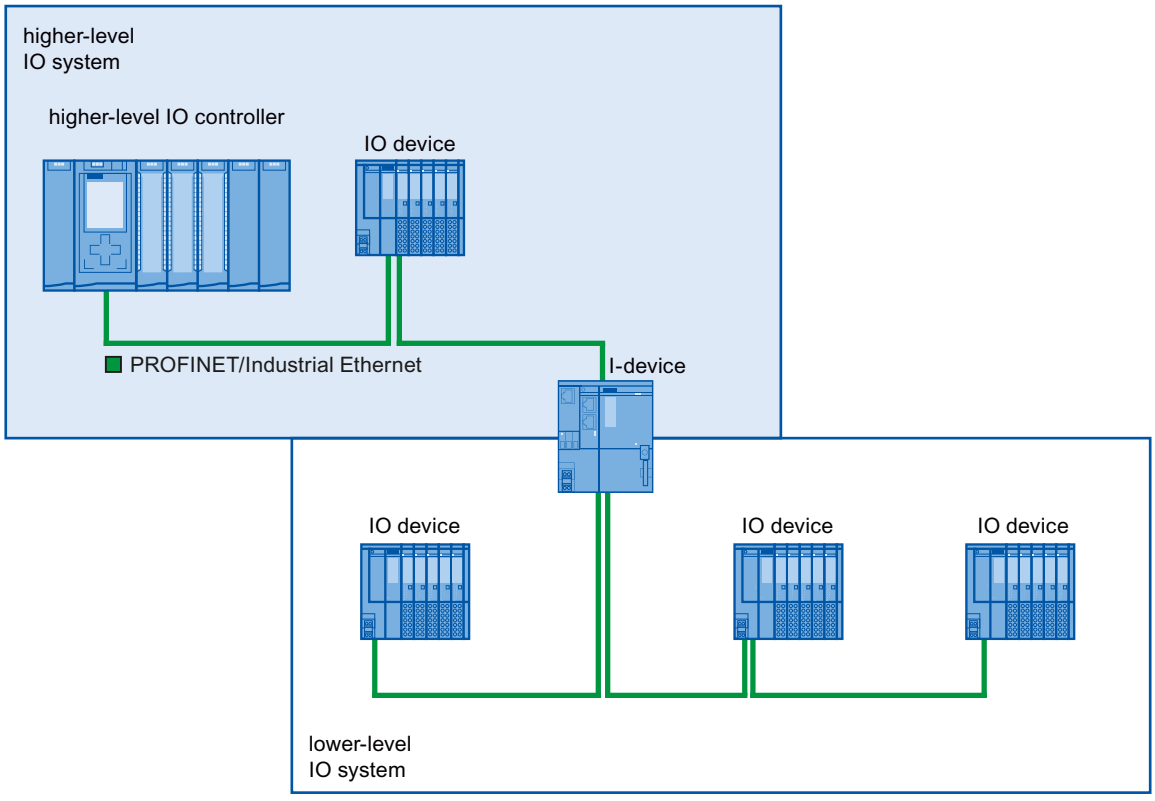


Figure 3-361 I-device with three or more ports

7.2.9 Boundary conditions when using I-devices

Note the following boundary conditions when using I-devices:

Bandwidth

The number of addresses of the configured transfer areas affects the usable bandwidth of the I-device:

- Bandwidth of the transfer areas + bandwidth of the lower-level IO system = total bandwidth used on the I-device

If the address space of the transfer areas is too large, this indicates a larger bandwidth requirement and can thus lead to longer update times.

Tip: Keep the address space of the transfer area as small as possible.

Rules for RT and IRT communication.

IO systems with I-devices are also suitable for setting up real-time applications with RT and IRT communication. The following rules must be followed for this:

- Both the higher-level and the lower-level IO system support RT communication. You can use RT communication for both IO systems at the same time.
- You can use IRT communication in one of the two IO systems. Use IRT either in a higher-level or in a lower-level IO system. The following restrictions apply to RT communication:
  - If you use IRT communication in the lower-level IO system, you can use RT communication in the higher-level IO system.
  - If you use IRT communication in the higher-level IO system, you can only use RT communication for isochronous I-devices in the lower-level IO system.
- If the PROFINET interface configured as an I-device uses RT communication, you can use IRT communication for a connected PROFINET IO system.

7.2.10 Configuring PROFIenergy with I-devices

The requirement for program-controlled pauses for saving energy with PROFINET devices is that the PROFINET devices support the PROFIenergy protocol.

Only if a PROFINET device (I/O device) supports the PROFIenergy protocol does an I/O controller actually send PE commands to this I/O device, for example to start or stop pauses.

If an I/O device supports the PROFIenergy protocol, this property is saved in its PROFINET GSD file and is available for configuration in an engineering system.

For S7-1500 CPUs as intelligent I/O devices (I-devices), you have the option with STEP 7 V13 service pack 1 or later to set PROFIenergy support for each transfer area.

If you have selected the "Enable PROFIenergy communication" option for a transfer area and import the generated PROFINET GSD file into another project, you can handle an I-device as a PE entity there.

Requirements

- STEP 7 as of V13 service pack 1
- CPU supports PROFIenergy with I-devices, for example CPU 1215C DC/DC/DC as of firmware version 4.2
- You use the PROFINET IO interface as an I-device and have created transfer areas.
- The user program in the I-device handles PROFIenergy commands

  Background: You need to program PROFIenergy functions with I-devices in the user program using the "PE_I_DEV" instruction and corresponding auxiliary blocks; this is different compared with IO devices for which this functionality is made available by the firmware. You may therefore only activate the PROFIenergy support for transfer areas if the user program in the I-device is configured correspondingly as well.

Enabling PROFIenergy for transfer areas of I-devices

Proceed as follows to assign parameters for the support of PROFIenergy:

1. Select the PROFINET interface (X1) of the CPU.
2. Select the required transfer area in the area navigation, for example: Operating mode > I-device communication > Transfer_area_1.
3. Select the check box "Enable PROFIenergy communication".

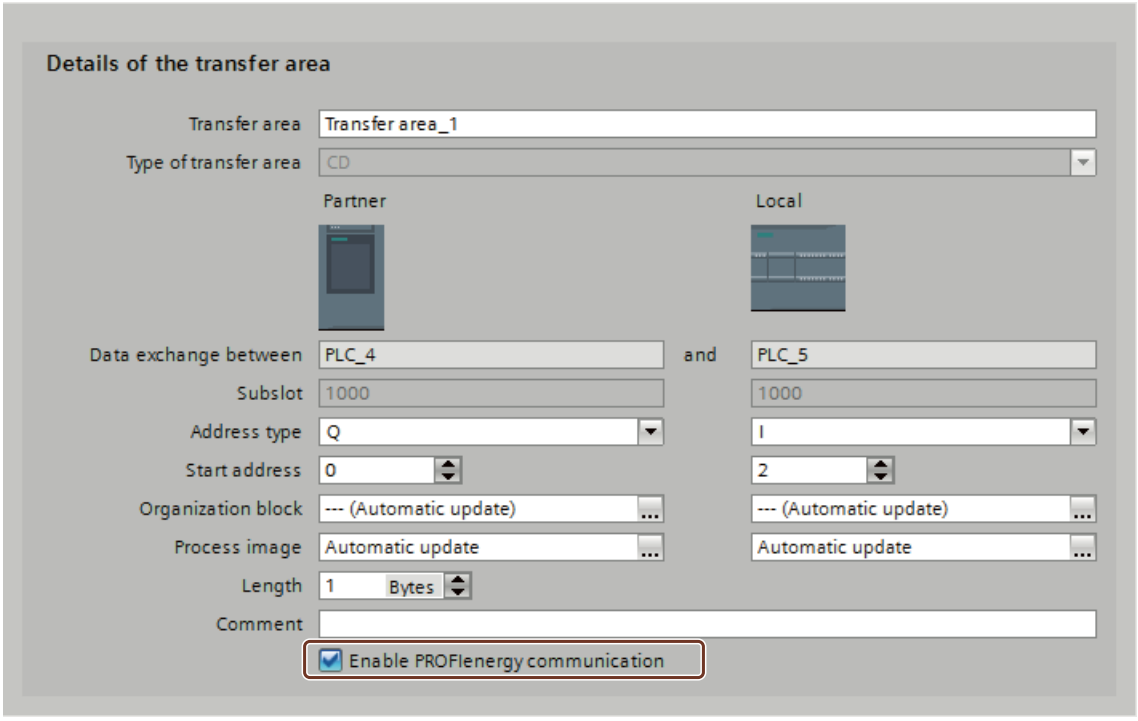


Figure 3-362 Configuring PROFIenergy with I-devices

Once the I-device is fully configured, generate the GSD file for the I-device and import this file in the project for the I/O controller. The GSD file generated contains an entry that specifies that the I-device supports the PROFIenergy profile.

To address the I-device, for example for the PE command "PE_START_END", use the hardware identifier of the "PROFIenergy supporting" transfer area in the I-device.

To address the IO controller for the PE command "PE_I_DEV", use the hardware identifier of the transfer area that is supplied with the data for PROFIenergy on the IO controller.

You can find more information on PROFIenergy in the sectoin Saving energy with PROFIenergy (Page 288).

7.2.11 Enabling/disabling I-device in the user program of the I-device CPU

When a PROFINET interface of a CPU was configured as an I-device in STEP 7, the I-device function is active after a status transition of the CPU from STOP > RUN. If no higher-level IO controller can be reached in this case, the I-device CPU signals an error using its ERROR LED.

As of firmware version 2.9 of an S7-1500/ET 200SP/ET 200pro CPU, you can locally disable or enable the I-device function in the user program of the I-device CPU. You use the "D_ACT_DP" instruction for this. After disabling the function, the I-device CPU no longer signals an error using its ERROR LED.

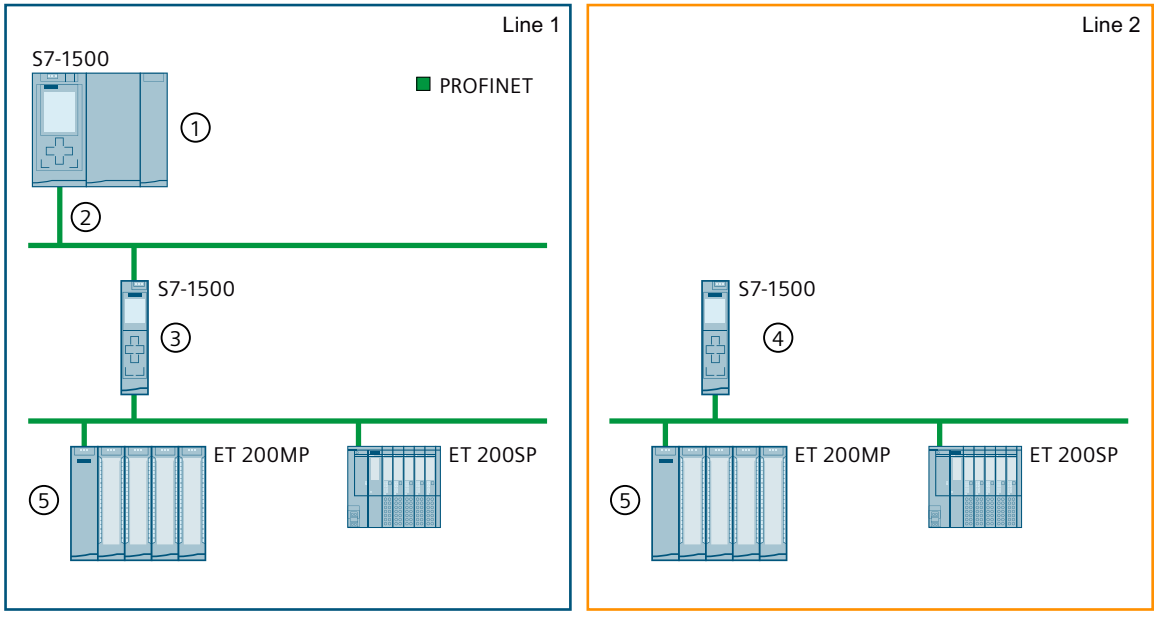
You can enable/disable the function with the user program at the CPU-internal PROFINET interfaces and for S7-1500 CM 1542-1 as of firmware version V3.0.

Application examples

From a machine OEM's point of view, there are numerous device options possible in **series production of machines**. However, each delivered machine includes only one combination of selected options. All possible machine options can be configured as I-devices by the manufacturer to create and maintain a common user program having all possible options.

A higher-level IO controller used for line control, for example, is not necessary in every machine. In this case, the user program can disable the I-device function in the I-device CPU with the instruction "D_ACT_DP", for example, during startup.

Two production lines are shown schematically in the figure below. The same user program runs in both CPUs with I-device configuration. The I-device in line 1 is controlled by a higher-level IO controller.



① Higher-level IO controller
② ... controls I-device CPU S7-1500 in the line
③ I-device function is enabled in the user program of this CPU
④ I-device function is disabled in the user program of this CPU
⑤ IO devices

Figure 3-363 Enable/disable the I-device function in the I-device CPU

Automation task control of vehicles in a ride

In a ride (ghost train), the vehicles are connected as I-devices to a higher-level controller via PROFINET.

Feature
The higher-level IO controller takes over the entire coordination and monitoring of the vehicles in the station. Among other things, the higher-level IO controller registers the following states:

- When the vehicles are available in the station
- When the vehicles exit the station

As soon as passengers are seated in the vehicle and the vehicle is closed, the higher-level IO controller issues the start signal.

Along the entire track, the vehicles are traveling independently and do not have a connection to the higher-level IO controller. Because this state does not represent an error, no errors should be signaled via the ERROR LEDs of the CPUs.

Solution
Depending on the position of the vehicle, inside or outside the station, the user program enables or disables the I-device function in the I-device CPU of the vehicle. No diagnostics were signaled via LED on the I-device CPU for enabling and disabling.

Requirements

You operate the CPU as an I-device on one or multiple IO controllers or you have configured the CPU as I-device ("IO device" check box is selected). In the following figure, the right CPU 1518-4 PN/DP is the I-device at the higher-level IO controller CPU 1518-4 PN/DP (PLC_2).

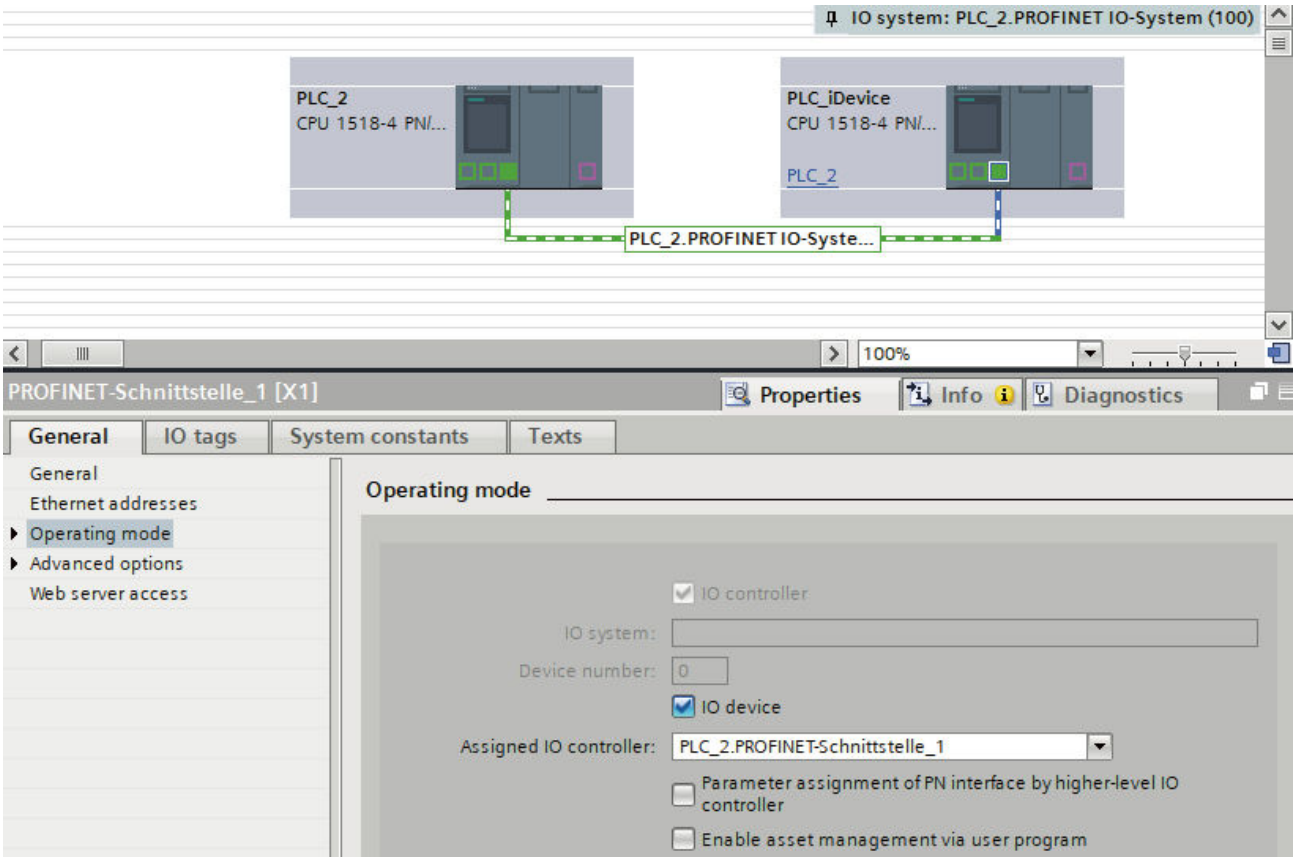


Figure 3-364 Example: Enable I-device

"D_ACT_DP" is an asynchronous instruction. Processing extends over multiple calls. You have started the job by calling "D_ACT_DP" with REQ = 1 in the startup OB of the I-device CPU.

You can find additional information on the "D_ACT_DP" instruction in the STEP 7 online help.

Disabling the I-device function at a PROFINET interface

NOTE

Only disable the I-device function in the I-device CPU when the I-device is not operated on a higher-level IO controller.

You disable the I-device function with the instruction "D_ACT_DP":

- Via the symbolic name or the hardware identification of the I-device of the respective PROFINET interface as LADDR parameter, in the example, HW identification 260
- Via the MODE parameter = 2

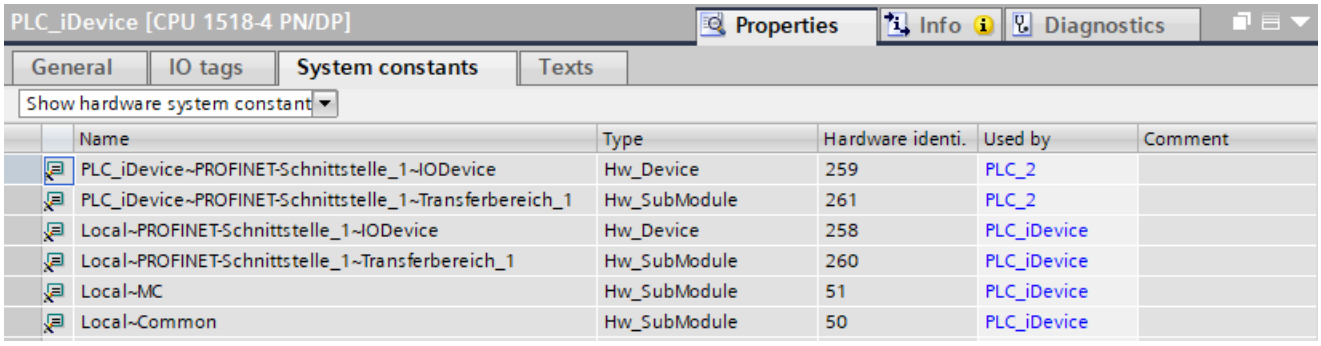


Figure 3-365 Example: I-device system constants

Result: The goal has been accomplished: The CPU with disabled I-device function is no longer available for the data exchange with a higher-level IO controller. The higher-level IO controller can be reached again when the I-device function was enabled in the user program of the I-device CPU.

When an I-device that has been active on an IO controller disables itself, all application relations (ARs) that were set up between the I-device and the IO controller in the network are terminated. An IO device failure is signaled at the IO controller end. In the diagnostic buffer of the I-device CPU, "IO device user disable" is displayed with information on the associated PROFINET interface or the name of the IO controller.

Enabling the I-device function at a PROFINET interface

You use the instruction "D_ACT_DP" to enable an inactive I-device function:

- Via the symbolic name or the hardware identification of the I-device of the respective PROFINET interface as LADDR parameter, in the example, HW identification 260
- Via the MODE parameter = 1

Result: After enabling, the I-device can exchange data with a higher-level IO controller.

If at least one IO controller is missing or the connection does not exist, "Hardware component removed or missing" is entered in the diagnostic buffer of the I-device CPU.

NOTE

Temporary access errors

Enabling the I-device function in the user program can result in temporary access errors "I/O data failure in hardware component", for example, because access to the I/O data of the I-device is already possible even though the data has not been declared as valid by the IO controller yet.

These messages are incoming and outgoing error events that can be neglected.

The behavior of IO controller and I-device in case of a station failure and station return still applies as described in the section Diagnostics and alarm response (Page 135).

Calling up the status information of an I-device with the instruction "D_ACT_DP"

You are requesting the status information of an I-device:

- Via the hardware identification of the I-device of the respective PROFINET interface as LADDR parameter, in the example, HW identification 260
- Via the MODE parameter = 0

The status is returned in the RET_VAL parameter:

- RET_VAL = 0x0000: "D_ACT_DP" was completed without errors (disabling an inactive I-device/enabling an active I-device)
- RET_VAL = 0x0001: I-device is enabled
- RET_VAL = 0x0002: I-device is disabled

7.3 Shared device

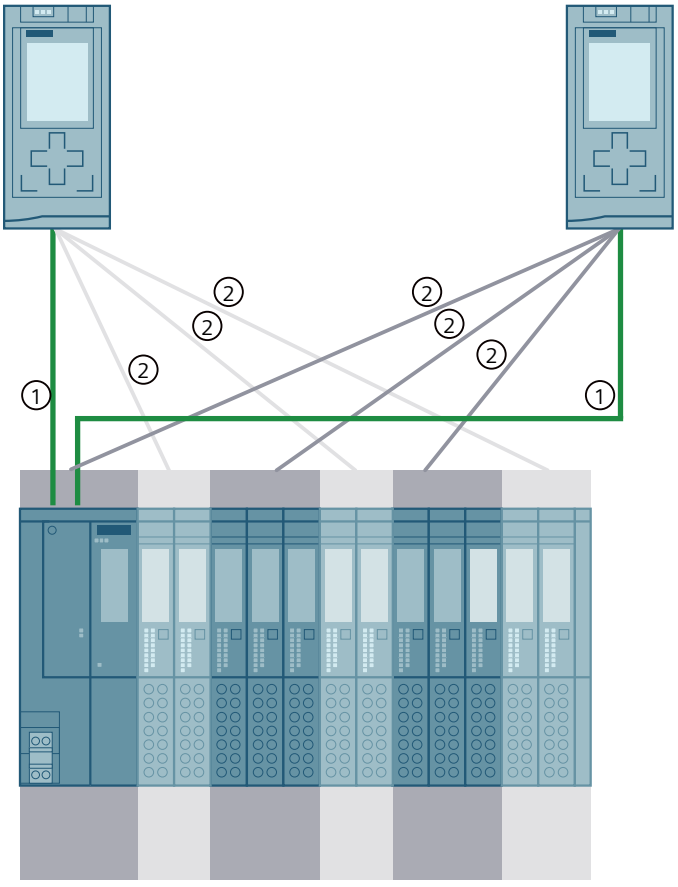
7.3.1 Useful information on shared devices

Shared device functionality

Numerous IO controllers are often used in larger or widely distributed systems.

Without the "shared device" function, each IO module of an IO device is assigned to the same IO controller. If sensors that are physically close to each other must provide data to different IO controllers, several IO devices are required.

The "Shared Device" function allows the modules or submodules of an IO device to be divided up among different IO controllers. Thus allowing flexible automation concepts. You can, for example, combine IO modules that are physically close to one other in one IO device. Drives such as SINAMICS S120 also support the shared device functionality. As of STEP 7 V20, S7-1500 Software Controllers FW version V40 and higher also support the shared I-device functionality.



① PROFINET
② Logical assignment

Figure 3-366 Example: Shared device with two IO controllers

Principle

Access to modules and submodules of the shared device is then divided up among the individual IO controllers. Each module or submodule of the shared device is assigned exclusively to one IO controller.

Configuration possibilities of shared devices

You can configure a shared device and the IO controllers that access it in one of the following ways:

- In a common project
- Distributed among several projects

It is preferable to configure a shared device in a common project together with the IO controllers that access it. As a result, all components of a shared device configuration are known to the project. Therefore, configuration in a common project offers the following advantages compared to configuration in multiple projects:

- Reduction of possible sources of error: STEP 7 checks the complete consistency within a project.
- Less configuration effort: A common STEP 7 project contains all devices.
- Improved diagnostics: Complete diagnostics in one project.

Using a shared device and its IO controllers in a common project:

- Since STEP 7 V18: You can configure a shared device and two CPUs accessing it (IO controllers) in a single project.
- From STEP 7 V19: You can also configure a shared I-device and two CPUs accessing it (IO controllers) in a single project.
  - Requirement: Use an S7-1500 CPU FW version V3.1 or higher as the shared I-device.
- From STEP 7 V20: You can configure a shared device/shared I-device and all IO controllers that access it in a single project. You can also use a CM 1542-1 communications module with FW version V4.1 or higher as an IO controller.

If you use a shared device in multiple projects, the shared device must be configured in each project containing IO controllers that access it.

Using a shared device in multiple projects:

- Since STEP 7 V12 SP1, S7-1500 CPUs and SIMATIC distributed I/O devices support the "Shared Device" function. The shared device must be present in every project, although it is present only once in the installation. A separate project is required for each CPU accessing the shared device. To find out which components support the "Shared Device" function, see the following FAQ (https://support.industry.siemens.com/cs/us/en/view/102325771).

Setting of the real-time properties

If in addition to the CPUs in the project, other CPUs outside the project have access to the shared device, you must enter the number of project-external IO controllers for the PROFINET interface of the shared device. Only then does STEP 7 correctly calculate the communication load and thus the resulting update times.

The maximum possible number of IO controllers for the shared device depends on the device. You can find this number as follows:

- In the GSD file of the shared device.
- In the equipment manuals of the IO devices or CPUs that you intend to use as the shared device.

With a CPU used as an IO controller, you can set a very fast send clock. The send clock can be shorter than the shortest send clock supported by the shared device. In this case, the IO controller operates the shared device with a send clock it supports (send clock adaptation).

Example:

A CPU supports send clocks starting from 0.25 ms. One configured IO device also supports send clocks starting from 0.25 ms, while another IO device supports send clocks starting from 1 ms. In this case, you have the option of setting the short send clock of 0.25 ms for the CPU. The CPU operates the "slow" IO device with the send clock of 1 ms, for example.

Response in the event of fault

You can find out how PROFINET IO controllers behave in the event of an error when accessing the data of a shared device in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/109572804).

7.3.2 Shared device and assigned IO controllers in the common project

Requirements

- The shared device and the IO controllers accessing it must be in the same subnet.
- The shared device must be assigned to each IO controller.
- There must be at least one module or submodule assigned to each connected IO controller.

If these conditions are not met, the configuration as a shared device is inconsistent. When an inconsistent configuration is compiled in STEP 7, a corresponding error message is displayed.

Restrictions

- In STEP 7 V18, only IO devices that have been installed in the hardware catalog via GSD files are permitted as shared devices in the common project.
  Starting from STEP 7 V19, you can insert and configure IO devices as shared devices in the common project directly from the STEP 7 hardware catalog without prior installation of GSD. You can find an overview of which IO devices support this usage in the following FAQ (https://support.industry.siemens.com/cs/us/en/view/102325771).

- In STEP 7 V19, a maximum of two IO controllers (CPUs) may access a shared device within a project. As of STEP 7 V20, this restriction no longer applies.
- The shared device does not support system redundancy.
- You can find specifics on handling fail-safe IO devices in the SIMATIC Safety - Configuring and Programming V19 (https://support.industry.siemens.com/cs/us/en/view/54110126) Programming and Operating Manual.
- "TIA Portal Openness" does not support shared device.
- Loading both CPUs as a new station into the same project is not supported. Load the two CPUs that share the shared device into different projects. As of STEP 7 V20, this restriction no longer applies.

Access to modules and submodules

Each IO controller only has access to the modules and submodules assigned to it. This means:

- Data is exchanged only with the assigned modules or submodules
- Alarms and diagnostics are only received from assigned modules or submodules
- Only parameters of assigned modules or submodules are configured

Rules for the configuration

The following rules apply to the configuration of a shared device in a common project and are checked automatically by STEP 7 when the configuration is compiled:

- Only one IO controller at a time may have full access to one submodule.
- I/O addresses of a module or submodule can only be edited in the address area of the IO controller to which the shared device is assigned.
- The send clock must be identical for all IO controllers that have access to the shared device.
- The following functions are only possible with the IO controller to which the interface module of the shared device is assigned:
  - Isochronous mode (IRT)
  - Media redundancy
  - Prioritized startup
  - Parameter assignment of the port properties
- STEP 7 V20 does not support the "Use name as extension for device name" option for shared devices.
- If you change the name of the shared device, then you must subsequently load all the CPUs that share this IO device.
- The maximum total of the communication relationships (ARs) for the shared device must not be exceeded. The maximum total of the communication relationships may be found, for example, in the Equipment Manual of the IO device you wish to use as the shared device.

  Example:
  An ET 200SP interface module supports up to four communication relations as a shared device. The shared device has already been assigned to two IO controllers in the project. A maximum of two more IO controllers that have been configured in other projects may

access modules or submodules of this shared device. As of STEP 7 V20, you can configure the shared device and all IO controllers that access it in a single project.

7.3.3 Configuring a shared device in a common project

Below, you will find a description of how to configure a distributed I/O system as a shared device with STEP 7 version V18 or higher.

If your project contains a shared device that is accessed by IO controllers outside the project, read section "Configuring a shared device for different projects (Page 158)". These IO controllers are configured either in another TIA Portal project or with a different engineering tool.

A "distributed" configuration with different engineering tools for different IO controller families is generally possible. However, the description of the procedure is based exclusively on STEP 7 V18 or higher.

Since STEP 7 V18, only one project is needed for a shared device configuration. The project contains the shared device and a maximum of two IO controllers that access it. As of STEP 7 V20, you can configure a shared device and all IO controllers accessing it in a common project.

The following description is limited to two IO controllers of the S7-1500 family that share a shared device in a common project.

Requirements

- STEP 7 (TIA Portal) V18 or higher
- The IO controllers support the shared device function, e.g. CPU 1513-1 PN FW version V3.0 or higher.
- The IO device supports the shared device function, e.g. IM 155-5 PN ST interface module.
- STEP 7 V18: GSD files for the IO devices are installed and being used.
- STEP 7 as of V19: You can use IO devices from the hardware catalog of STEP 7 without prior installation of their GSD files. The desired IO device must support the shared device function when directly used from the hardware catalog.

Procedure - Creating project

To create a common project with two IO controllers and a shared device, follow these steps:

1. Start STEP 7.
2. Create a new project, for example with the name "Shared Device".
3. In the network view, insert an IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
4. Assign a name, for example "PLC_1".
5. Insert another IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
6. Assign a name, for example "PLC_2".
7. Connect the PROFINET interface X1 of the inserted IO controllers to each other. The PROFINET interfaces of the IO controllers are then in the same subnet.

8. Insert an IO device (e.g. IM 155-6 PN ST) from the hardware catalog as follows:
   - STEP 7 V19 or higher: Use the default entries, for example, under "Distributed I/O > ET 200SP > interface module > PROFINET".
   - STEP 7 V18: You can find the IO devices installed from the GSD files under "Other field devices > PROFINET IO > IO > SIEMENS AG".
9. Double-click the inserted IO device. The device view opens.
10. Insert all required modules and submodules from the hardware catalog into the device overview table. If the shared device was installed and inserted as GSD, also use the installed modules and submodules from the GSD files.
11. Assign parameters for the individual IO modules.
12. Switch to the network view.
13. Assign the IO device to the IO controllers one after the other, e.g. "PLC_1" and "PLC_2".
14. Save the project.

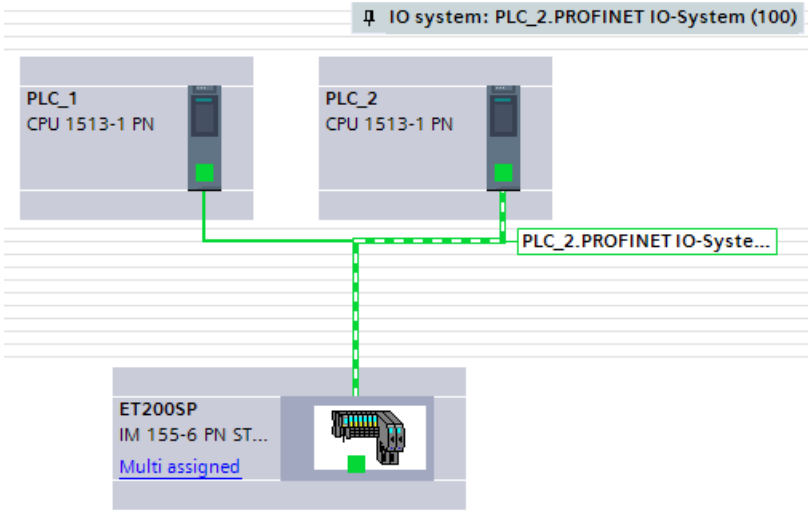


Figure 3-367 Shared device assigned in the common project

Procedure - Configuring the assignment of the modules or submodules

After the first assignment of the shared device to an IO controller, all modules or submodules are assigned to this IO controller.

Newly added modules or submodules are assigned to the IO controller to which the interface module is also assigned. If a shared device is disconnected from an IO controller, the assigned modules or submodules obtain the "unknown" access status.

To change the assignment, proceed as follows:

1. In the network view or the device view of the project, select the interface module of the shared device.
2. In the Inspector window, select the "Shared Device" tab under "Properties > General > Module parameters".

   A table shows which IO controller has access to the respective module or submodule. The default setting for all modules and submodules is the IO controller to which the shared device was first assigned.
3. Keep the "PLC_1" setting for all modules and submodules that are to remain in the address area.

   For all modules or submodules that you want to assign to the address area of the other IO controller, select the setting "PLC_2".

   Special consideration: With the "Outside of project" option, you can select IO controllers that are connected to the PROFINET IO system but are configured in another TIA project or engineering tool.

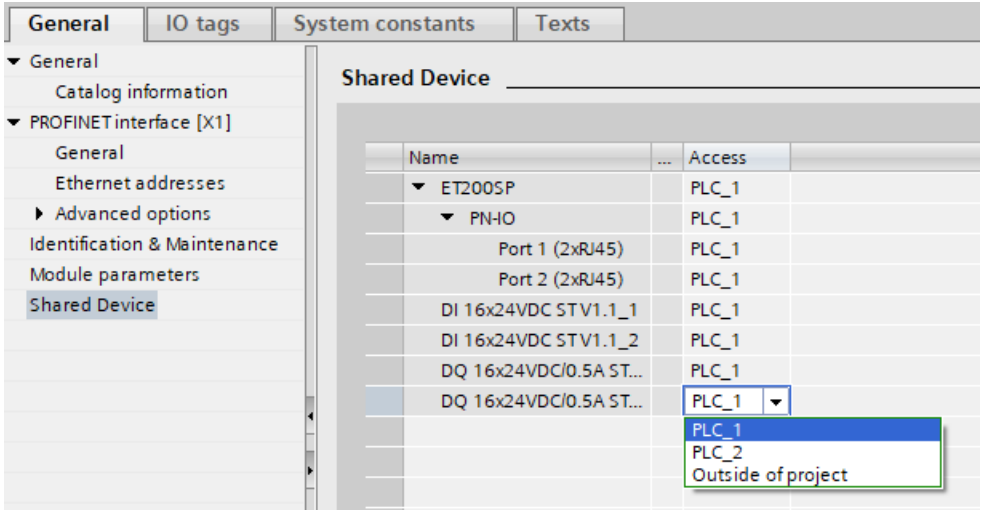


Figure 3-368 Configuring a project-internal shared device

Procedure - Adjusting the real-time settings

Adjusting and checking the settings listed below ensures the following properties:

- All IO controllers and shared devices are operated with the appropriate send clock.
- Update times are calculated correctly with respect to the communication load.

To adjust and check these settings, proceed as follows:

1. Select the interface module of the shared device in the network view.
2. In the Inspector window, navigate to the "PROFINET interface > Advanced options > Real time settings > IO cycle" area.
3. If IO controllers from other projects also access this shared device: Set the number of IO controllers outside the project in the "Shared Device" area. The maximum number depends on the IO device. You can find the maximum number as follows:
   - In the GSD file of the shared device.
   - In the Equipment Manual of the IO device you wish to use as the shared device.

4. For each IO controller that has access to modules or submodules of the shared device, you must adapt the real-time settings on a CPU-specific basis.
5. You must set the same send clock for each IO controller that has access to modules or submodules of the shared device:
   – If you configure an additional IO controller outside the project with STEP 7 (TIA Portal):
     Open the corresponding project.
     Select the PROFINET interface of the IO controller.
     Select the "Advanced options > Real time settings > IO communication" area in the Inspector window and set the same send clock.
   – If you configure an additional IO controller outside the project with a different engineering tool:
     Select the PROFINET interface of the shared device in STEP 7 (TIA Portal) and read out the send clock on the shared device ("Advanced options > Real time settings" area)
     Enter the read send clock in the engineering tool.
   – Special consideration: If you configure **all** IO controllers that have access to the shared device in a common STEP 7 project (STEP 7 V5.5 or higher), shorter send clocks can be set at the IO controller than are supported by the shared device (send clock adaptation).

Compiling and loading

When you select the shared device and click on "Compile" in the toolbar, the configuration of all IO controllers accessing it is checked for data consistency.

You must load the configurations for the various IO controllers into the IO controllers one after the other.

NOTE

Synchronizing router settings with the IO controller

The "Synchronize router settings with IO controller" option is selected by default for IO devices. If the connected IO controllers use the same router or no router, leave this setting as it is.

If the connected IO controllers use different routers, deselect the "Synchronize router settings with IO controller" option. In this case, manually configure the corresponding router address on the shared device.

7.3.4 Shared device and assigned IO controllers in different projects

Requirements

- STEP 7 V12 Service Pack 1 or higher.
- IO device supports the shared device function, e.g. IM 155-5 PN ST interface module.
- IO controller supports the shared device function, e.g. CPU 1516-3 PN/DP FW version V1.1 or higher or CPU 1215 DC/DC/DC FW version V4.1 or higher.

Configuring the access

The modules and submodules of an IO device must be assigned to the different IO controllers in the various projects. This requires the IO device to be present in all projects in which an IO controller accesses this IO device.

Use the "Shared Device" parameter of the interface module to define the modules or submodules to which the IO controller has access:

- If the local IO controller has access to the configured module, select the name of the IO controller from the list.
- If an IO controller from another project is to have access to the configured module, select the entry "Outside of project".

The configuration is consistent with regard to access when each module or submodule has been assigned to an IO controller in exactly one project.

Module or submodule is assigned to another IO controller

The following section is about the consequences of the "Outside of project" setting of the "Shared Device" parameter from the point of view of the local IO controller.

In this case, the local IO controller does not have access to the module configured in this way. Specifically, this means:

- No parameter assignment of the module or submodule
- No data exchange with the module or submodule
- No reception of alarms or diagnostics, which means no display of the diagnostics status in the online view

Rules for the configuration

- IO controllers that use the shared device are created in different projects. In each project, care must be taken that the shared device is configured identically in each station.
- If you have selected the "Use router" option for the IO controllers involved, you must have set the same router address in all these IO controllers. You as the user must ensure consistency.
- The shared device must have the same IP parameters and the same device name in each project.
- The S7 subnet ID of the subnet to which the shared device is connected must be identical in all projects.
- Only one IO controller at a time may have full access to one submodule. Inconsistencies in the configuration result in a failure of the shared device.
- I/O addresses of a module or submodule can only be edited if a module or submodule has been assigned to the IO controller in the same project.
- The send clock must be identical for all IO controllers that have access to the shared device.

- The following functions are only possible with the IO controller to which the interface module of the shared device is assigned:
  - Isochronous mode (IRT)
  - Media redundancy
  - Prioritized startup
  - Parameter assignment of the port properties
- If you change the name of the shared device, then you must subsequently load all the CPUs that share this IO device.
- The maximum total of the communication relationships (ARs) for the shared device must not be exceeded. The maximum total of the communication relationships may be found, for example, in the Equipment Manual of the IO device you wish to use as the shared device.

  Example:
  An ET 200SP interface module supports up to four communication relations as a shared device. The shared device has already been assigned to two IO controllers in the project. A maximum of two more IO controllers that have been configured in other projects may access modules or submodules of this shared device.

Constraints

The following constraints result because a shared device configuration is distributed across different projects:

- In the address overview of each IO controller that has access to a shared device, the addresses of modules or submodules that are not assigned to this IO controller are missing.
- The modules or submodules that are not assigned are not taken into consideration in the configuration limit calculation for the shared device during the consistency check. For this reason, you must yourself check that the maximum number of submodules or the maximum amount of cyclic IO data for the shared device is not exceeded.
  For information on the maximum configuration limits, refer to the documentation of the devices you are using.
- Configuration errors such as assignment of a module or submodule to more than one IO controller are not detected by STEP 7.
- CPUs that are loaded with a shared device configuration do not have any information on whether the IO device is a shared device. Modules or submodules that have been assigned to other IO controllers, and therefore other CPUs, are missing in the loaded configuration. These modules or submodules are therefore displayed neither in the CPU web server nor in the CPU display.

See also

Response in the event of fault
(https://support.industry.siemens.com/cs/ww/en/view/109572804)

7.3.5 Configuring a shared device for different projects

Below, you will find a description of how to configure a distributed I/O system as a shared device with STEP 7 version V12, Service Pack 1 or higher.

A "distributed" configuration with different engineering tools for different IO controller families is in principle possible. However, this description of the procedure is based exclusively on STEP 7 V12, Service Pack 1 or higher. The following description is limited to two IO controllers of the S7-1500 family that share a shared device in different projects.

Two projects are created (Shared-Device-1 and Shared-Device-2), each with one IO controller (PLC_1 and PLC_2). You must create the shared device in both projects, even though it is physically one and the same IO device.

Requirements

- STEP 7 (TIA Portal) as of V12 Service Pack 1
- The IO controllers support the shared device function, e.g. CPU 1513-1 PN, FW version V1.1 or higher.
- The IO device supports the shared device function, e.g. IM 155-5 PN ST interface module, FW version V2.0 or higher.

Procedure - Creating project 1

To create the first project with a shared device, follow these steps:

1. Start STEP 7.
2. Create a new project, for example with the name "Shared-Device-1".
3. In the network view, insert an IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
4. Assign a name, for example "PLC_1".
5. Insert an IO device (e.g. IM 155-6 PN ST) with the "Shared device" function from the hardware catalog.
6. Assign the IO device to the IO controller "PLC_1".
7. Double-click the IO device and insert all required modules and submodules from the hardware catalog into the device overview table.
8. Assign the module parameters.
9. Save the project.

Procedure - Creating project 2

To create the second project with a shared device, follow these steps:

1. Start STEP 7 once again.
   A new instance of STEP 7 opens.
2. In the new instance, create a new project, for example with the name "Shared-Device-2".
3. In the network view, insert an IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
4. Assign a name, for example "PLC_2".

5. Copy the IO device from the "Shared-Device-1" project and insert it into the network view of the "Shared-Device-2" project.
6. Assign the IO device to the IO controller "PLC_2".
7. Save the project.

Both projects now have an identically structured IO device that must be configured in the next step for the different IO controller accesses.

Procedure - Configuring the assignment of the modules or submodules

The modules and submodules you insert in the shared device are automatically assigned to the local CPU. To change the assignment, follow these steps:

1. Select the interface module in the network view or device view of the "Shared-Device-1" project.
2. In the Inspector window, select the "Shared Device" tab under "Properties > General > Module parameters".

   A table shows which CPU has access to the respective module or submodule for all configured modules. The default setting is that the local CPU has access to all modules and submodules.
3. Keep the "PLC_1" setting for all modules and submodules that are to remain in the address area of the local CPU.

   Select the "Outside of project" setting for all modules or submodules that are to be located in the address area of the CPU from the "Shared-Device-2" project ("PLC_2"). This means that an IO controller outside of the project is to have access to the module or submodule.

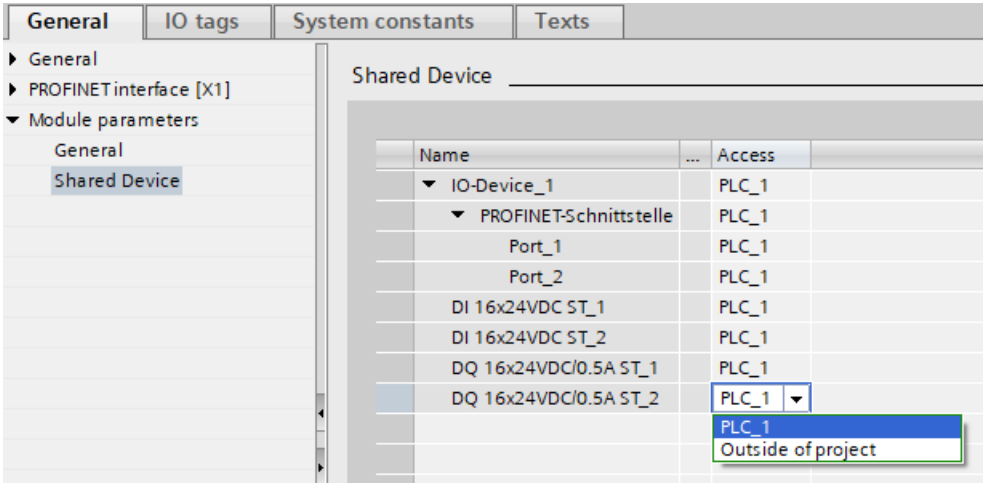


Figure 3-369 Configuring shared device

4. Select the interface module in the network view or device view of the "Shared-Device-2" project.
5. In the Inspector window, select the "Shared Device" tab under "Properties > General > Module parameters".

   A table shows which CPU has access to the respective module or submodule for all configured modules.
6. Select the "Outside of project" setting for all modules or submodules that are to be located in the address area of the CPU from the "Shared-Device-1" project ("PLC_1").

7. Finally, check whether the settings for access are "complementary" for each module or submodule in both projects. This means that if the local CPU has access in one project, the "Outside of project" option must be set in the other project and vice versa.

   Special consideration: The option "Outside of project" for the PROFINET interface and therefore for the ports makes the associated parameters read-only and not changeable. Parameters of the PROFINET interface and port parameters can only be edited in the project in which the PROFINET interface is assigned to the local CPU. The ports can be interconnected in both projects regardless of this.
8. Check whether the same IP address parameters and device name are set for the shared device in all projects.

   Check whether the same S7 subnet ID is set in all projects for the subnet to which the shared device is connected (subnet properties, "General" area in the Inspector window).

NOTE

If you make changes to the shared device: Make the same changes in each project on the shared device. Make sure that only one IO controller at a time has access to a module or submodule!

Procedure - Adjusting the real time settings

Adjusting and checking the settings listed below ensures the following properties:

- All IO controllers and shared devices are operated with the appropriate send clock.
- Update times are calculated correctly based on the communication load.

To adjust and check these settings, proceed as follows:

1. Select the project whose IO controllers have access to the PROFINET interface and the ports of the shared device.
2. Select the interface module of the shared device in the network view.
3. In the Inspector window, navigate to the "PROFINET interface > Advanced options > Real time settings > IO cycle" area.
4. In the "Shared Device" area, set the number of project-external IO controllers. The maximum number depends on the IO device (specification in GSD file).
5. For each IO controller that has access to modules or submodules of the project-internal shared device, you must adapt the real-time settings on a CPU-specific basis.

6. You must set the same send clock for each IO controller that has access to modules or submodules of the shared device:
   - If the IO controller is configured with STEP 7 (TIA Portal):
     Open the corresponding project.
     Select the PROFINET interface of the IO controller.
     Select the "Advanced options > Real time settings > IO communication" area in the Inspector window and set the same send clock.
   - If the IO controller is configured with a different engineering tool:
     Select the PROFINET interface of the shared device in STEP 7 (TIA Portal) and read out the send clock on the shared device ("Advanced options > Real time settings" area)
     Enter the read send clock in the engineering tool.
   - Special consideration: If **all** IO controllers that have access to the shared device are configured in STEP 7 (TIA Portal or STEP 7 V5.5 or higher), you can set shorter send clocks at the IO controller than are supported by the shared device (send clock adaptation).

Compiling and loading

You must compile the configurations for the different IO controllers and load them into the CPUs one after the other.

Due to the distributed configuration with separate projects, STEP 7 does not output consistency errors in the case of incorrect access parameter assignment. Example for incorrect access parameter assignment:

- Multiple IO controllers have access to the same module
- IP address parameters or send clocks are not identical

These errors do not show up until operation and are output as configuration errors, for example.

NOTE

After a configuration has been loaded in the IO controller, non-assigned modules or submodules retain their current parameterization state to ensure the independence from the parameterizations of other IO controllers.

See also

Module-internal shared input/shared output (MSI/MSO) (Page 175)

7.3.6 Shared I-device and assigned IO controllers in the common project

Requirements

- The I-device as shared device (shared I-device) and the IO controllers accessing it must be in the same subnet.
- The shared I-device must be assigned to each IO controller.

If these conditions are not met, the configuration as a shared I-device is inconsistent. When an inconsistent configuration is compiled in STEP 7, a corresponding error message is displayed.

Restrictions

- In STEP 7 V19, a maximum of two IO controllers (CPUs) may access a shared I-device within a project. As of STEP 7 V20, this restriction no longer applies.
- Devices of the SIMOTION product family do not support the shared I-device function.
- The shared I-device does not support system redundancy.
- "TIA Portal Openness" does not support shared I-device.
- The simultaneous loading of CPUs and shared I-device into a new project is not supported. Load each station individually into the new project. As of STEP 7 V20, this restriction no longer applies.

Access to modules and submodules

Each IO controller only has access to the modules and submodules of its IO devices that are assigned to it. This means:

- Data is exchanged only with the assigned modules or submodules
- Alarms and diagnostics are only received from assigned modules or submodules
- Only parameters of assigned modules or submodules are configured

Rules for the configuration

The following rules apply to the configuration of a shared I-device in a common project and are automatically checked by STEP 7 when the configuration is compiled:

- A maximum of two IO controllers share one shared I-device. As of STEP 7 V20, this restriction no longer applies.
- There must be at least one transfer area assigned to each connected IO controller.
- Only one IO controller at a time may have full access to one submodule.
- The send clock must be identical for all IO controllers that have access to the shared I-device.
- Isochronous mode (IRT) is only possible with the IO controller to which the interface module of the shared I-device is assigned.

- STEP 7 V20 does not support the "Use name as extension for device name" option for shared devices.
- If you change the name of the shared I-device, then you must subsequently load all the CPUs that share this shared I-device.

7.3.7 Configuring a shared I-device in the common project

Below, you will find a description of how to configure an S7-1500 CPU as a shared I-device with STEP 7 version V19 or higher.

If your project contains a shared I-device that is accessed by IO controllers outside the project, read section "Configuring a shared I-device in different projects (Page 167)". These IO controllers are configured either in another TIA Portal project or with a different engineering tool.

A "distributed" configuration with different engineering tools for different IO controller families is generally possible. However, the description of the procedure is based exclusively on STEP 7 from V19.

Since STEP 7 V19, only one project is needed for a configuration with a shared I-device. The project contains the shared I-device and a maximum of two IO controllers that access it. As of STEP 7 V20, you can configure a shared I-device and all IO controllers accessing it in a single project.

The following description is limited to two IO controllers of the S7-1500 family that share a shared I-device in a common project.

Requirements

- STEP 7 (TIA Portal) V19 or higher
- The IO controllers that access the shared I-device support the shared device function, e.g. CPU 1513-1 PN FW version V3.1 or higher.
- The IO controller that is used as a shared I-device supports the shared device function, e.g. CPU 1513-1 PN FW version V3.1 or higher.

Procedure - Creating project

To create a common project with two IO controllers and a shared I-device, follow these steps:

1. Start STEP 7.
2. Create a new project, for example with the name "Shared I-device".
3. In the network view, insert an IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
4. Assign a name, for example "PLC_1".
5. Insert another IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
6. Assign a name, for example "PLC_2".
7. Connect the PROFINET interface X1 of the inserted IO controllers to each other. The PROFINET interfaces of the IO controllers are then in the same subnet.
8. Insert another IO controller (e.g. CPU 1513-1 PN) from the hardware catalog.
9. Assign a name, for example "PLC_I-Device".

Procedure - Configuring I-device functionality

To configure I-device functionality for the PROFINET interface X1 of the IO controller "PLC_I-Device", follow these steps:

1. Select the PROFINET interface X1 of PLC_I-Device.
2. In the Inspector window, navigate to "Properties > General > Operating mode".
3. Enable the "IO device" option. The table below is editable.
4. Click on the entry "Assign to new IO controller" in the table.
5. Select the PROFINET interface of an IO controller from the drop-down list, for example, "PLC_1.PROFINET interface_1."
   The next free device number in the higher-level IO system will be assigned by default as the device number.
6. Repeat steps 4 and 5 for a further IO controller.
7. If required, activate the "Parameter assignment of PN interface by higher-level IO controller" option.
   The drop-down list below is activated. In this case, select a higher-level IO controller from the drop-down list, for example, PLC_1.

8. If necessary, enable additional options. The "Activate DCP write protection" option is enabled by default for all IO devices that support this function. If an I-device can additionally synchronize the default values from the IO controller, the "Synchronize DCP settings with default values from IO controller" option is shown and enabled by default.

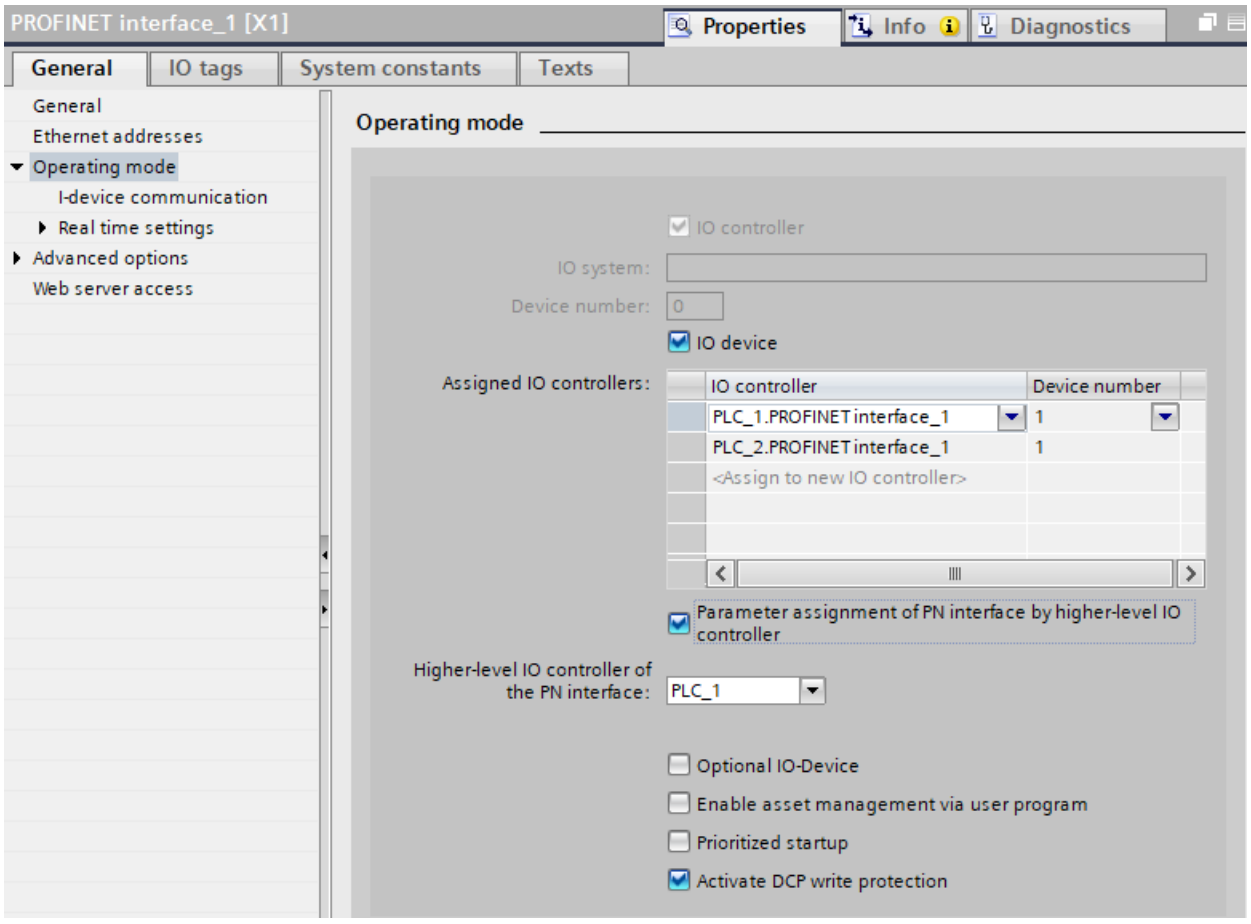


Figure 3-370 Configuring operating mode of I-device

Result: You have configured an S7-1500 CPU as an I-device and assigned it to two IO controllers.

Procedure - Creating and configuring transfer areas

Transfer areas that are assigned to IO controllers are defined as the I/O interface. At least one transfer area must be assigned to each IO controller accessing the shared I-device.
To configure a transfer area, follow these steps:

1. Select the PROFINET interface X1 of the IO controller PLC_I-device.
2. In the Inspector window, navigate to "Properties > General > Operating mode > I-device communication".
3. Double-click the table entry "Add new". A new transfer area is created.
4. Repeat steps 1 through 3 to create further transfer areas.

Intermediate result: You have created the required transfer areas. You can view the transfer areas with their basic settings in the Inspector window in the I-device communication area. To configure a transfer area, e.g. change an input area to an output area, follow these steps:

1. Select the desired transfer area, for example, Transfer area_1, in the Inspector window under "Properties > General > Operating mode > I-device communication".
   The selected transfer area is displayed in the Inspector window.
2. Select the desired type from the drop-down list "Address type" under "Partner" or "Local."
   The address type at the partner will be automatically adjusted in the event of changes.

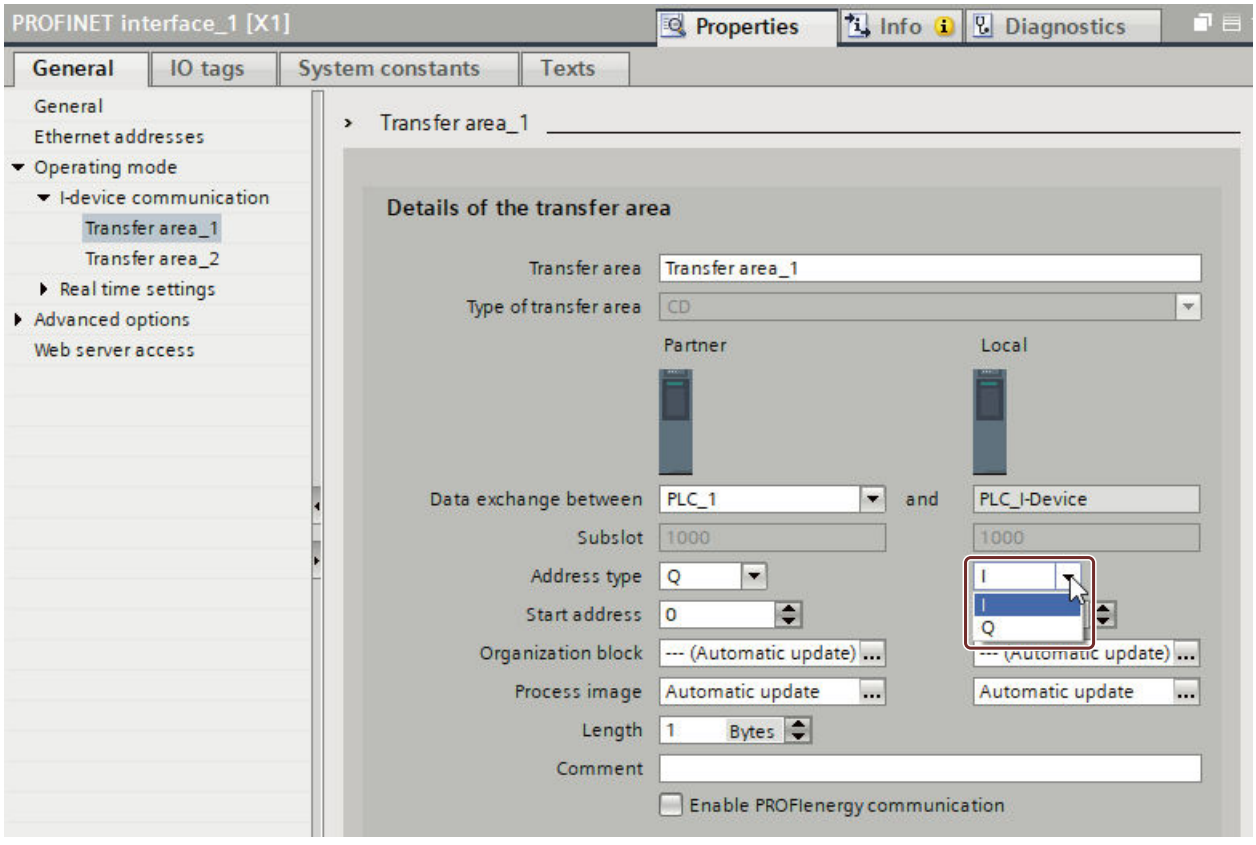


Figure 3-371 Configuring a transfer area of an I-device

Result: You have created and configured transfer areas of the I-device.

Procedure - Adapting the send clock in the real-time settings

You must set the same send clock for each IO controller that has access to modules or submodules of the shared I-device. This ensures that update times are calculated correctly with respect to the communication load.

To adjust and check these settings, proceed as follows:

1. At an assigned IO controller, select the PROFINET interface that is connected to the shared I-device.
2. In the Inspector window, navigate to the "General > Advanced options > Real-time settings > IO communication" area.
3. In the drop-down list, select a common send clock.
4. Repeat steps 1 to 3 for the other assigned IO controller.

In the common STEP 7 project, all the IO controllers that have access to the shared I-device are configured. In this case, it is possible to also set shorter send clocks on the IO controllers than supported by the shared I-device (send clock adaptation).

Compiling and loading

When you select an IO controller and click on "Compile" in the toolbar, the configuration of this IO controller and the shared I-device is checked for data consistency.
Alternatively, mark both IO controllers that access the shared I-device. When you click on "Compile" in the toolbar, the full configuration (both IO controllers and the shared I-device) is checked for data consistency.

You must compile the configurations for the different IO controllers and shared I-device and load them into the CPUs one after the other.

7.3.8 Configuring a shared I-device in different projects

Below, you can find a description of how you configure an S7-1500 as an I-device with STEP 7 Version 13 or higher and then use it in 2 projects as a shared device.

A "distributed" configuration with different engineering tools for different IO controller families is generally also possible here. The procedure described below is based on STEP 7 V13 and is limited to a configuration with 2 IO controllers of the S7-1500 family that share the transfer areas of an I-device as a shared device. The I-device itself is also an S7-1500 CPU.

Create 3 projects with one IO controller each (PLC-I-Device, PLC_1 and PLC_2).

The "PLC-I-Device" project is used to configure the I-device. The PROFINET GSD variant of "PLC-I-Device" is used in the "PLC_1" and "PLC_2" projects in order to assign the transfer areas in the respective higher-level IO controller.

Shared I-device concept

To introduce the shared I-device concept, 2 roles are introduced here:

- The role of manufacturer (e.g., machine manufacturer): The manufacturer configures and programs an I-device that performs a particular automation task. Transfer areas are defined as the I/O interface to the operator of the machine. These transfer areas can be assigned to different IO controllers. For the connection to higher-level IO controllers, the manufacturer provides a PROFINET GSD file and discloses the transfer areas via which the I-device can be accessed.

- The role of the operator: The operator uses the I-device as a PROFINET GSD variant during configuration of the PROFINET IO system and, in this process, specifies the I/O addresses under which the IO controllers access the transfer areas.

Manufacturer view

You assign the following parameters for an S7-1500 CPU as an I-device, with centralized and distributed I/O, the desired transfer areas, and the number of IO controllers having access to this I-device (always greater than 1 for a shared device!).

Special consideration: The I-device is configured without a higher-level IO controller. As a result, only the local I/O addresses of the transfer area are available (= "Address in the I-device") in order to create the user program for editing the addresses from the transfer area. The I-device that has been completely configured except for the connection to the higher-level IO controller is loaded to the S7-1500 CPU.

You export a PROFINET GSD file from the I-device configuration.

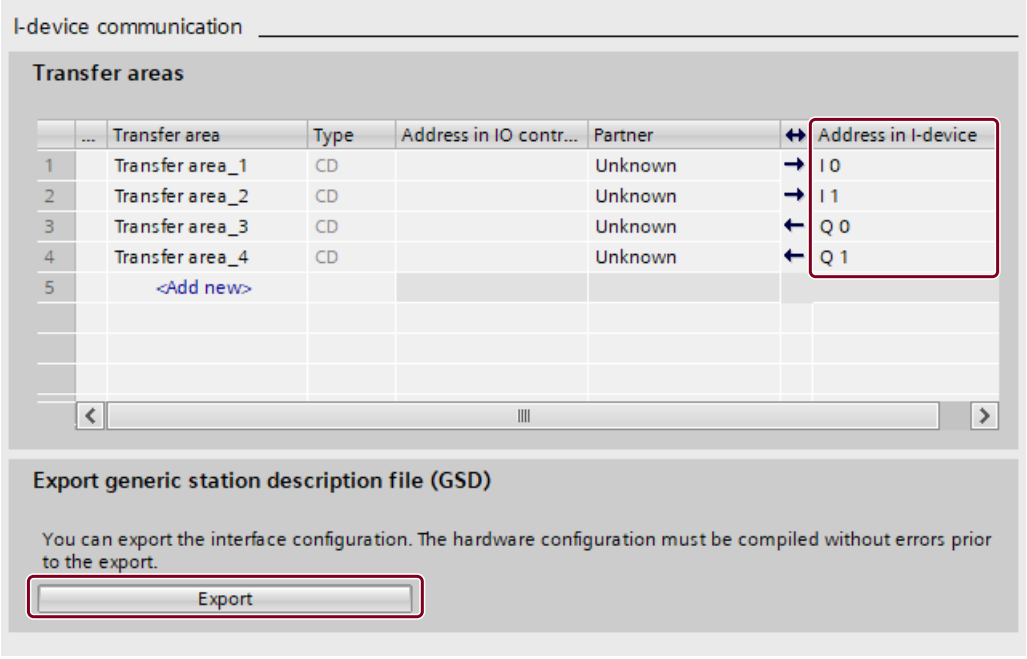


Figure 3-372 Exporting an I-device as a GSD file

Operator view

You must install the PROFINET GSD file created from the I-device configuration in all engineering systems that are involved in configuring a PROFINET IO system with this shared I-device. If all uses of this I-device will be configured with STEP 7 V13, it is sufficient to install the GSD file in STEP 7.

You configure the I-device as a GSD variant on the PROFINET IO system in the projects involved. In STEP 7 V13, this I-device can be found under "Other field devices > PROFINET IO > PLCs & CPs" following installation.

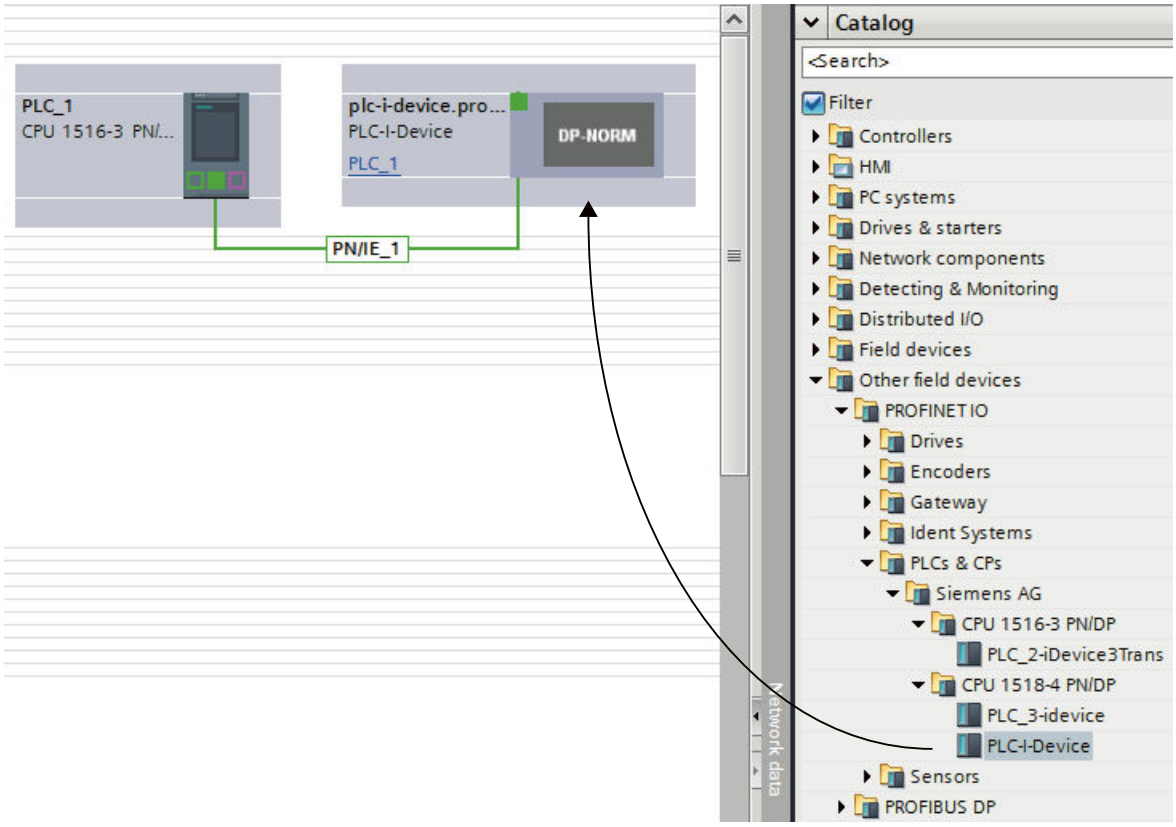


Figure 3-373 Configuring an I-device as a GSD file

In each of the projects involved, you define which transfer areas are assigned exclusively to the higher-level IO controller (default setting: all). Set the remaining transfer areas to "Outside of project". As a result of this setting, the local IO controller has no access to this transfer area and it can therefore be assigned to another IO controller in another project.

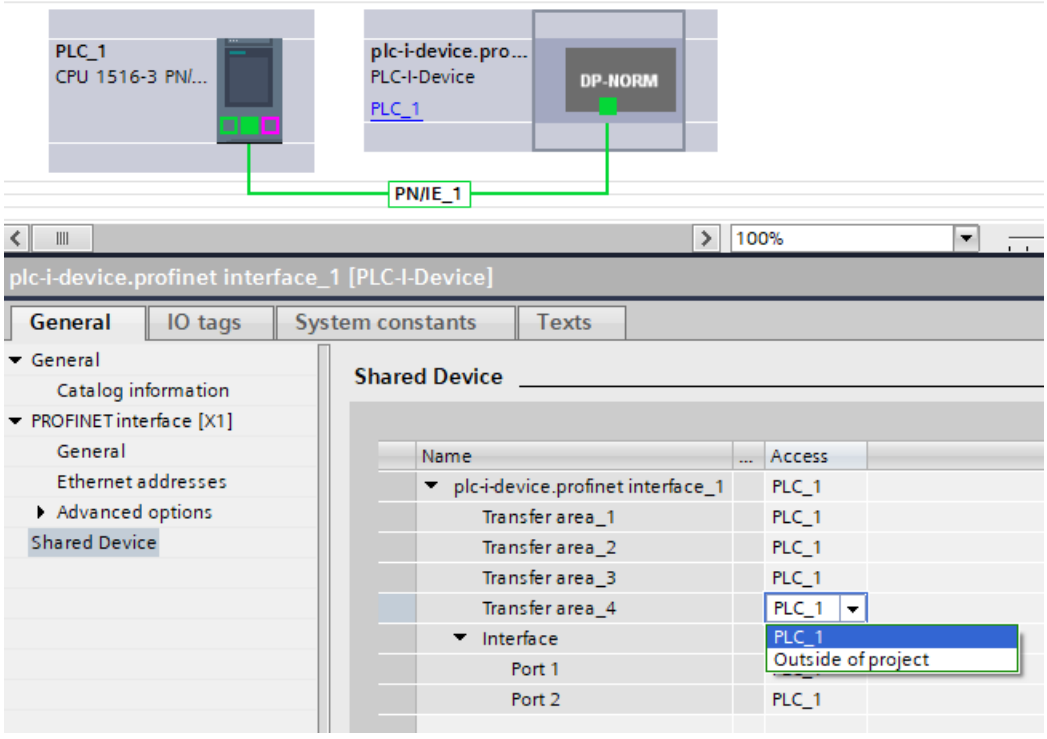


Figure 3-374 Setting the access to the shared I-device

You adapt the addresses from the view of the IO controller in the device overview. To open the device overview, double-click the I-device.

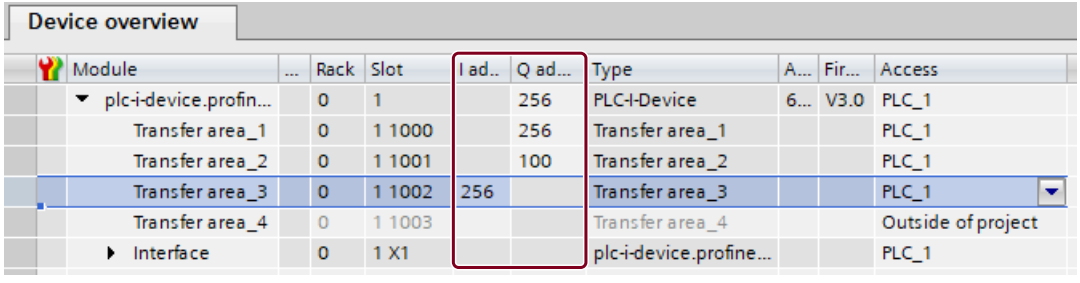


Figure 3-375 I/O addresses of the transfer areas in the device overview

Requirements

- STEP 7 as of V13

Procedure - Creating the PLC-I-device project

To create the project with a shared I-device, follow these steps:

1. Start STEP 7.
2. Create a new project with the name "PLC-I-device".
3. Insert, for example, a CPU 1518-4 PN/DP from the hardware catalog in the network view.
4. Assign a name, for example "PLC-I-Device".
5. Double-click the IO device and configure all required modules and submodules.
6. Assign the module parameters.

   In particular, the following settings for the CPU are necessary in the area of the PROFINET interface [X1]:

   – Activate the "IO device" option in the "Operating mode" area.
   – Activate the "Parameter assignment of PN interface by higher-level IO controller" option in the "Operating mode" area.
   – Configure the transfer areas in the "Operating mode > I-device communication" area. The "Address in IO controller" column remains empty because no IO controller is assigned.

     Note: To change an input area to an output area, and vice versa, you must navigate to the area of the corresponding transfer area.

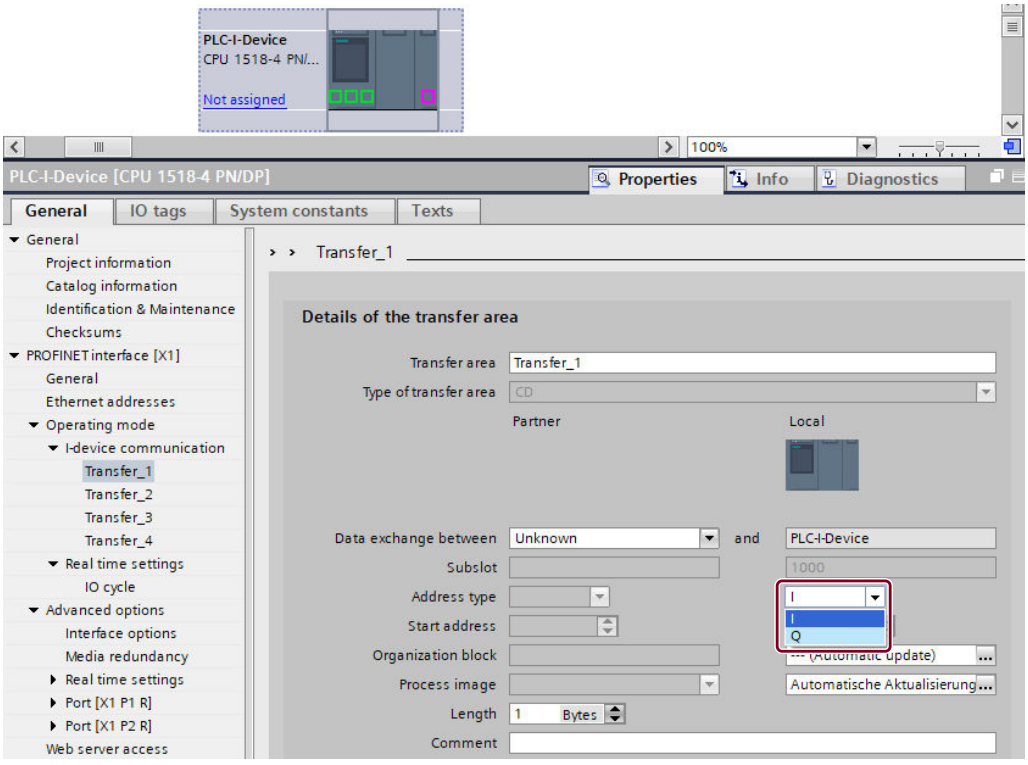


Figure 3-376 Changing the address type for the transfer area

   – Select the number of IO controllers outside the project with access to the I-device. If there is one IO controller outside the project, select "1" ("Operating mode > Real time settings", section "Shared device").

7. Click the "Compile" button in the toolbar to check your project for consistency errors. Inconsistent projects are not exported as GSD file by STEP 7.

8. Save the project.
9. Click the "Export" button ("Operating mode > I-device communication" area, "Export generic station description file (GSD) section").

   If you do not change the name in the Export dialog, the GSD file has a name in the form "GSDML-V2.31-#Siemens-PreConf_PLC-I-Device-20130925-123456", for example.

Procedure - Creating the PLC_1 project

To create the first project with a shared I-device, follow these steps:

1. Start STEP 7.
2. Install the PROFINET GSD file from the export of the I-device CPU (PLC-I-Device).
3. Create a new project with the name "PLC_1".
4. Insert, for example, a CPU 1516-3 PN/DP in the network view.
5. Assign a name, for example "PLC_1".
6. Insert the I-device from the hardware catalog (Hardware catalog: "Other field devices > PROFINET IO > PLCs & CPs").
7. Assign the I-device to the IO-controller "PLC_1".
8. Select the "Shared Device" area in the properties of the I-device.

   In the table, all transfer areas and the PROFINET interface are assigned to the local IO controller (PLC_1).
9. Define the transfer areas to which the "PLC_1" CPU should **not** have access. Select the "Outside of project" entry for these areas. These transfer areas are provided for the "PLC_2" CPU.
10. Save the project.

Procedure - Creating the PLC_2 project

To create the second project with a shared I-device, follow these steps:

1. Start STEP 7 once again.

   A new instance of STEP 7 opens.
2. In the new instance, create a new project with the name "PLC_2".
3. Insert, for example, a CPU 1516-3 PN/DP in the network view.
4. Assign a name, for example "PLC_2".
5. Insert the I-device from the hardware catalog (Hardware catalog: "Other field devices > PROFINET IO > PLCs & CPs").
6. Assign the I-device to the IO-controller "PLC_2".
7. Adapt the access to the transfer areas as in the "PLC_1" project. Ensure that no duplicate assignments result.
8. Adapt the parameters of the subnet and PROFINET interface. Because the shared I-device involves the same device in different projects, these data must match.
9. Save the project.

Both projects now have an identically configured shared I-device. The IO controller access and the parameters of the PROFINET interface must still be checked in the various projects during the next step.

Summary - Assigning parameters for access to the shared device

The transfer areas are automatically assigned to the local IO controller. To change the assignment, follow these steps:

1. Click the "PLC-I-Device" device in the network view of the "PLC_1" project, and select the "Shared Device" area.
2. A table shows which CPU has access to each of the configured transfer areas. The default setting is that the local CPU has access to all modules and submodules.
3. Keep the "PLC_1" setting for all transfer areas that are to remain in the address area of the local CPU

   Select the "Outside of project" setting for all transfer areas that are to be located in the address area of the "PLC_2" CPU from the "PLC_2" project. This means that an IO controller outside the project is to have access to the transfer area.
4. Follow the same procedure for the remaining projects.
5. Finally, check whether the settings for access are "complementary" for each module or submodule in both projects. This means that if the local CPU has access in one project, the "Outside of project" option must be set in the other project and vice versa.

   Special consideration: The "Outside of project" option for the PROFINET interface and therefore for the ports makes the associated parameters read-only and they cannot be changed. Parameters of the PROFINET interface and port parameters can only be edited in the project in which the PROFINET interface is assigned to the local CPU. The ports can be interconnected in both projects regardless of this.
6. Check whether the same IP address parameters and device name are set for the shared device in all projects.

   Check whether the same S7 subnet ID is set in all projects for the subnet to which the shared device is connected (subnet properties, "General" area in the Inspector window).

NOTE

If you make changes to the I-device (e.g., change the number or length of the transfer areas):
Export the I-device as a GSD file again. Re-install the GSD file in each project that uses the I-device as a shared device. Make sure that only one IO controller has access to a transfer area.

Procedure - Adapting the send clock in the real-time settings

You must set the same send clock for each IO controller that has access to modules or submodules of the shared I-device. This ensures that update times are calculated correctly with respect to the communication load.

To adjust and check these settings, use one of the following options:

- If you configure the IO controller with STEP 7 (TIA Portal):
  - Open the corresponding project.
  - At the IO controller, select the PROFINET interface that is connected to the shared I-device.
  - In the Inspector window, navigate to the "General > Advanced options > Real-time settings > IO communication" area.
  - In the drop-down list, select a common send clock.

- If you configure the IO controller with a different engineering tool:
  - Select the PROFINET interface of the shared device in STEP 7 (TIA Portal).
  - In the Inspector window, go to "General > Advanced options > Real-time settings >IO communication".
  - Read the send clock of the shared device.
  - Enter the read send clock in the other engineering tool.

Special consideration: If you configure **all** IO controllers that have access to the shared I-device in STEP 7 (TIA Portal or V5.5), you can set shorter send clocks on the IO controller than supported by the shared device (send clock adaptation).

Compiling and loading

You must compile the configurations for the different IO controllers and load them to the CPUs one after the other.

Due to the distributed configuration with separate projects, STEP 7 does not output consistency errors in the case of incorrect access parameter assignment. Example for incorrect access parameter assignment:

- Several IO controllers have access to the same module
- IP address parameters or send clocks are not identical

These errors do not show up until operation and are output as configuration errors, for example.

NOTE

After a configuration has been loaded in the IO controller, non-assigned modules or submodules in the IO device retain their current parameter assignment state. This ensures the independence to configurations of other IO controllers.

7.3.9 Module-internal shared input/shared output (MSI/MSO)

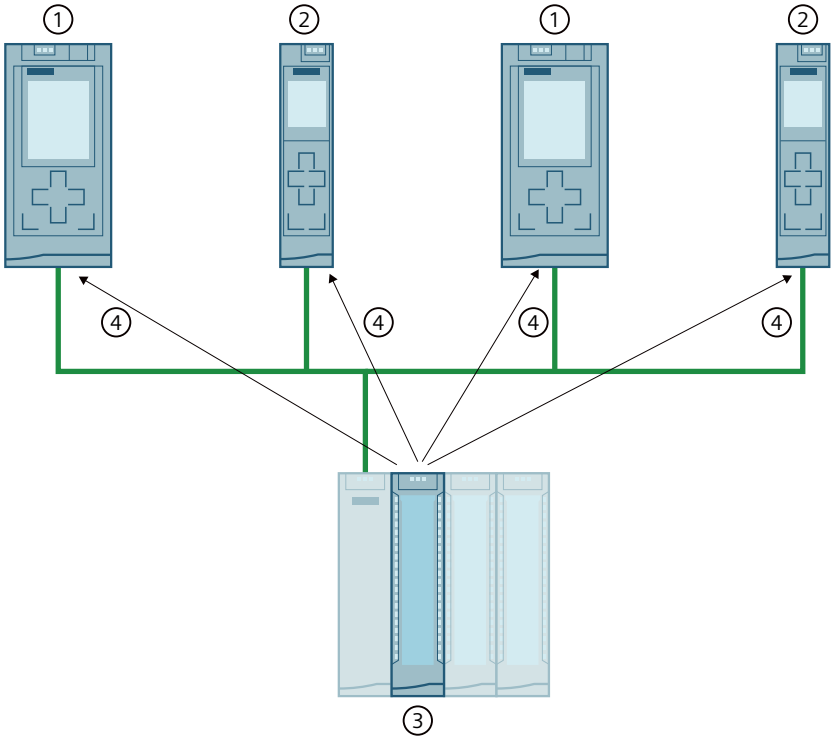
Introduction

This section describes the module-internal shared input/shared output (MSI/MSO) functionality for I/O modules that are operated on PROFINET.

Module-internal shared input/shared output functionality

The module-internal shared input (MSI) function allows an input module to make its input data available to up to 4 IO controllers. Each controller has read access to the same channels.

The following figure shows the MSI functionality.

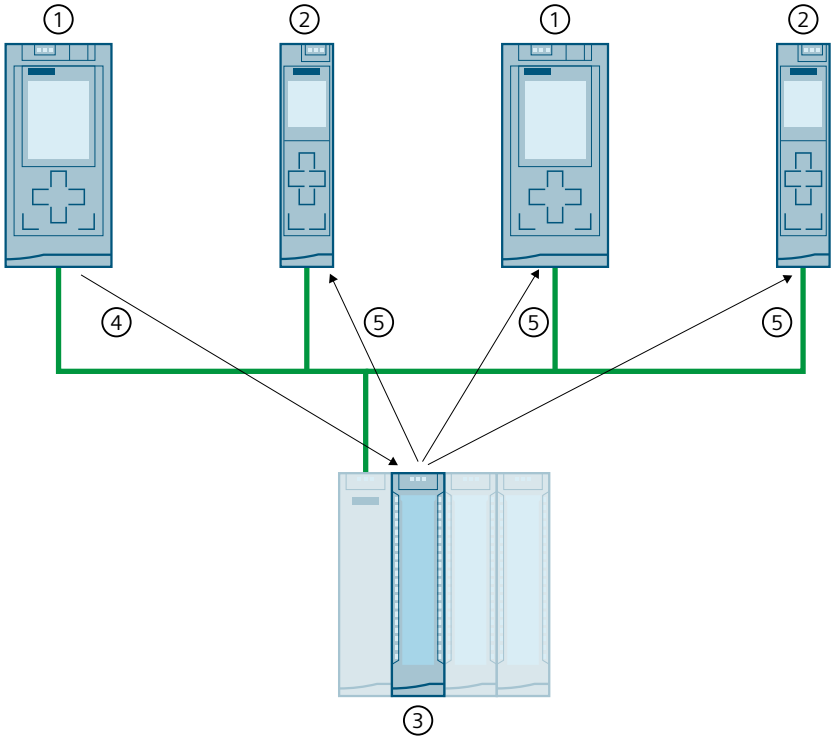


① CPU 1516-3 PN/DP as IO controller
② CPU 1511-1 PN as IO controller
③ Input module with MSI
④ Read access to the input channels of the input module
⑤ Write access to the channels of the I/O module (only with MSO)

Figure 3-377 Example configuration with MSI

The module-internal shared output (MSO) function allows an output module to make its output data available to up to 4 IO controllers. An IO controller has write access to the channels of the output module. Up to 3 IO controllers can additionally have read-access to the channels.

The following figure shows the MSO functionality.



① CPU 1516-3 PN/DP as IO controller
② CPU 1511-1 PN as IO controller
③ Output module with MSO
④ Write access to the output channels of the output module
⑤ Read access to the output channels of the output module

Figure 3-378 Example configuration with MSO

Advantages of MSI/MSO

Module-internal shared input/shared output (MSI/MSO) offers the following advantages:

- Real-time acquisition in multiple CPUs
- Lower costs due to saving on additional IO devices and modules
- Lower space requirements due to saving on additional IO devices and modules
- Reduced communication load because no CPU-CPU communication is needed
- No additional programming effort is needed for CPU-CPU communication

Requirements for the use of MSI/MSO

Observe the following requirements:

- MSI/MSO can only be used with PROFINET IO
- Configuration software: STEP 7 (TIA Portal) as of V12 SP1 with GSD file; the modules are integrated in the hardware catalog as of V13.
- The IM 155-5 PN ST interface module and the modules support MSI/MSO as of firmware version V2.0.0.

Constraints for using of MSI/MSO

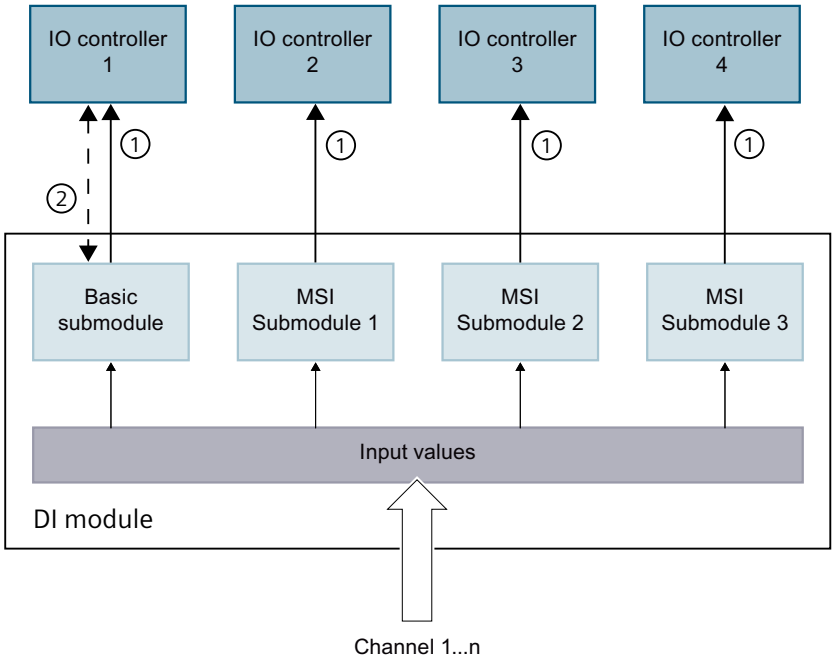
Note the following constraints:

- The use of MSI/MSO is not possible in the case of module grouping.
- Modules with MSI/MSO cannot be operated in isochronous mode.
- The maximum number of IO controllers is dependent on the interface module. You can find out how many IO controllers the interface module supports in the equipment manual for the respective interface module.

MSI submodules

The input values of all channels are copied to a basic submodule and up to 3 other MSI submodules during MSI configuration of an input module. The channels of the module are then available with identical input values in the basic submodule and the MSI submodules. The MSI submodules can be assigned to up to 3 IO controllers when the module is used in a shared device. Each IO controller has read access to the same channels.

The following figure shows a digital input module with the basic submodule and 3 MSI submodules. Each submodule is assigned to an IO controller. Diagnostics and parameter assignment of the digital input module can be performed from the IO controller 1 via the basic submodule.



① Read access
② Parameter assignment and system diagnostics

Figure 3-379 DI module with MSI submodules

Value status (Quality Information, QI)

The meaning of the value status depends on the submodule to which it pertains.

With basic submodule (= 1st submodule), the "0" value status indicates that the value is incorrect.

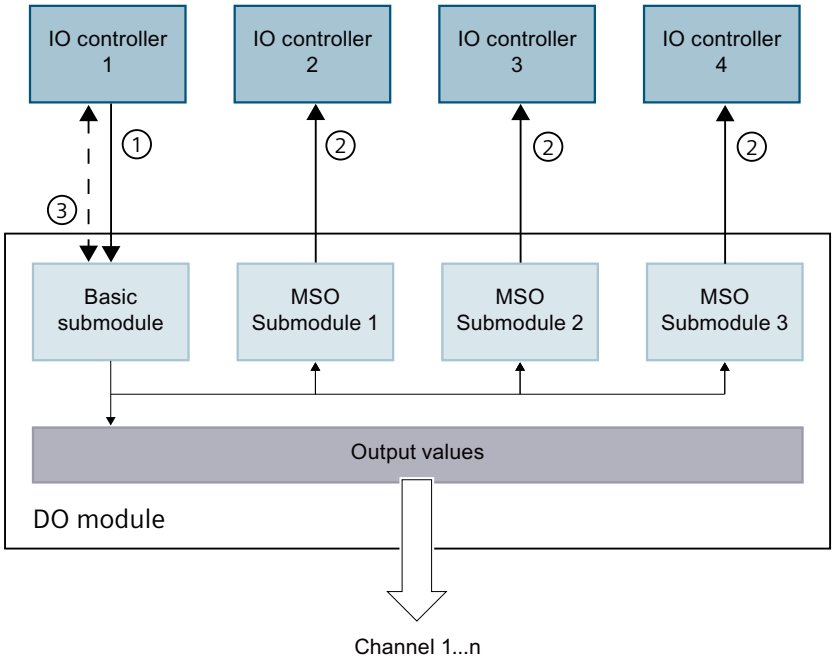
With an MSI submodule (2nd to 4th submodule), the "0" value status indicates that the value is incorrect or the basic submodule has not yet been configured (not ready).

MSO submodules

During MSO configuration of an output module, the output values of all channels of the module are copied from a basic submodule to up to 3 other MSO submodules. The channels of the module are then available with identical values in the basic submodule and the MSO submodules. The MSO submodules can be assigned to up to 3 IO controllers when the module is used in a shared device:

- The IO controller to which the basic submodule is assigned has write access to the outputs of the module. The basic submodule therefore occupies output addresses in the process image of the IO controller.
- The IO controllers to which the MSO submodules are assigned have read access to the outputs of the module. MSO submodules therefore occupy input addresses in the process image of the IO controller.

The following image shows a digital output module with the basic submodule and 3 MSI submodules. Each submodule is assigned to an IO controller. Diagnostics and parameter assignment of the digital output module can be performed from IO controller 1 via the basic submodule.



① Write access
② Read access
③ Parameter assignment and system diagnostics

Figure 3-380 DQ module with MSO submodule

Value status (Quality Information, QI)

The meaning of the value status depends on the submodule to which it pertains.

With basic submodule (= 1st submodule), the "0" value status indicates that the value is incorrect.

With MSO submodule (= 2nd to 4th submodule) the "0" value status indicates that the value is incorrect or one of the following errors has occurred:

- The basic submodule parameters have not yet been assigned (not ready for operation).
- The connection between the IO controller and the basic submodule has been interrupted.
- The IO controller from the basic submodule is in the "STOP" or "POWER OFF" state.

Configuring I/O modules with MSI/MSO submodules

Requirements

- STEP 7 as of V13
- IO device supports MSI/MSO (for example IM 155-5 PN ST as of firmware version 2.0.0)

Procedure

1. In the network view of STEP 7, insert an interface module, for example IM 155-5 PN ST as of V2.0.
2. Double-click the IO device.
   You are now in the device view.
3. Place the I/O modules from the hardware catalog in a suitable slot.
4. Add MSI/MSO submodules to the I/O modules:
   - Input modules: Select the number of MSI submodules under "Module parameters > DI Configuration" or "AI Configuration" in the area "Copy of module for Shared Device (MSI)".
   - Output modules: Select the number of MSO submodules under "Module parameters > DO configuration" or "AW configuration" in the area "Copy of module for shared device (MSO)".

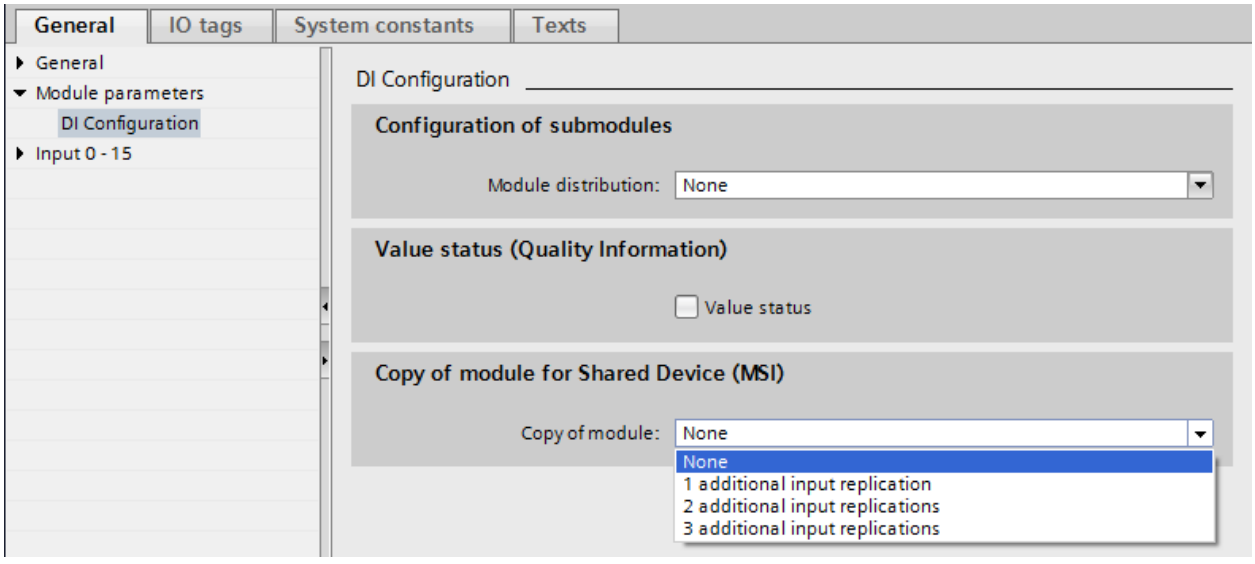


Figure 3-381 Configuring I/O modules with MSI/MSO

Assigning MSI/MSO submodules to an IO controller

You can assign the submodules in a shared device to an IO controller.

You can find additional information under "Configuring a shared device for different projects (Page 158)".

Configuring access to a shared device and the module-internal shared input / shared output (MSI /MSO) function

You can learn how to access a shared device and the MSI /MSO function in STEP 7 with this FAQ (https://support.industry.siemens.com/cs/ww/en/view/109736536).

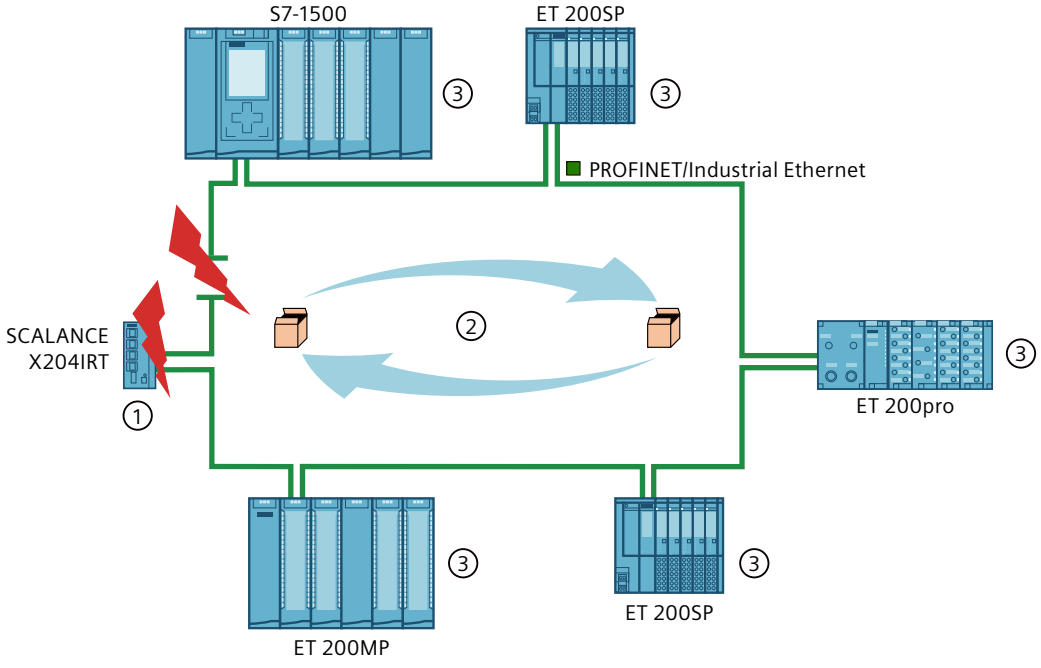
7.4 Media redundancy (ring topologies)

In order to increase the network availability of an Industrial Ethernet network with optical or electrical linear bus topologies, you can convert a linear bus topology to a ring topology by joining the ends together.

Media redundancy in ring topologies

Devices in a ring topology can be IO devices, IO controllers, external switches and/or the integrated switches of communication modules.

To set up a ring topology with media redundancy, you need to bring together the two free ends of a linear bus topology in one device. Closing the linear bus topology to form a ring is achieved with two ports (ring ports) of a device in the ring. One device of the resulting ring then takes over the role of the redundancy manager. All other devices in the ring are redundancy clients.



① Redundancy manager
② Test frames
③ Redundancy clients

Figure 3-382 Media redundancy in ring topology

The ring ports of a device are the ports that establish the connection to the two neighboring devices in the ring topology. The ring ports are selected and set in the configuration of the relevant device (is also preset, if applicable).

How media redundancy works in a ring topology

The data paths between the individual devices are automatically reconfigured if the ring is interrupted at any point. The devices are available again after reconfiguration.

In the redundancy manager, one of the two ring ports is blocked in uninterrupted network operation for normal communication so that no data frames are circulated. In terms of data transmission, the ring topology is a linear bus topology. The redundancy manager monitors the ring for interruptions. For this purpose, it sends test frames not only from ring port 1 but also from ring port 2. The test frames pass through the ring in both directions until they arrive at the other ring port of the redundancy manager.

An interruption of the ring can be caused by loss of the connection between two devices or by failure of a device in the ring.

If the test frames of the redundancy manager no longer arrive at the other ring port during an interruption of the ring, the redundancy manager connects its two ring ports. This substitute path once again restores a functioning connection between all remaining devices in the form of a linear bus topology.

The time between the ring interruption and restoration of a functional linear topology is known as the reconfiguration time.

As soon as the interruption has been eliminated, one of the two ring ports is blocked again in the redundancy manager. The redundancy clients are informed about the change and use the original paths to the other devices again.

Media redundancy method

The standard method of media redundancy in SIMATIC is MRP (Media Redundancy Protocol) with a typical reconfiguration time of 200 ms. Up to 50 devices can participate per ring.

In addition, the real-time capable media redundancy process MRPD (Media Redundancy with Planned Duplication of frames) is also available.

7.4.1 Media Redundancy Protocol (MRP)

Media Redundancy Protocol (MRP)

The "MRP" process works in conformity with the Media Redundancy Protocol (MRP) that is specified in the standard IEC 62439-2.

Requirements

- All devices in the ring support MRP.
- You have complied with the rules for topology set out below. STEP 7 monitors compliance with the rules during compilation and outputs corresponding alarms.

Topology

The following schematic shows a possible topology for devices in a ring with MRP. The devices inside the shaded oval are in the redundancy domain.

Example of a ring topology with the MRP media redundancy protocol:

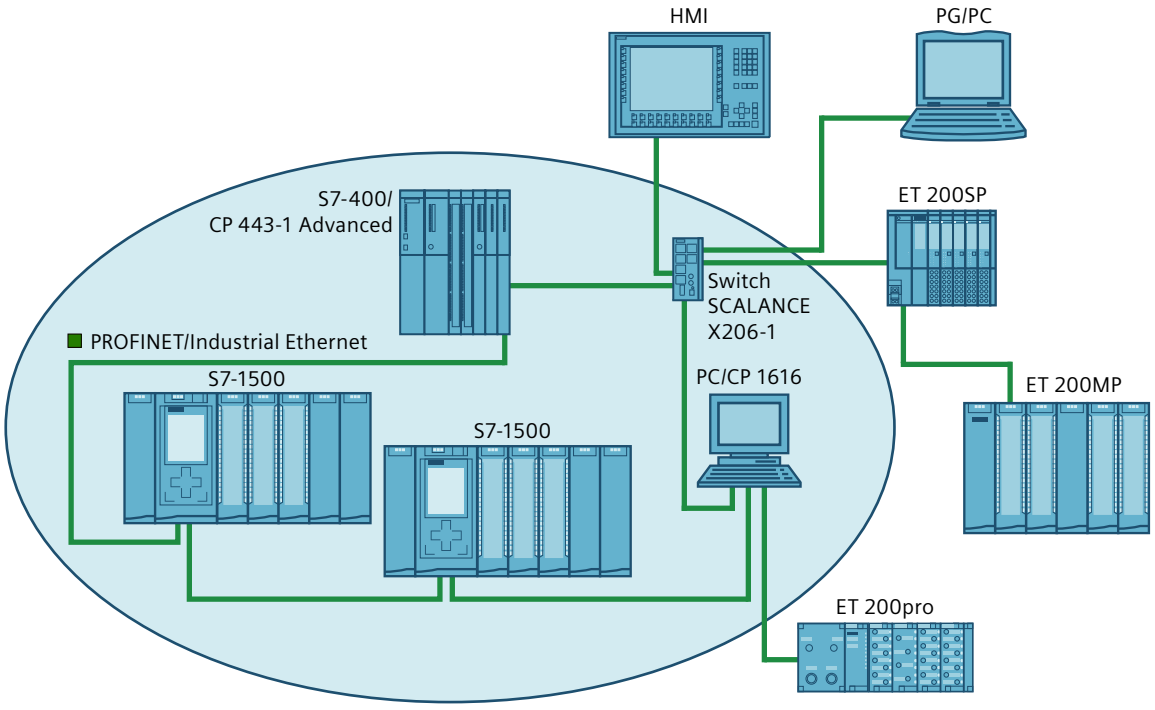


Figure 3-383 Example of a ring topology with the MRP media redundancy protocol:

The following rules apply to a ring topology with media redundancy using MRP:

- All devices must be connected to one other via their ring ports.
- All devices in the ring belong to the same redundancy domain.
- A device in the ring takes on the task of a redundancy manager.
  - One device only has the role of "Manager". No other device may have the role of "Manager". Or
  - One device or multiple devices in the ring have the role of "Manager (auto)". The devices with the role of "Manager (auto)" then negotiate between themselves which device is to take on the role of redundancy manager. In this case, no device is permitted to have the role of "Manager".
- All other devices in the ring are redundancy clients.
- You can connect up to 50 devices in a ring.

Non MRP-compliant devices can, for example, be connected to the ring via a SCALANCE X switch or via a PC with a CP 1616.

Rules for loading the devices of an MRP domain

When loading devices of an MRP domain, frame loops can occur and result in network failure if there is an invalid MRP configuration.

Example: You change the MRP roles of several devices and consecutively load the configuration into the devices involved. Configurations can arise that contradict the roles mentioned above, for example, there may be devices that simultaneously have the "Manager" and "Manager (auto)" roles in the ring.

To ensure that an invalid MRP configuration does not result in the failure of the network, open the ring before loading.

Follow these steps:

1. Open the ring.
2. Load the error-free and consistent MRP configuration from your project onto all the devices involved and ensure that the devices are in data exchange mode (i.e. the application relations (ARs) are set up).
3. Close the ring.

Boundary conditions

MRP and RT
RT operation is possible with the use of MRP.

NOTE
The RT communication is disrupted (station failure) if the reconfiguration time of the ring is greater than the selected response monitoring time of the IO device. This is why you should select a response monitoring time of the IO devices that is sufficiently large.

MRP and IRT
IRT mode is not possible together with MRP.

If you want to use media redundancy together with IRT in a ring, only use devices that support MRPD.

MRP and TCP/IP (TSEND, HTTP, ...)
The TCP/IP communication with MRP is possible, because lost data packages are resent, if applicable.

MRP and prioritized startup
If you configure MRP in a ring, you cannot use the "prioritized startup" function in PROFINET applications on the devices involved.

If you want to use the "prioritized startup" function, then you must disable MRP in the configuration (the device may also not be part of the ring).

Information on S7-1500R/H

You can find information on the media redundancy method MRP of the redundant S7-1500R/H system in section Configuring PROFINET IO on a redundant S7-1500R/H system (Page 330).

Application example: Reading the MRP status in the user program

The "LPNDR_ReadMRPState" function block from the "LPNDR" block library helps you to determine the status of the MRP ring per program. The block reads the MRP information from the PROFINET device (MRP Manager) and outputs the status.

The "LPNDR" block library and the corresponding documentation can be found in this application example (https://support.industry.siemens.com/cs/ww/de/view/109753067).

7.4.2 Configuring media redundancy

Configuring MRP

Proceed as follows to create a PROFINET IO configuration with MRP in STEP 7:

1. Generate a ring via the port interconnections in the topology view. First interconnect the devices to a line topology. Connect the unassigned port of the last device in the line with the unassigned port of the first device.
   The following example shows one CPU 1516-3 PN/DP and two interface modules IM 155-6 PN HF that are interconnected in a ring in the topology view of STEP 7.

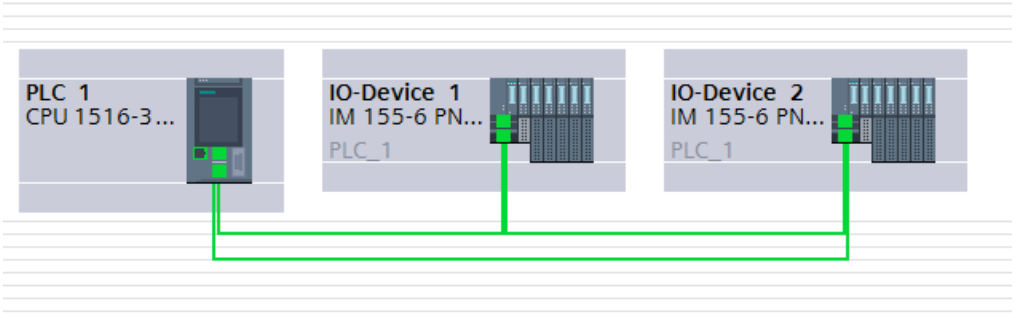


Figure 3-384 Configuring media redundancy

2. Select the PROFINET IO system in the network view.
3. In the Inspector window, navigate to "Properties" > "General" > "PROFINET" > "MRP domains" in the "Ring interconnections" field.
   This field shows you all the topological rings in the IO system with the associated MRP domains.
4. Select the ring generated above in the "Ring interconnections" field.
   The table below it shows all the PROFINET devices in the ring.

5. Set the media redundancy role for the PROFINET devices in the MRP role column.

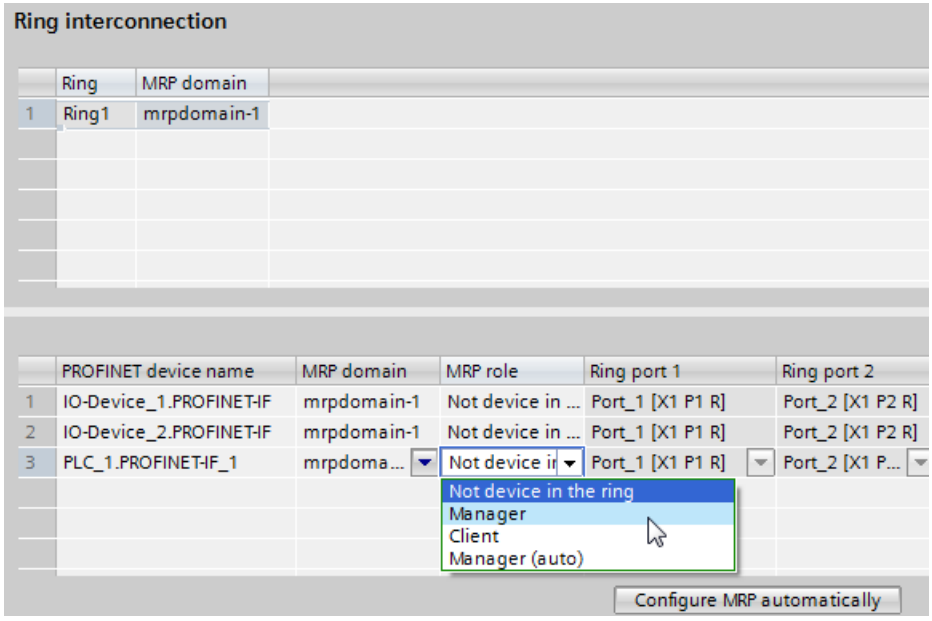


Figure 3-385 MRP domain

Automatic MRP configuration
You can also have the media redundancy roles assigned automatically for your PROFINET devices in the ring.

To have the media redundancy roles assigned automatically, click the "Configure MRP automatically" button. STEP 7 automatically assigns the media redundancy role for each device in the ring. After the automatic MRP configuration, you can make modifications to the media redundancy roles in the "MRP role" column.

"Media redundancy" setting options

Media redundancy role
Depending on the device used, the roles "Manager", "Manager (auto)", "Client" and "Not device in the ring" are available.

Rules:

- A ring must have precisely one device with the role "Manager". No additional devices with the role "Manager" or "Manager (auto)" are permissible. All the other devices may only have the "Client" role.
- If a ring has no device with the "Manager" role, the ring must at least have a device with the role "Manager (auto)". Any number of devices with the "Client" role may exist.
- Managers and clients of an MRP domain can be configured in different projects. In the project without a manager, you need to select the "Redundancy manager outside the project" option so that the configuration can be compiled. For multiple ring configurations, you need to set the option identically for each MRP domain.

Ring port 1 / Ring port 2
Select one at a time those ports you want to configure as ring port 1 or ring port 2. The drop-down list box shows the selection of possible ports for each device type. If the ports are set at the factory, then the fields are unavailable.

If you use single-stage commissioning, use the preset ring ports in STEP 7.

Diagnostic interrupts

If diagnostic interrupts to the MRP state are to be output in the local CPU, select the "Diagnostic interrupts" check box. The following diagnostic interrupts can be configured:

- Wiring or port error
  Diagnostic interrupts will be generated for the following errors in the ring ports:
  - A neighbor of the ring port does not support MRP.
  - A ring port is connected to a non-ring port
  - A ring port is connected to the ring port of another MRP domain.
- Interruption / return (redundancy manager only)
  - In case the ring is interrupted, a diagnostic interrupt "Ring open (incoming)" is generated.
  - When the ring is closed, the diagnostics "Ring open (outgoing)" is generated.

You can respond to these events in the user program by programming the appropriate response in the diagnostic error interrupt OB (OB 82).

Reference

You can find the procedure for configuring a common MRP ring and the topology with two projects in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/109741671).

7.4.3 Media redundancy with planned duplication of frames (MRPD; not for S7-1500R/H)

MRP extension "Media Redundancy with Planned Duplication of frames" (MRPD)

The MRP extension "Media Redundancy with Planned Duplication of frames" (MRPD) provides the advantage that, in the case of a failure of a device or a line in the ring, all other devices continue to be supplied with IO data without interruption and with short update times.

MRPD is based on IRT and MRP. To realize media redundancy with short update times, the PROFINET devices participating in the ring send their data in both directions. The devices receive this data at both ring ports so that there is no reconfiguration time.

Requirements for media redundancy with MRPD

- All the devices of the ring must support MRPD, for example interface module IM 155-6 PN HS as of firmware version 4.0.
- You have configured MRP for all the devices of the ring. You have assigned the MRP role "Not device in the ring" to devices that are not located in the ring.
- You have configured IRT for all the involved components.

Configuring MRPD

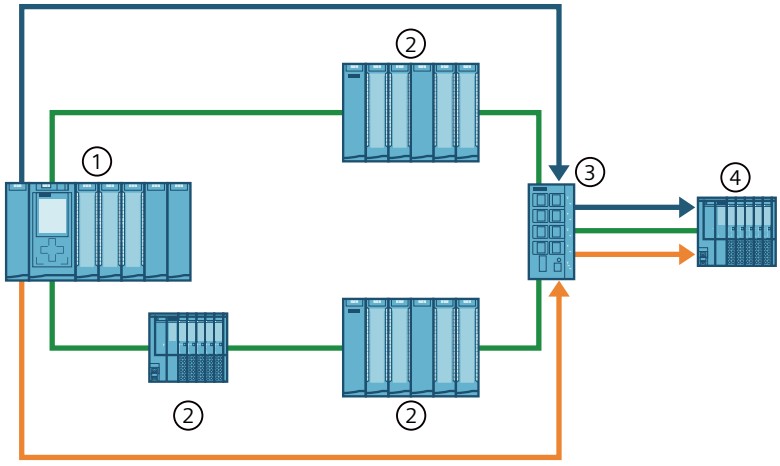
You do not have to explicitly activate MRPD in STEP 7. The function is available automatically as soon as all the requirements for MRPD are fulfilled.

Redundancy levels of IO devices with MRPD

The redundancy level of an IO device specifies how strongly the real-time communication is influenced in the case of a power interruption between an IO device and its IO controller.

- Full redundancy: No influence, because the IO controller and IO device are located in the same ring.
- Partial redundancy:
  - If the interruption takes place on a non-redundant part (line) between the IO device and IO controller, real-time communication is influenced.
  - If the interruption takes place on a redundant part (ring), real-time communication is not influenced.
- No redundancy: No redundant path between the IO device and its IO controller, communication is always influenced.

The figure below shows the redundancy levels of the IO devices for an example configuration with MRPD. The three devices in the ring and the switch have the redundancy level "Full redundancy". Device 4 has the redundancy level "Partial redundancy", because the connection between the switch and the device is not redundant.



① IO controller in the ring
② IO device in the ring with redundancy level "Full redundancy"
③ Switch in the ring with redundancy level "Full redundancy"
④ IO device in the spur with the redundancy level "Partial redundancy"

Figure 3-386 Example configuration with MRPD

The figure below shows the display of the redundancy levels in STEP 7 for the example configuration.

IO devices

PROFINET device name	RT class	Synchronization role	Redundancy level	DFP group
plc_1.profinet interface_1	RT,IRT	Sync master		
io-device_1	IRT	Sync slave	Full redundancy	
io-device_2	IRT	Sync slave	Full redundancy	
io-device_3	IRT	Sync slave	Full redundancy	
io-device_4	IRT	Sync slave	Partial redundancy	
switch_1	IRT	Sync slave	Full redundancy	

Figure 3-387 Display of the redundancy levels in STEP 7

7.4.4 Multiple rings

Multiple rings

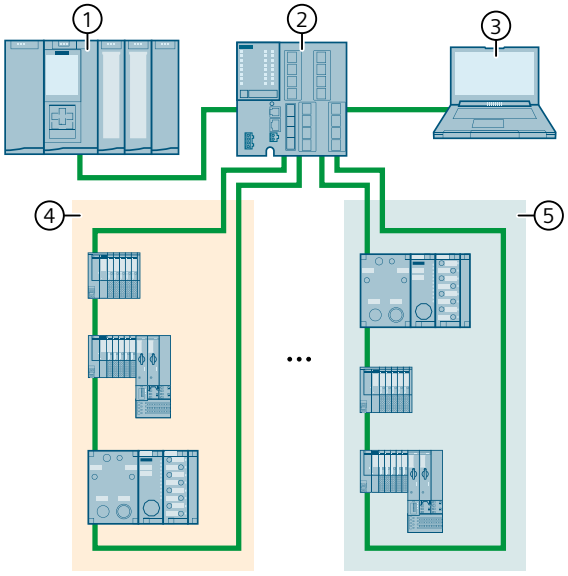
Use multiple rings to achieve higher availability for PROFINET IO networks with star topology.

In a multiple ring configuration, several PROFINET lines lead from a switch (star topology). The individual PROFINET lines lead from IO device to IO device. Redundant PROFINET cables run back to the switch from the last IO device on the individual lines.

The switch operates as a manager. The manager must have 2 ring ports for each ring. Depending on the number of available ring ports, several rings are possible.

The manager monitors all the rings individually: It checks for each particular ring (an MRP domain) whether the transmission path is intact. For this, the manager uses a separate MRP

instance each time. An MRP instance is required for each connected ring (set up by STEP 7 automatically).



① IO controller
② Switch, e.g. SCALANCE XM416-4C
③ PG/PC
④ MRP ring 1
⑤ MRP ring n

Figure 3-388 Configuration with several rings

Requirements

- SCALANCE X414 as of Version V3.10
- SCALANCE X300 as of version 4.0 (configured via GSD file)
- SCALANCE XM416 as of Version V6.4

Rules for the configuration of multiple rings

- You can find the rules for configuring multiple rings, for example, in the following Internet entry (https://support.industry.siemens.com/cs/us/en/view/109820936)
- MRP role at multiple rings:
  - The device that belongs to all rings must take on the role of "Manager".
  - All the other devices must have the "Client" role.

Configuring multiple rings

To configure an MRP configuration with multiple rings, follow these steps:

1. In the topology view, interconnect the ring ports of the devices that are intended to belong to an MRP domain to form a ring.
2. Select the PROFINET IO system in the network view.
3. In the Inspector window, navigate to "Properties" > "General" > "PROFINET Subnet" > "MRP domains" in the "Ring interconnection" field.
   This field shows you all the topological rings in the IO system with the associated MRP domains.
4. Select one of the rings generated above in the "Ring interconnection" field.
   The table below shows all the PROFINET devices in the ring.
5. Set the media redundancy role for the PROFINET devices in the MRP role column.

Example of multiple rings on a SCALANCE XM416

The following figure shows an example configuration for multiple rings.

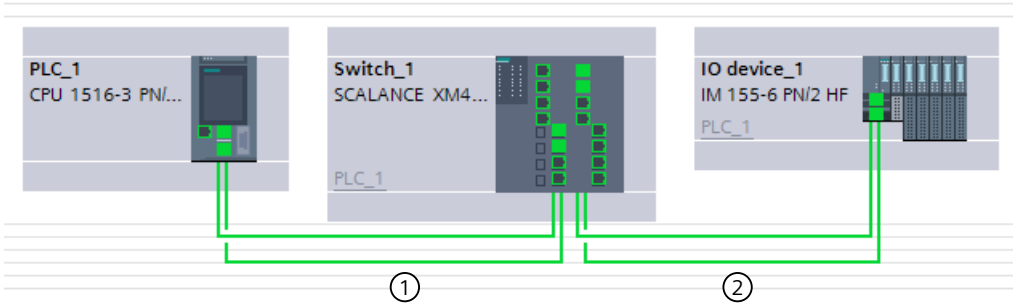


Figure 3-389 Example configuration with two rings ① and ②

In the example, Switch 1 belongs to two MRP rings. Ring 1 is formed by Switch 1 and PLC 1, Ring 2 by Switch 1 and IO device 1.

STEP 7 automatically assigns the "Manager" role to the switch. The other devices receive the "Client" role.

The manager is located at the point of intersection of the two rings 1 and 2. The manager monitors the two rings separately. To do this, it uses two MRP instances.

One MRP instance checks whether all devices in ring 1 are reachable, another instance monitors whether all devices in ring 2 are reachable (only one device in each case in the example).

You can configure each MRP instance separately.

The following figure shows the two MRP instances in the manager (PROFINET interface of the switch). Here in the example, MRP instance 1 checks whether the devices in the MRP domain "mrpdomain-1" can be reached. The MRP instance 2 is responsible for monitoring the devices of the MRP domain "mrpdomain-2".

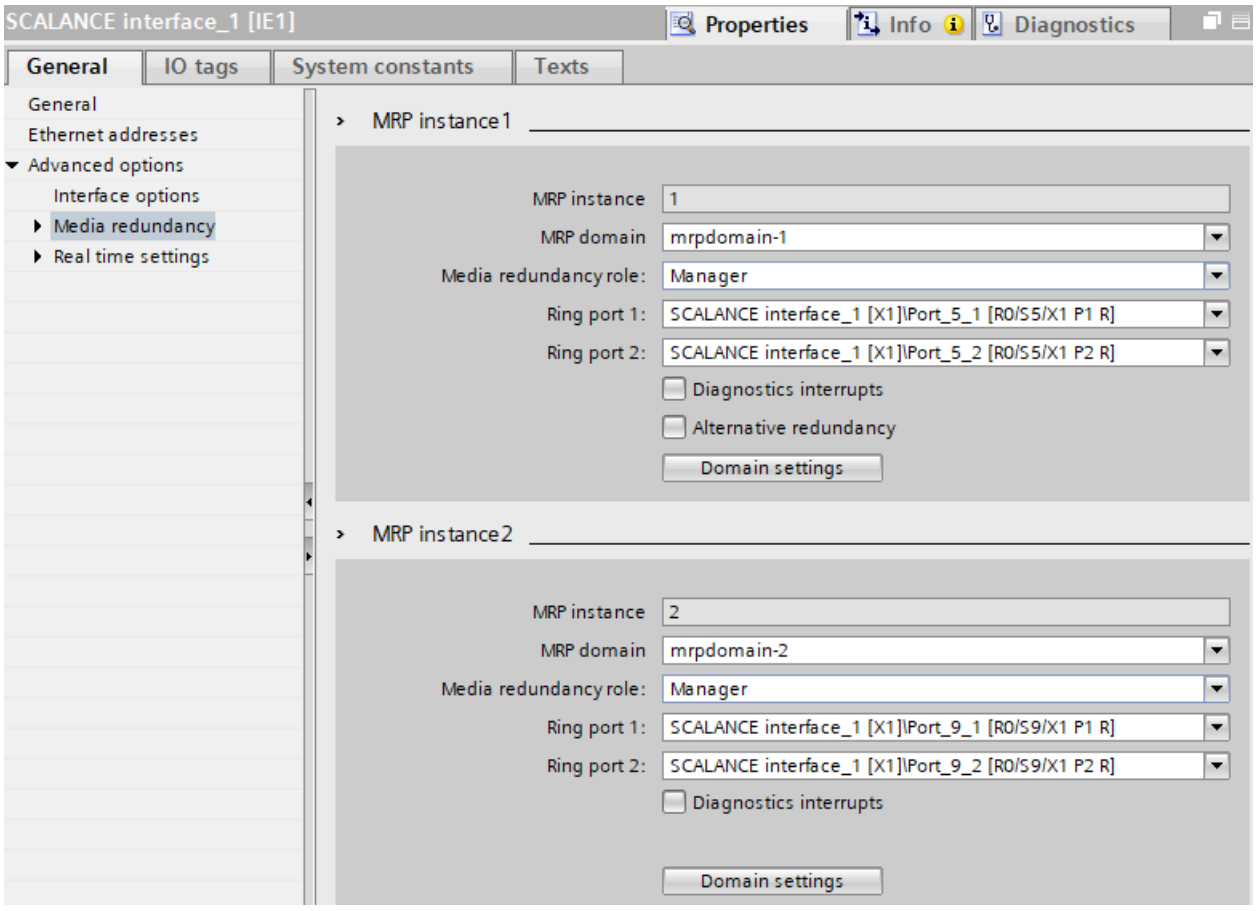


Figure 3-390 Setting media redundancy for multiple rings

The following figure shows Ring 1 (mrpdomain-1). The participants of the mrpdomain-1 are the PROFINET interface of the CPU as the "Client" and the MRP interface 1 of the PROFINET interface of the switch as the "Manager".

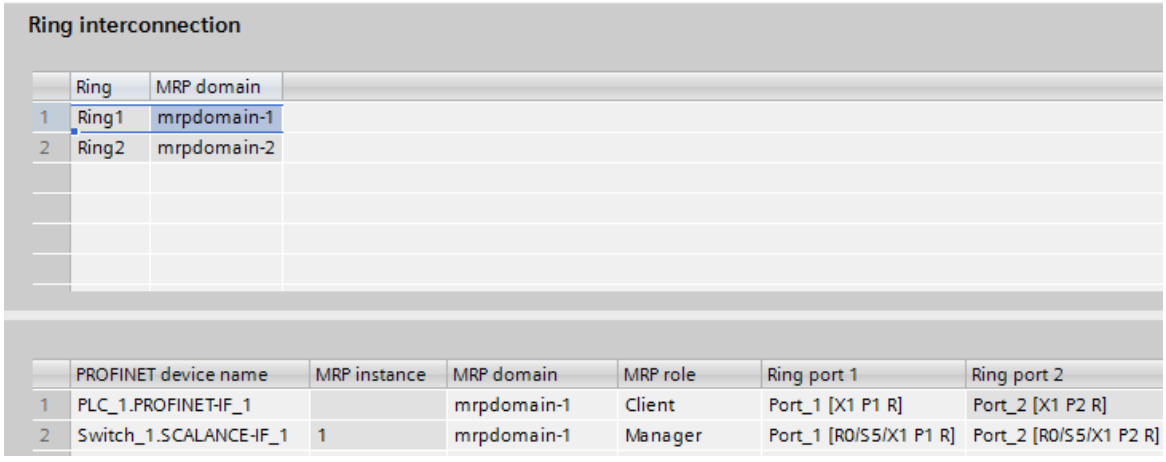


Figure 3-391 Ring 1

The following figure shows Ring 2 (mrpdomain-2). The participants of the mrpdomain-2 are the PROFINET interface of the IO device as the "Client" and the MRP instance 2 of the PROFINET interface of the switch as the "Manager".

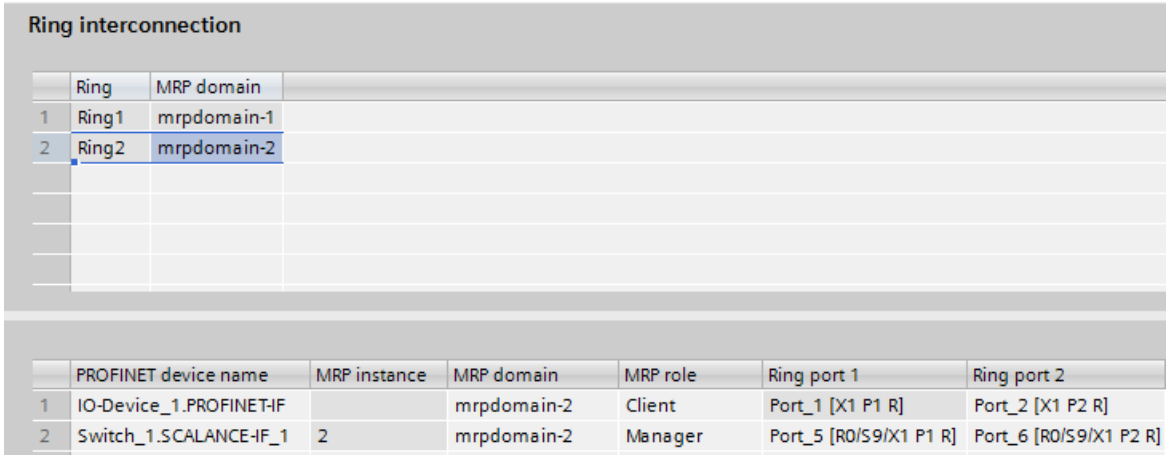


Figure 3-392 Ring 2

7.4.5 MRP interconnection

Definition

The process MRP interconnection is an enhancement of MRP and allows the redundant coupling of two or more rings with MRP in PROFINET networks. MRP interconnection is - like MRP - specified in the standard IEC 62439-2 (Edition 3).

Advantages

MRP interconnection allows the monitoring of larger topologies with ring redundancy. With MRP interconnection, you are not limited to the maximum number of 50 devices in a ring when setting up redundant network topologies. For information on the quantity structure of MRP Interconnection, refer to the SCALANCE XM-400/XR-500 Web Based Management (WBM) (https://support.industry.siemens.com/cs/ww/en/view/109760840) configuration manual.

Requirements

- The media redundancy procedure MRP is used in the participating rings.
- Each ring has its own MRP domain with an MRP manager and MRP clients.
- As MRP managers in the rings, the PROFINET devices support MRP interconnection (see technical specifications of the devices).

  S7-1500 CPUs as of firmware version V2.9 support MRP interconnection.
- If you use PROFINET devices with more than 2 ports as MRP clients in the ring, then MRP interconnection is binding for these devices. For a device without MRP interconnection, telegrams leave the ring. This results in an additional load on the network.
- If you use PROFINET devices with only 2 ports in the ring as MRP clients, then MRP interconnection is recommended for all devices in the ring.

4 devices for MRP interconnection connections

2 MRP-interconnection connections provide redundant coupling between 2 MRP rings. Four devices are required for the 2 connections:

- A Media Redundancy Interconnection Manager (MIM)
- 3 media-redundancy interconnection clients (MIC):
  - Primary MIC
  - Primary Coupled MIC
  - Secondary Coupled MIC

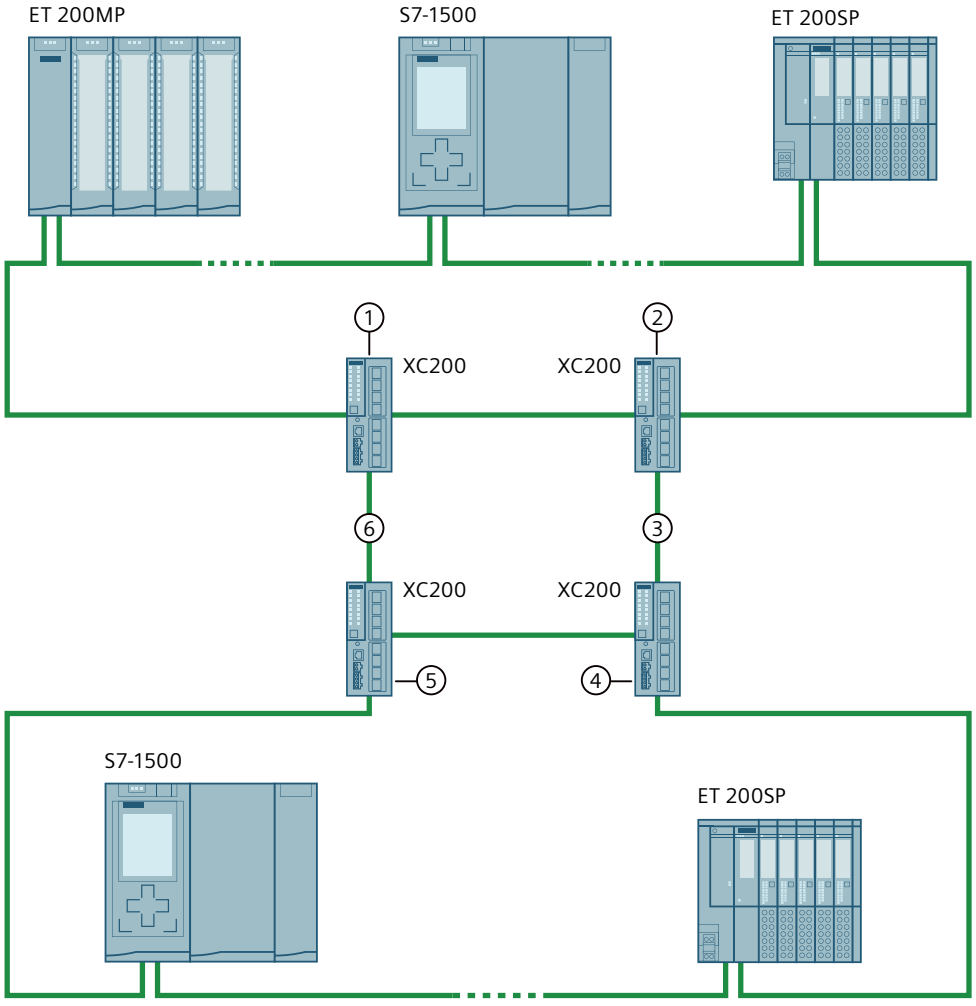
Since each of the four devices is part of an MRP ring, each device also assumes a media redundancy role.

Each of the 4 devices can take over the MRP manager role or MRP client role.

Topology

The following screen shows the redundant coupling of 2 MRP rings.

Redundancy: If the primary connection (primary link) between the two rings is interrupted, the secondary connection (secondary link) takes over the data exchange between the rings after a short reconfiguration time.



① Primary MIC
② Media Redundancy Interconnection Manager (MIM)
③ Secondary link
④ Secondary Coupled MIC
⑤ Primary Coupled MIC
⑥ Primary link

Figure 3-393 Example: Redundant connection of 2 rings with MRP interconnection

Function of the interconnection ports

Interconnection ports are appropriately configured PROFINET ports of the 4 devices for MRP interconnection. The primary or secondary connection of the rings exists between the interconnection ports.

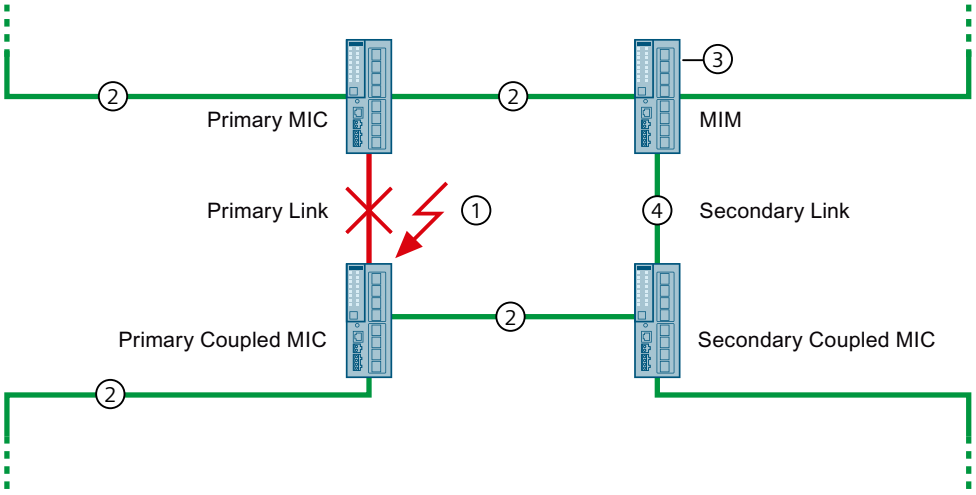
Via the interconnection ports; the MIM is always informed about the connection status between the Primary MIC and the Primary Coupled MIC ("primary connection") as well as its own connection to the Secondary Coupled MIC ("secondary connection").

Depending on the connection status of the interconnection ports, each MIC sends a message to the MIM when its status changes (Link-Up or Link-Down).

In regular operation the data between the two rings is exchanged over the primary connection (primary link) and the MIM blocks its interconnection port.

Link-Down of the primary connection

In the figure below, the primary connection was interrupted (Link-Down).



① Link-Down
② Status message: Link-Down primary connection
③ Blocking of the interconnection port is released
④ Data exchange via secondary connection

Figure 3-394 Link-Down of the primary connection

With a Link-Down of the primary connection ①, Primary MIC and Primary Coupled MIC send the status message "Link-Down" via all lines ②.

The MIM then unblocks its interconnection port at ③ and informs the MRP managers in both rings to trigger the reconfiguration of the rings.

After the reconfiguration, the data exchange between the two rings takes place via the secondary connection ④.

As soon as Primary MIC and Primary Coupled "Link-Up" for the primary connection, the MIM blocks its interconnection port and informs the MRP managers in both rings to trigger the reconfiguration of the rings.

After the reconfiguration, the data exchange is again carried out via the primary connection.

Configuring and assigning MRP interconnection parameters

NOTE

MRP interconnection is not integrated into the TIA Portal. This means you cannot configure, parameterize and diagnose MRP interconnection in STEP 7.

You configure and assign MRP interconnection parameters via the integrated web pages (Web Based Management) of the SCALANCE switches used as MIM and MIC (e.g. SCALANCE XC200, XM-400, XR-500).

For the configuration, follow the step-by-step instruction in the configuration manual SCALANCE XM-400/XR-500 Web Based Management (WBM) (https://support.industry.siemens.com/cs/ww/en/view/109760840).

Reconfiguration and watchdog timer

The reconfiguration time of the rings is typically less than 200 milliseconds.

In order for the data exchange to work after a reconfiguration, the watchdog timers of the IO devices must be set sufficiently large. Therefore, when using MRP interconnection, set the watchdog timer of the IO devices to 256 milliseconds or more.

7.5 Real-time communication

7.5.1 Introduction

Properties

PROFINET IO is a scalable real-time communication system based on the Layer 2 protocol for Fast Ethernet. With the RT transmission method, two real-time-support performance levels are available for time-critical process data and IRT for high-accuracy and also isochronous processes .

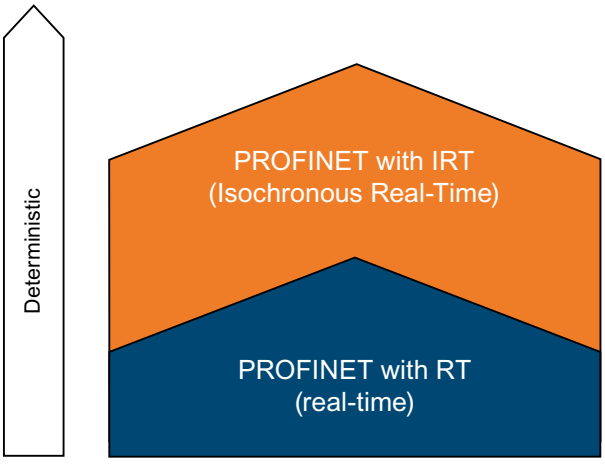


Figure 3-395 Real-time communication performance

Real-time communication and IT communication

Industrial communication, especially in the factory automation and process automation, requires a punctual and deterministic data transmission. This is why, for the cyclic exchange of time-critical IO user data, PROFINET IO does not use TCP/IP, it uses real-time communication (RT) or isochronous real-time communication (IRT) for the synchronized data exchange in reserved time intervals.

Fields of application of PROFINET with RT

PROFINET with RT is suited for:

- Time-critical applications in factory automation
- The implementation of large quantity structures in line process plants

Fields of application of PROFINET with IRT

PROFINET with IRT is particularly suitable for:

- Considerable deterministics with large quantity structures concerning the I/O user data communication (productive data)
- Considerable performance also with many devices concerning the I/O user data communication (productive data)
- Parallel transfer of productive and TCP/IP data via a cable, even with considerable data traffic whilst ensuring the forwarding of productive data by reserving the transmission bandwidth.

International standard IEC 61158

The communication procedures RT and IRT are standardized in the international standard IEC 61158.

7.5.2 RT

PROFINET IO with real-time communication (RT) is the ideal solution for integrating IO systems. This is a solution that also uses standard Ethernet in the devices and commercially available industrial switches as infrastructure components. A special hardware support is not required.

If you want to use PROFINET functions that provide an additional value, such as topology detection, diagnostics, device exchange without exchangeable medium/PG, you have to use switches that support the PROFINET standard according to the IEC 61158 standard. In the integrated switches of PROFINET devices and PROFINET switches (e.g., the SCALANCE product family), PROFINET functions in accordance with the PROFINET standard are implemented and can be used without restriction for integration in the PROFINET IO system (see also section Active network components (Page 40).

Real-time communication (RT)

PROFINET IO frames have priority over standard frames in accordance with IEEE802.1Q. This ensures the required determinism in the automation technology. The data is transferred via prioritized Ethernet frames. With RT, you can achieve update times ≥ 250 µs with RT.

Switching mechanisms

Switches in SIMATIC meet the real-time requirements with two mechanisms on PROFINET: "Store and forward" and "Cut through".

Store and forward

In the Store and forward method, the switch stores the frames completely and places them in a queue. If the switch supports the international standard IEEE 802.1Q, then the data is sorted according to its priority in the queue. The frames are then forwarded selectively to the specific port that can access the addressed node (Store and forward).

Cut through

In the Cut through process the entire data package is not stored temporarily in a buffer, it is passed directly onto the target port as soon as the target address and the target port have been determined.

The times required by the data package to pass through the switch are then minimal and independent of the frame length. The data are only stored temporarily in accordance with the Store and forward process as per priority when the section between the target segment and the port of the next switch is occupied.

7.5.3 IRT

Isochronous real-time communication (IRT)

IRT is a synchronized communication protocol for cyclic exchange of IRT data between PROFINET devices. A reserved bandwidth is available in the send cycle for IRT data. The reserved bandwidth ensures that the IRT data can be transferred at reserved synchronized intervals, without being influenced also by higher other network loads (such as TCP/IP communication, or additional real-time communication).

Advantages

PROFINET with IRT is synchronized communication in reserved time intervals. With IRT you have the option to be able to control time-critical applications such as motion control via PROFINET. With IRT you use further advantages:

- High-precision deterministics allow highest control quality and thus, for example, exact positioning of axes
- Simple and flexible integration of PROFINET devices for real-time applications in existing company networks

- Shortest response times and highest deterministics by means of bandwidth reservation and thus also for applications that have to satisfy highest performance requirements (e.g., printing control/position control for presses, print-mark recognition with packaging machines)
- Secured standard communication parallel to real-time communication via the same transmission medium
- You can continue to use standard components for your PROFINET IO system outside of the sync domain

Properties of isochronous real-time

Topology configuration is a prerequisite for IRT.

In addition to the reserved bandwidth, the frames from defined transmission paths are exchanged for the further optimization of data transfers. For this, the topological information from the configuration is used for planning the communication. Transmission and reception points of every individual data frame at every communication node are thus guaranteed. This allows you to achieve optimal usage of the bandwidth and reach the best possible performance in the PROFINET IO system.

Use of IRT allows you to achieve update times with very high deterministics ≥ 125 µs and a jitter accuracy of the send clock < 1 µs. Isochronous applications are possible with IRT (see section Isochronous mode (Page 220)).

* The minimum update time depends on the CPU used. The update times supported by a CPU are listed in the technical specifications of the CPU manual.

NOTE

IWLAN and IRT

PROFINET devices that are connected to PROFINET IO via access points, do not support IRT.

Synchronization

The prerequisite for the IRTcommunication is a synchronization cycle for all PROFINET devices in a sync domain for distributing a mutual time basis. A synchronism of the transmission cycle of the PROFINET devices within a sync domain is achieved with this basic synchronization.

A sync master specifies the clock to which sync slaves are synchronized. An IO controller or an IO device can have the role of sync master. If the sync master fails, all IO devices with IRT will fail.

Sync master and sync slaves are always devices in a sync domain. Bandwidth is reserved within the sync domain for IRT communication. Real-time and non-real-time communication (TCP/IP communication) is possible outside of the reserved bandwidth.

Default sync domain

If you have created a PROFINET subnet, a special sync domain is automatically created, the default sync domain. All PROFINET devices configured for the PROFINET subnet automatically belong to this sync domain.

For additional information on creating sync domains, refer to the STEP 7 online help.

Time ranges of the communication cycle

The communication cycle is divided into three time ranges, which are shown in the following chart:

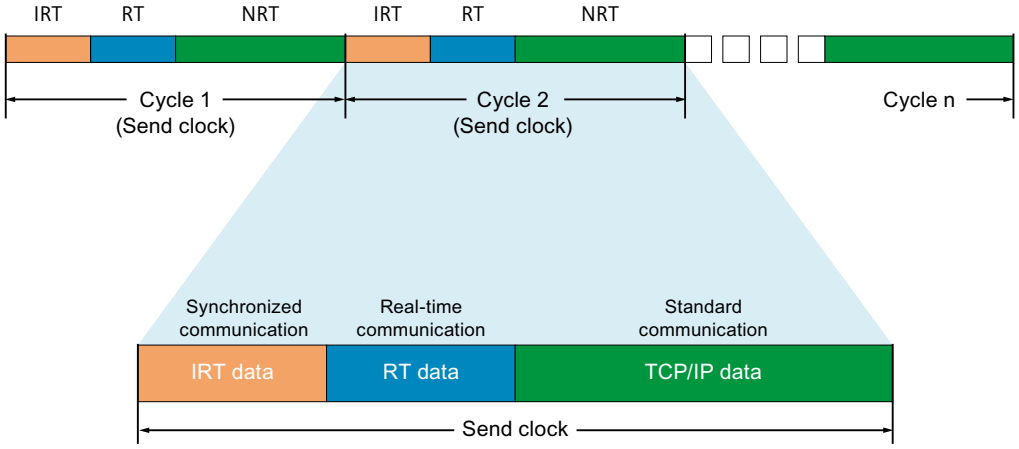


Figure 3-396 Reserving bandwidth

- IRT data (synchronized communication)

  This time range can be reserved in specific steps, depending on the send clock. Only IRT data is transmitted during this time range.
- RT data (real-time communication)

  The cyclic RT data is transferred in this time range. RT data is prioritized over "normal" TCP/IP data. TCP/IP data or Ethernet frames can have a priority of between 1 and 7. RT data have the Priority 6.
- TCP/IP data (standard communication)

  Standard communication (e.g., TCP/IP) is transmitted in the remaining interval of the communication cycle.

In STEP 7, you can set the ratio of the bandwidth usage of cyclic IO data to standard communication. For information on how to set the bandwidth usage, refer to the section Setting the bandwidth usage for the send clock (Page 205)

7.5.4 Comparison of RT and IRT

The most important differences between RT and IRT

Table 3-46 Comparison between RT and IRT

Property	RT	IRT
Transmission method	Prioritizing the RT frames through Ethernet priority (VLAN tag)	Path-based switching on the basis of a communication path plan; no transmission of TCP/IP frames in the time range with IRT communication.
Determinism	Variance of the duration of transmission by the shared use of the transmission bandwidth with other protocols (e.g., TCP/IP)	Exact, planned transmission, transmission and reception times are guaranteed for all topologies.

Property	RT	IRT
Hardware support through special Ethernet controllers is required	Not required	Required
Isochronous application	-	Yes
Starting time of the isochronous application	-	The point in time for the reception of the data is planned exactly. Application can be started synchronized to the cycle.

7.5.5 Configuring PROFINET IO with IRT

Introduction

If you want to configure a PROFINET IO system with IRT, you have to configure the PROFINET IO devices. These PROFINET devices must support IRT. Set which device acts as the sync master and synchronizes the other devices. This is done by configuring a sync domain with a sync master and at least one sync slave.

Requirement

- There is an IO system with an IO controller and at least one IO device.
- You have configured the topology for the IO system.
- The devices support IRT.

Procedure

Proceed as follows to enable an existing IO system for the use of IRT:

1. Select the PROFINET interface of the IO controller.
2. In the Inspector window, navigate to "Advanced options > Real time settings > Synchronization".

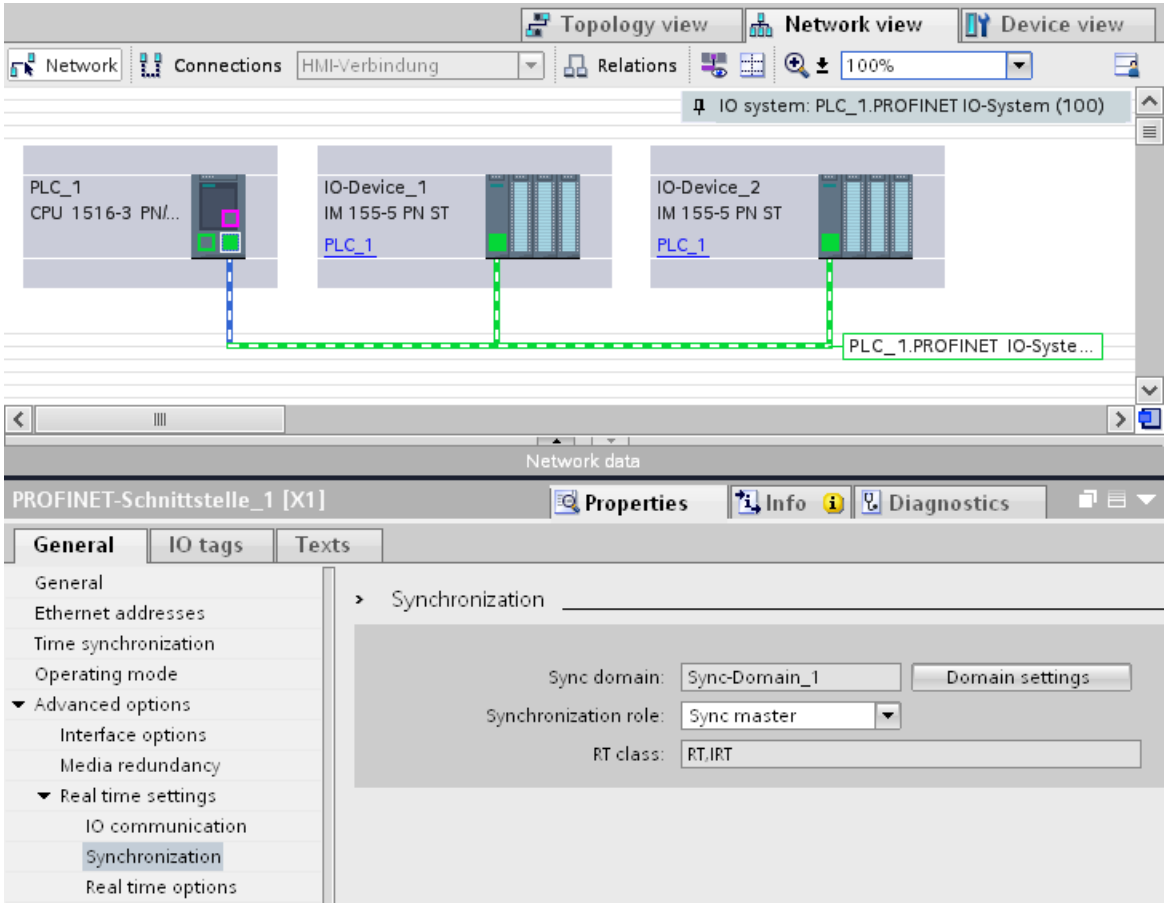


Figure 3-397 IRT configuring sync master

3. Assign the IO controller the role of sync master under "Synchronization role".
4. Select the PROFINET interfaces of an associated IO device.

5. In the Inspector window, navigate to "Advanced options > Real time settings > Synchronization".

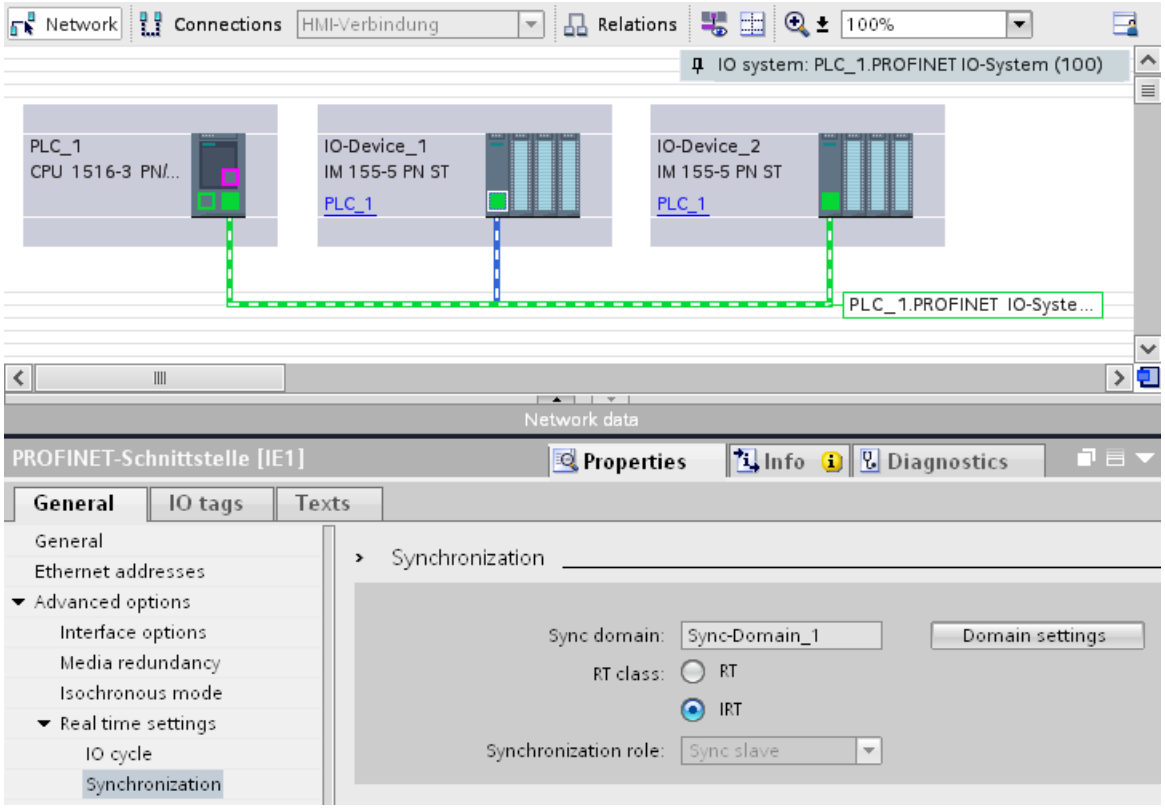


Figure 3-398 IRT configuring sync slave

6. Activate the RT class "IRT". The IO device will then automatically be assigned the synchronization role "sync slave".
7. You can check and correct your settings at any time using the "Domain settings" button.

Or

1. Highlight the PROFINET IO system in the network view.
2. Click on the PROFINET IO system.

3. Navigate to the device of the required sync domain in the Inspector window.

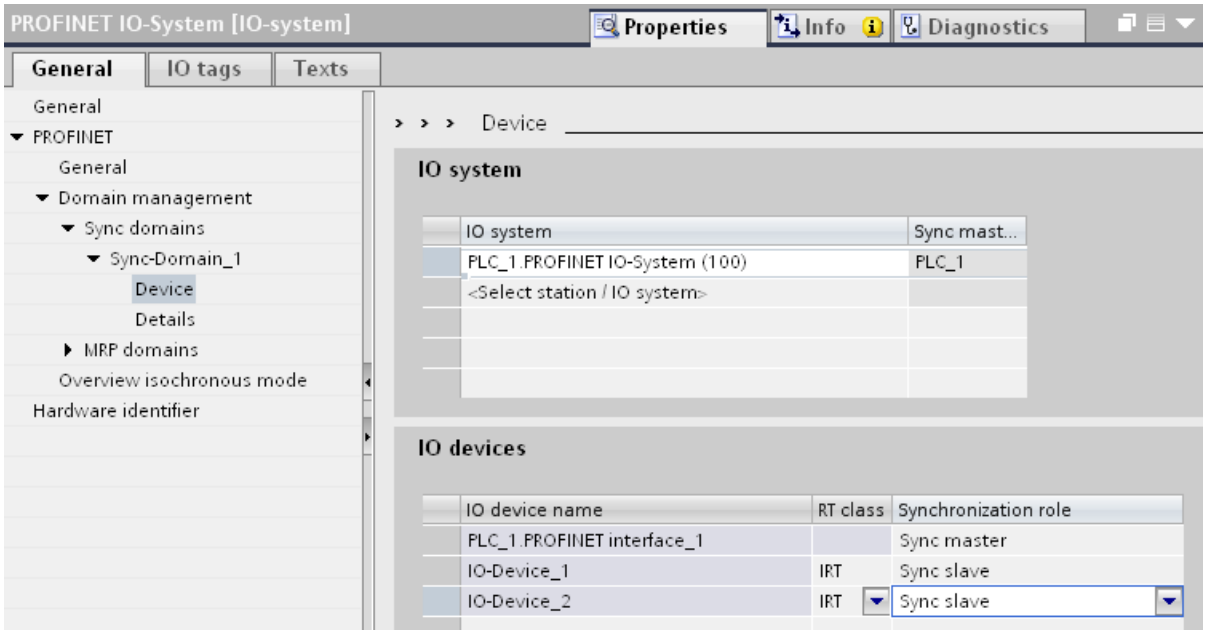


Figure 3-399 IRT configuring sync domain

4. Enter all necessary settings in the tables:
   - Select an IO system.
   - Set the synchronization role "sync master" for the IO controller.
   - Set the RT class for the IO devices to "IRT". The IO devices will then automatically be assigned the synchronization role "sync slave".

You can now load the configuration to the relevant devices with PROFINET IRT.

7.5.6 Setting the bandwidth usage for the send clock

Bandwidth level

For PROFINET IO with IRT, you can specify the maximum portion of the send cycle that you want to use for cyclic IO communication.

You have the following setting options for the bandwidth usage in STEP 7.

- Maximum 25% cyclic IO data. Focus on non-cyclic data.
- Maximum 37.5% cyclic IO data. Focus on non-cyclic data.
- Maximum 50% cyclic IO data. Balanced proportion.
- Maximum 90% cyclic IO data. Focus on cyclic IO data. (Requirement: The "Make 'high performance' possible" option is activated)

Setting the bandwidth usage

To set the bandwidth usage for a PROFINET IO system in STEP 7, follow these steps:

1. Select your IO system in the network view of STEP 7.
2. In the Inspector window, go to "Properties" > "General" > "PROFINET" > "Domain management" > "Sync domains" > "Name of the sync domain" > "Details".
3. Select the desired level of bandwidth usage from the "Bandwidth use" drop-drop down list box.

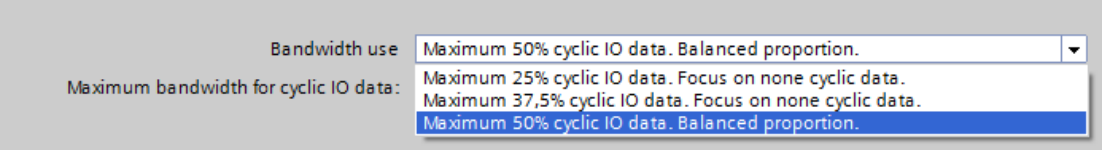


Figure 3-400 Setting the bandwidth usage

For information on how to set the bandwidth usage for IRT with maximum performance, refer to the section Configuration of IRT with high performance (Page 217)

7.5.7 Setup recommendations for optimizing PROFINET

Optimizing PROFINET with RT

PROFINET provides you with high-performance communication on all levels.
The following figures shows an example of an optimized PROFINET topology.

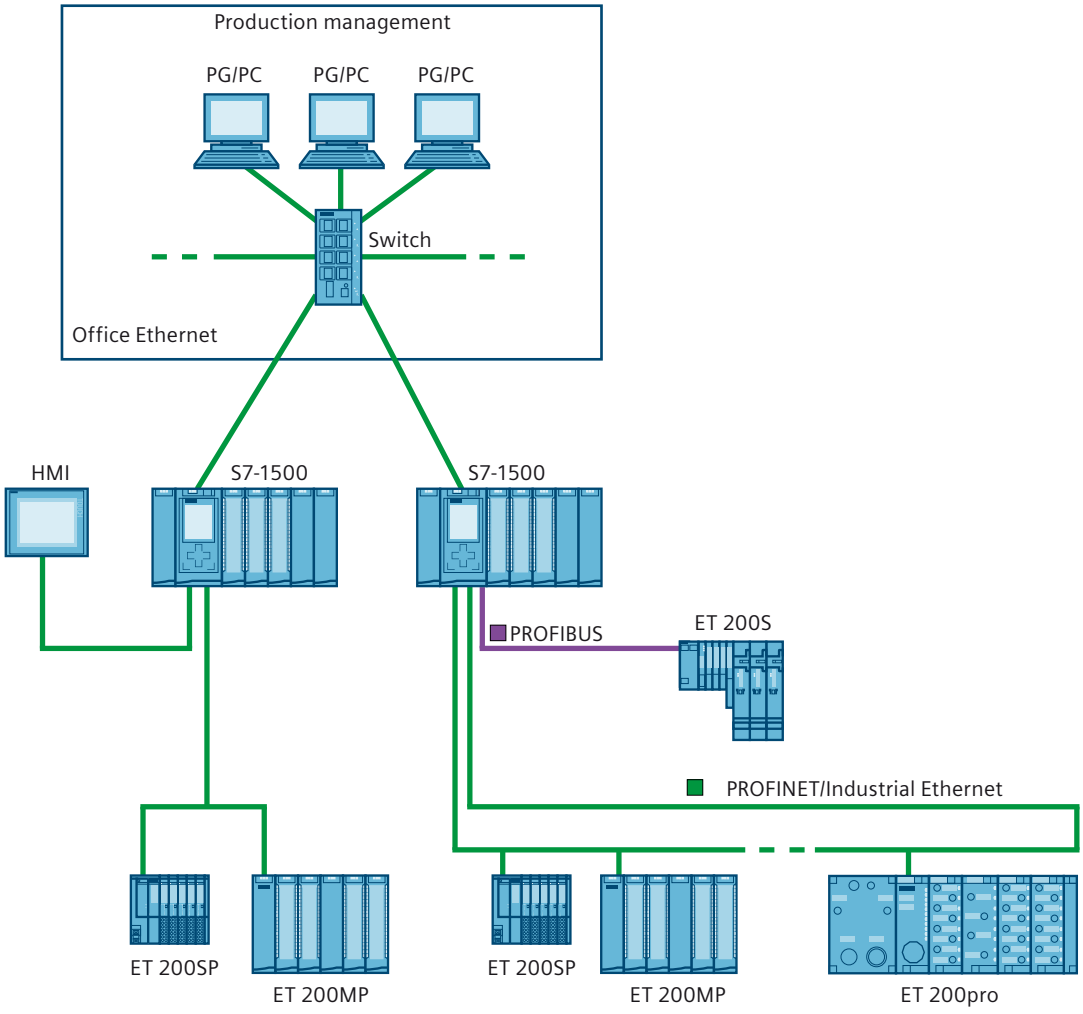


Figure 3-401 Optimized PROFINET topology

When setting up your PN network topology, take care that the various automation applications are distributed among separate network branches so that a sufficient bandwidth reserve will be available for future expansions.

- If you integrate standard Ethernet devices into the network topology or use standard Ethernet communication, take into account the network load caused by standard Ethernet and adapt the network topology as appropriate (max. bandwidth 100 Mbps).
- For communication with higher-level networks with a high data volume, use the most direct paths possible to the higher-level network infrastructure.

Also observe the Installation Guideline (http://www.profibus.com/nc/download/installation-guide/downloads/profinet-installation-guide/display/) of the PROFIBUS User Organization.

Setting up PROFINET with IRT

Keep in mind the following rules for setting up and operating a PROFINET IO system in IRT mode. These rules will ensure best possible operation of your PROFINET IO system.

- When using IRT, you must configure the topology. This will enable exact calculation of the update time, bandwidth, and other parameters.
- If you would like to use multiple sync domains, configure a sync boundary for the port which is currently connected to the PROFINET device of another sync domain.
- In a sync domain, you can only configure one sync master at a time.
- A PROFINET IO system may only be part of a single sync domain.
- If you configure PROFINET devices in a sync domain and want to synchronize with IRT, the PROFINET devices concerned must support IRT communication.
- If possible, use the same PROFINET device as the PROFINET IO controller and sync master.
- If only some of the PROFINET devices in a PROFINET IO system are synchronized, please keep in mind the following: Assign PROFINET devices that are not participating in the IRT communication to the RT class "RT" and the synchronization role "unsynchronized" in the sync domain.

Applications for CPU with multiple PROFINET IO interfaces

- Connecting machines: Your configuration contains machines located on separate IO lines. To operate the separate IO lines with real-time communication, select one of the following options:
  - Use an S7-1500 CPU that supports the same PROFINET functionalities at the PROFINET interface X2 as at the PROFINET interface X1. With these CPUs, you can operate a separate PROFINET IO system in isochronous mode at each of the PROFINET interfaces X1 and X2, or synchronize both PROFINET IO systems for a shared application. For information on how to operate the two PROFINET IO systems with each other in isochronous mode, refer to section Operating multiple PROFINET networks in isochronous mode (Page 232).
  - Alternatively, you can operate real-time communication between several CPUs via the PROFINET IO interface X2. Use the I-device or shared I-device function for this purpose. The figure below shows an example configuration for two machines connected over the X2 interface with an I-device relationship.

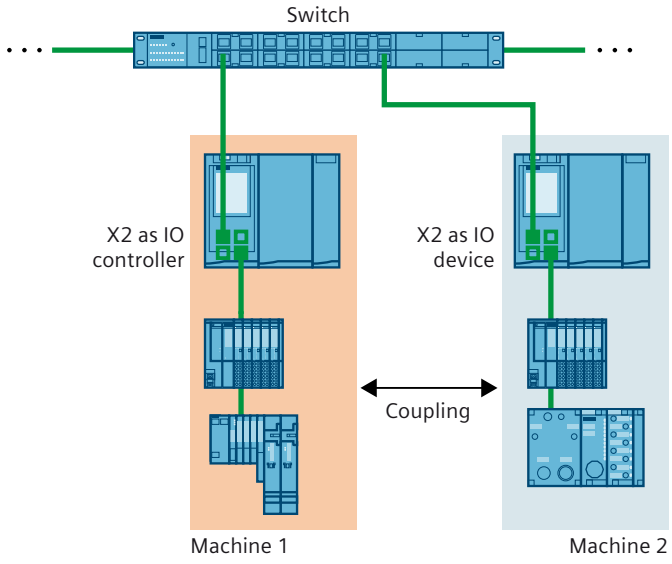


Figure 3-402 I-device connection over 2nd PNIO interface

- Distribution by automation tasks:
  - For automation tasks with high performance and deterministic requirements, use PROFINET with IRT over the X1 interface.
  - For other tasks that you can implement with RT, use the X2 interface.

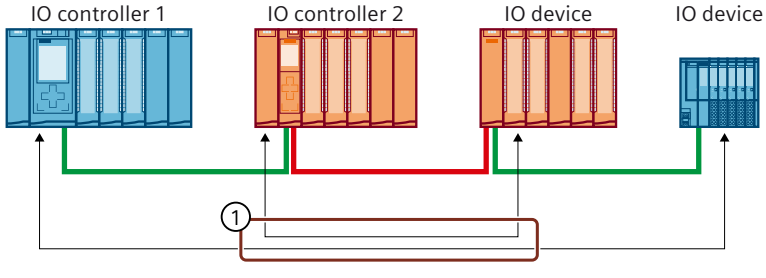
If you use interface X2 as the PROFINET IO interface for a CPU with FW version up to V2.9, this can affect performance. You can find additional information in the section PROFINET interface (Page 32) and in the Cycle and Response Times (https://support.industry.siemens.com/cs/ww/en/view/59193558) function manual.

Topological overlap of IO systems in multi-controller applications

In a configuration with multiple IO controllers, shared paths are subject to the combined network loads of all connected PROFINET IO systems.

To avoid high communication loads in multi-controller applications, observe the following recommendations:

- Avoid paths that are shared by multiple IO systems.
  The figure below shows a configuration with two PROFINET IO systems that use the same paths.



① Shared path

Figure 3-403 Multi-controller application with shared path

In the figure below, the two PROFINET IO systems do not use shared paths.

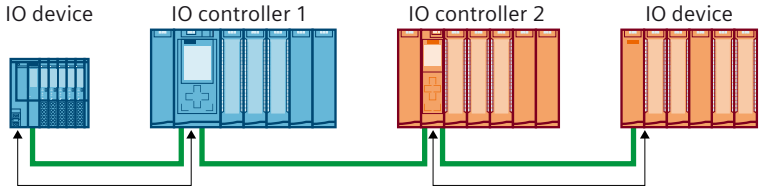


Figure 3-404 Multi-controller application with separate paths

- If separation is not possible: Increase the update time for the affected IO devices.

Installation guidelines of the PROFIBUS user organization

The installation guidelines can be found on the Internet (http://www.profibus.com/nc/download/installation-guide/downloads/profinet-installation-guide/display/).

7.5.8 Limitation of the data infeed into the network

Limiting the data infeed into the network on PROFINET interfaces

The "Limit data infeed into the network" function limits the network load of standard Ethernet communication which is fed into the network by the interface to a maximum value. This does not apply to cyclic real-time communication (RT/IRT).

In a PROFINET IO system, critical network loads can occur quickly with standard Ethernet communication, especially in line topologies. Devices which feed a lot of standard Ethernet communication into the PROFINET IO system, should support the function "Limit data infeed into the network". If necessary, you should optimize your topology by avoiding e.g. standard Ethernet devices in line topologies. You can find additional information on this in section Setup recommendations for optimizing PROFINET (Page 207).

Depending on the performance capability of the PROFINET interface, you can set in its properties whether or not the data infeed into the network should be limited. Requirements for adjustability:

- The interface offers sufficient performance.
- No IO data transfer is configured

If the conditions are not met, the data infeed is always limited.

Depending on the interface, you can activate or deactivate the "Limit data infeed into the network" function. If you use the X1 interface of an S7-1500 CPU as the IO controller or I-device, the "Limit data infeed into the network" function is always enabled. Example: If you are not using the X1 interface of an S7-1500 CPU as IO controller or I-device, you can enable or disable the function.

Uses of the limitation of the data infeed to the network

- Division of the bandwidth for standard Ethernet communication between devices:
  In PROFINET networks cyclic real-time communication and standard Ethernet communication share the same network. This means that only a limited bandwidth remains for standard Ethernet communication. The limitation of the data infeed ensures that the remaining bandwidth for standard Ethernet communication is not used just by one device, but is divided between several devices.
- Smoothing peaks in the data infeed:
  The limitation of the data infeed smooths peak loads of standard Ethernet communication (for example, from Open User Communication, access by the Web server).
- Prevent excessive data at the source:
  If applications in a device generate too much data, this data is not forwarded to the PROFINET network. Negative effects (for example data loss, communication interruption) remain limited to the device feeding in the data and its communications partner. Other nodes are not disturbed.

Setting limitation of the data infeed into the network for a CPU

To set the limitation of the data infeed into the network, follow these steps:

1. In the network view of STEP 7, select the interface of the CPU.
2. In the Inspector window, go to "Properties" > "General" > "Advanced options" > "Interface options".
3. Select or clear the "Limit data infeed into the network" check box.

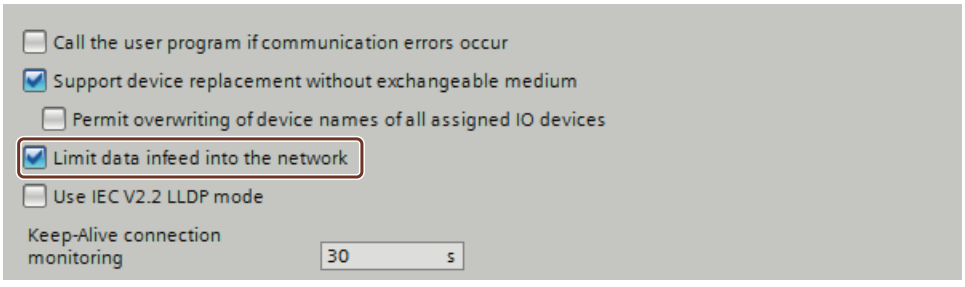


Figure 3-405 Limit data infeed into the network

7.6 PROFINET with performance upgrade

Performance upgrade

The performance upgrade implements the application class "High Performance" of the PROFINET specification V2.3.

The performance upgrade provides a series of measures that lead to the following improvements for PROFINET with IRT:

- Reduction of runtime delays in the IO devices
- Increase in the bandwidth for cyclic IO data
- Reduction of the bandwidth used for PROFINET frames
- Reduction of the send clocks

The improvements achieved with the performance upgrade mean that you can operate your PROFINET IO system with more devices with the same send clock or the same number of devices with a shorter send clock.

With PROFINET, it was previously possible to reach a send clock of 250 µs.

With the performance upgrade, it is now possible to achieve isochronous send clocks of up to 125 µs with the fast forwarding, dynamic frame packing and fragmentation procedures, depending on the performance capability of the CPU (see Technical Specifications in the device manuals). With short send clocks, standard communication remains possible.

The performance upgrade will help you to implement applications with high speed and send clock requirements.

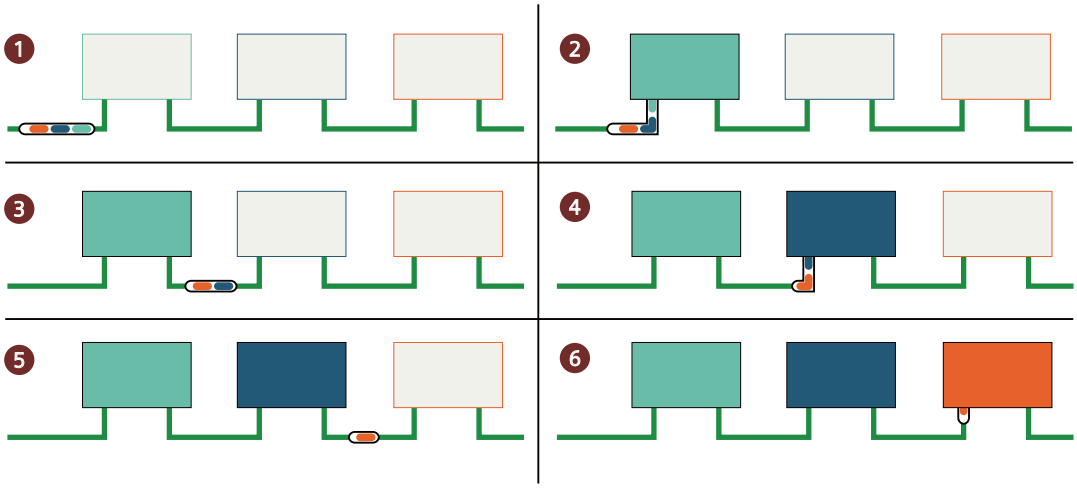
7.6.1 Dynamic frame packing

Dynamic frame packing

Previously, individual PROFINET IO frames were sent for every PROFINET IO device.

The performance upgrade uses the dynamic frame packing procedure that is based on the summation frame method. With the summation frame method, a frame contains the user data for neighboring devices on a line. With Dynamic Frame Packing, every IO device takes its data from the frame and forwards the rest. The frame is shortened from IO device to IO device. Dynamic frame packing improves the use of the bandwidth in a line topology.

The following figure shows how Dynamic Frame Packing works based on the example of a frame containing the user data for 3 IO devices.



① The PROFINET IO frame contains the user data for all 3 IO devices (green, blue and orange).
② The PROFINET IO frame reaches the first IO device. The IO device takes its user data (green) from the frame and forwards the remaining frame.
③ The PROFINET IO frame contains the user data for two IO devices (blue and orange).
④ The PROFINET IO frame reaches the second IO device. The IO device takes its user data (blue) from the frame and forwards the remaining frame.
⑤ The PROFINET IO frame contains the user data for one IO device (orange).
⑥ The PROFINET IO frame reaches the last IO device. The IO device saves the entire frame including user data (orange).

Figure 3-406 Dynamic Frame Packing (DFP)

DFP groups

Dynamic frame packing automatically groups IO devices that support the performance upgrade into DFP groups. To be grouped together in a DFP group. the IO devices (IRT devices) must be located one after the other in a line and must have the same update time and watchdog timer.

The following circumstances automatically lead to the creation of a new DFP group; the TIA Portal takes over the division into DFP groups:

- The maximum frame size (1440 bytes) for the DFP group has been exceeded.
- The maximum sub-frame size (256 bytes) for an IO device has been exceeded. This means that a large I/O quantity structure (> 256 bytes) of an IO device causes an interruption of the DFP group. The first DFP-capable IO device after this device opens a new DFP group.
- The maximum number of DFP capable IO devices (63) for a DFP group has been reached.
- DFP-capable IO devices are not in a line one behind the other but are interrupted by "normal" IRT devices (non-DFP-capable IO devices). The first DFP-capable IO device after a "normal" IRT device opens a new DFP group.

The maximum number of DFP groups per PROFINET interface is 8.

STEP 7 displays the DFP groups in "Domain management" > "Sync domains" > "Name of the sync domain" > "Device" in the "IO devices" box.

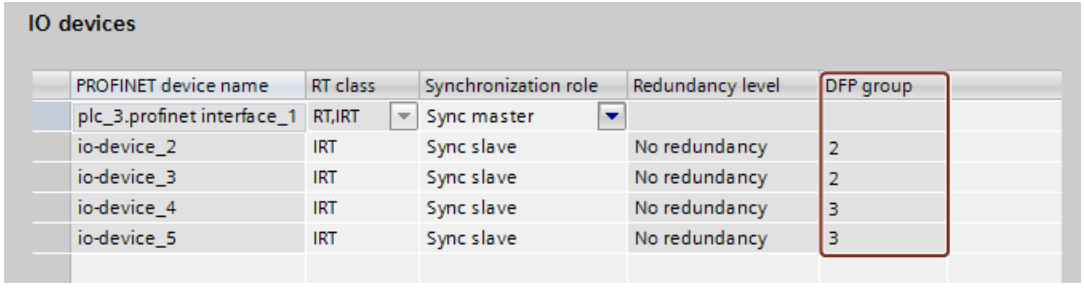


Figure 3-407 Display of the DFP groups in STEP 7

NOTE

Dynamic frame packing with high watchdog times

If you set the "Accepted update cycles without IO data" parameter higher than 31 for an IO device, Dynamic Frame Packing does not place this IO device in a DFP group.

Increase of the quantity structure for IRT devices by DFP

You can also use a line configuration with DFP-capable IO devices (DFP-capable IRT devices) to increase the number of connectable IRT devices.

Example from the technical specifications of a CPU 1517-3 PN (firmware version V4.0):

- Number of IO devices that can be connected to PROFINET interface X1 or X2 with IRT: 64; with DFP: 256 IO devices in (max.) 8 DFP groups

The following section explains how to interpret this technical specifications and which rules need to be considered. To assist you, the TIA Portal reports rule violations when compiling the PROFINET configuration.

Rules for the maximum line depth: To ensure synchronization accuracy, only 64 IRT devices may be arranged in a line – even if more than 64 IRT devices can be connected. With a

quantity structure of more than 64 IRT devices (with or without DFP), use IRT switches to comply with this rule.

Rules for the maximum number of communication relations: The number of communication relations to IRT devices and DFP groups is limited to 64.

The devices in a DFP group share a communication relationship, so when DFP-capable IRT devices are used, it is also possible to connect more than 64 IRT devices. A DFP group "uses up" an IRT communication relation just like a non-DFP-capable IRT device.

Example: **Valid configuration**

A configuration consists of 8 DFP groups with a total of 250 DFP-capable IRT devices. There are also 6 additional IRT devices (non-DFP-capable) between the DFP groups.

This ensures that the specified limits from the technical specifications are complied with:

- Number of IRT devices (DFP-capable or non-DFP-capable): 250 DFP-capable + 6 non-DFP-capable = 256 (which corresponds to the maximum number).
- Number of IRT devices (non-DFP-capable): 6 (which is below the limit of 64 IRT devices).
- Number of IRT communication relations: 8 DFP groups + 6 non-DFP-capable IRT devices = 14 (which is below the limit of 64 IRT communication relations).

If there are fewer DFP-capable IRT devices in the 8 groups and these devices are replaced by "normal" IRT devices (without DFP), the number of communication relations to IRT devices may be exceeded.

Example: **Invalid configuration**

The configuration consists of 8 DFP groups with a total of 195 DFP-capable IRT devices. There are also 61 additional IRT devices (non-DFP-capable) between the DFP groups.

- Number of IRT devices (DFP-capable or non-DFP-capable): 195 DFP-capable + 61 non-DFP-capable IRT devices = 256 (which corresponds to the maximum number).
- Number of IRT devices (non-DFP-capable): 61 (which is below the limit of 64 IRT devices).
- Number of IRT communication relations: 8 DFP groups + 61 non-DFP-capable IRT devices = 69 (which is above the limit of 64 IRT communication relations).

NOTE

Ensure sufficient program run time and reserves for other network loads.

When calculating the cycle time for isochronous applications, you must ensure that there is enough time available for other communication tasks and for processing data from the distributed I/O.

Use the "Details" area of the corresponding sync domain; here, the bandwidth for cyclic data is calculated and displayed from the PROFINET configuration.

You can access the "Details" area as follows: Properties of the PROFINET interface > Advanced options > Real time settings > Synchronization. In the "Synchronization" area, click on "Domain settings". Then navigate to the "Details" area under Domain Management > Sync domains > Sync domain_x.

The difference between "send clock" and "calculated bandwidth for cyclic data" is the maximum time available for the program to process the data. In addition, the update time for process image partitions reduces the program processing time (see the Function Manual Cycle and response times, section "Update time for process image partitions" – documented CPU-specific as copy time for distributed I/O via PROFINET).

To determine the program run time, use the "RUNTIME" instruction.

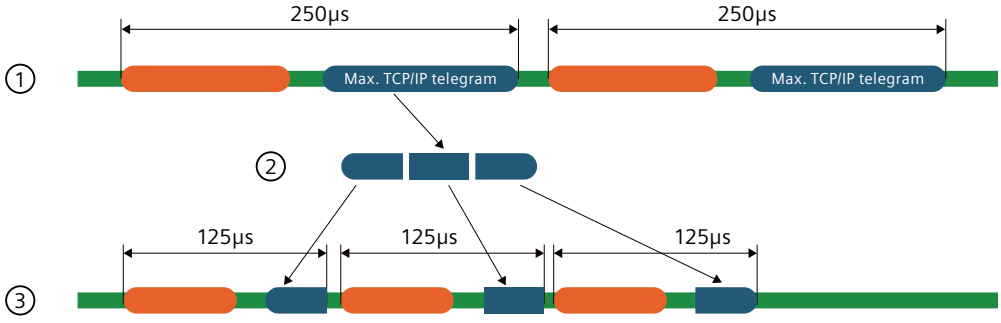
7.6.2 Fragmentation

The transfer of a complete standard Ethernet frame with TCP/IP data takes up to 125 µs. This means that the cycle time for PROFINET IO data cannot be reduced by any desired amount.

The performance upgrade uses the fragmentation procedure, which breaks down TCP/IP frames into sub-frames. These frame segments are transferred to the target device over multiple send clocks; there they are reassembled to the original TCP/IP frame.

Fragmentation is a requirement for cycle times lower than 250 µs. In these short send clocks, you can use more bandwidth for cyclic IO data, since the fragments of the standard Ethernet frames use significantly less bandwidth than a complete standard Ethernet frame.

For information on which send clocks a CPU supports, refer to the technical specifications in the Equipment Manual of the CPU. The following figure shows how fragmentation works at PROFINET interface X1 of a CPU 1518-4 PN/DP.



① A standard Ethernet frame with TCP/IP data is up to 125 µs.
② During fragmentation, the standard Ethernet frame is divided into frame segments.
③ The frame segments are divided into multiple short send clocks.

Figure 3-408 Fragmentation

NOTE
The PROFINET IO interface of the IO controller supports fragmentation if all the ports except one are deactivated.

Requirements for fragmentation

If you use the following combinations for send clock and bandwidth settings, the devices in the IO system use the fragmentation process.

- Send clock cycle 125 µs: Always fragmentation irrespective of the bandwidth setting.
- Send clock cycle 187.5 µs: Fragmentation with the bandwidth settings "Maximum 50% cyclic IO data. Balanced proportion." and "Maximum 90% cyclic IO data. Focus on cyclic IO data."

PROFINET interface X1 of the IO controller supports fragmentation as follows:

- CPUs up to FW version V3.1: Only one port may be active at PROFINET interface X1.
- CPUs as of FW version V4.0: Both ports may be active at PROFINET interface X1.

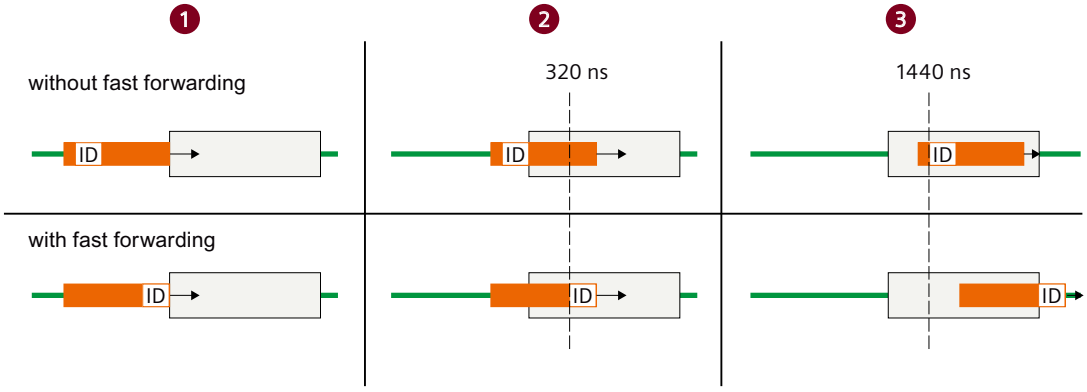
7.6.3 Fast forwarding

To be able to decide whether a frame should be forwarded or used, a PROFINET IO device requires the frame ID. It previously took 1440 ns until the frame ID was present in the IO device.

The performance upgrade uses the fast forwarding procedure in which the frame ID is located nearer the front of the frame. The throughput time in the device is reduced to 320 ns.

With fast forwarding, the throughput time of the frame is reduced in your PROFINET IO system. This results in decisive performance advantages, particularly in line, ring and tree topologies.

The figure below compares the throughput of a PROFINET IO frame in an IO device with and without fast forwarding.



① Start:
- Both PROFINET frames reach the IO device.
  The IO devices start to check the frames for the frame ID

② After 320 ns:
- Without fast forwarding: The IO device is still checking the PROFINET frame for the frame ID.
- With fast forwarding: The IO device receives the frame ID from the PROFINET frame and forwards the frame.

③ After 1440 ns:
- Without fast forwarding: The IO device receives the frame ID from the PROFINET frame and forwards the frame.
- The PROFINET frame with fast forwarding is "ahead" of the PROFINET frame without fast forwarding.

Figure 3-409 Fast forwarding

7.6.4 Configuration of IRT with high performance

High-end applications with IO communication require excellent performance in IO processing, for example in the control of wind turbines (converter control).

To use IRT communication with the highest performance in your PROFINET IO system, enable the option "Make 'high performance' possible".

When you enable the "Make 'high performance' possible" option, this has the following effects:

- You can set send clocks of 187.5 µs and 125 µs (for example CPU 1518-4 PN/DP) or 187.5 µs (for example CPU 1517-3 PN/DP), see Technical specifications in the CPU device manuals.
- You can set more bandwidth use for cyclic IO data.
- You can use the option "Allows the use of 'fast forwarding'".

Requirements

- S7-1500 CPU as of firmware version V2.0

Enable the "Make 'high performance' possible" option.

Follow these steps to activate the "Make 'high performance' possible" option:

1. Select the PROFINET IO system in the network view of STEP 7.
2. In the Inspector window, go to "Properties" > "General" > "PROFINET" > "Domain management" > "Sync domains" > "Name of the sync domain".
3. Enable the "Make 'high performance' possible" option.

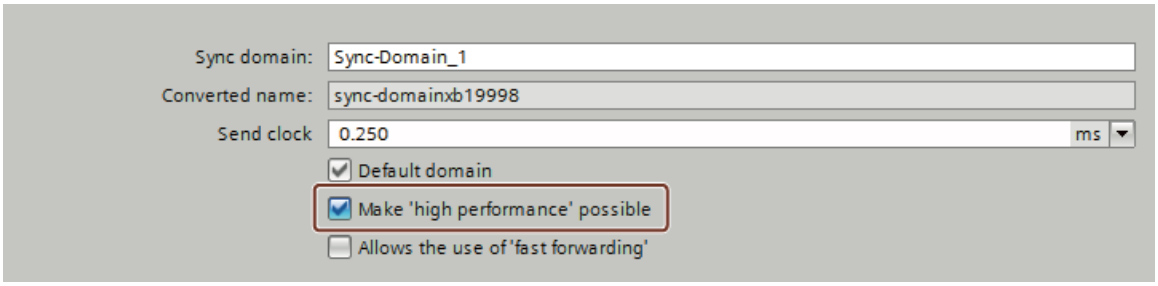


Figure 3-410 Activating high performance

Using more bandwidth for cyclic IO data

Requirement: The "Make 'high performance' possible" option is enabled.

To set more bandwidth for cyclic IO data for your PROFINET IO system, follow these steps:

1. Select your IO system in the network view of STEP 7.
2. In the Inspector window, go to "Properties" > "General" > "PROFINET" > "Domain management" > "Sync domains" > "Name of the sync domain" > "Details".

3. In the drop-down list, select "Maximum 90% cyclic IO data. Focus on cyclic IO data".

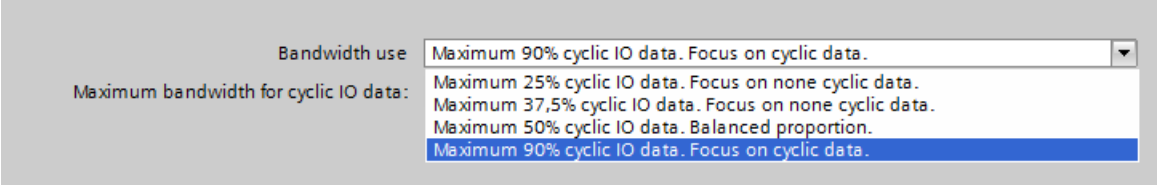


Figure 3-411 Using more bandwidth for cyclic IO data

NOTE

Bandwidth usage in isochronous mode

If you operate your PROFINET IO system in isochronous mode, avoid using the setting for the bandwidth usage "Maximum 90% cyclic IO data. Focus on cyclic IO data."

Setting low send clocks (example CPU 1518-4 PN/DP)

Requirement: The "Make 'high performance' possible" option is enabled.

1. Select the PROFINET IO system in the network view of STEP 7.
2. In the Inspector window, go to "Properties" > "General" > "PROFINET" > "Domain management" > "Sync domains" > "Name of the sync domain".
3. Select the send clock for "Send clock" in the drop-down list.

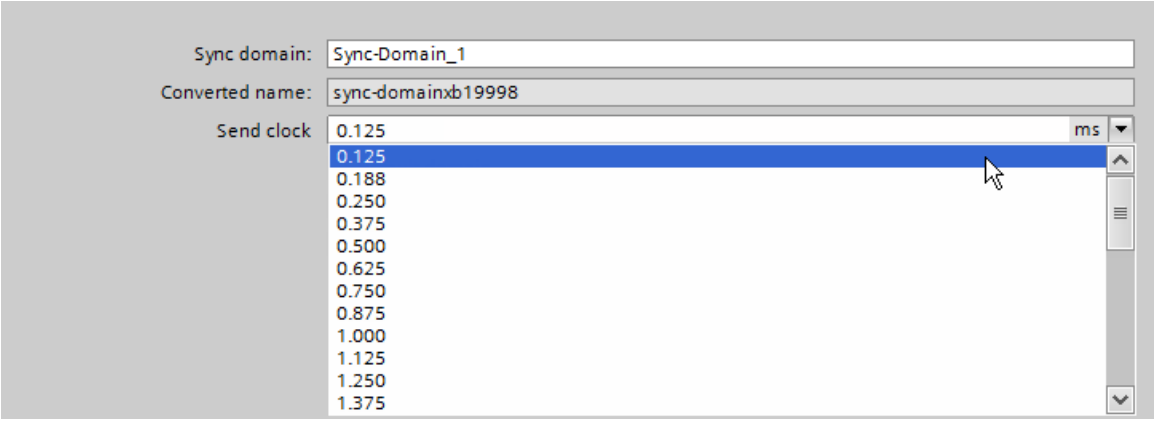


Figure 3-412 Setting low send clocks

Optimizing port settings for low send clocks

You can further optimize the bandwidth use in your PROFINET IO system by using cables with a short cable length (< 20 m) or a short signal delay (max. 0.12 µs) between the devices.

To configure cables with a shorter length or signal delay in STEP 7, follow these steps:

1. Select the port in the topology view of STEP 7.
2. Navigate in the Inspector window to "Port interconnection" in the "Partner port" box.
3. Select the option "Cable length" or "Signal delay:".

4. Select the cable length or enter the signal delay.

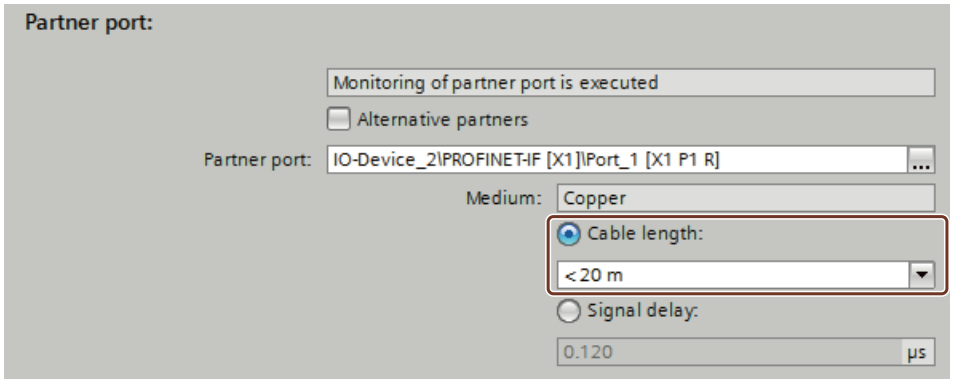


Figure 3-413 Optimizing port settings for low send clocks

Allowing fast forwarding

Requirements:

- The PROFINET IO device has to support the fast forwarding process so that the process can be used by the device.
- The "Make 'high performance' possible" option is enabled.
- The PROFINET IO interface supports fast forwarding if all the ports except one are deactivated.

Follow these steps to allow fast forwarding:

1. Select the PROFINET IO system in the network view of STEP 7.
2. In the Inspector window, go to "Properties" > "General" > "PROFINET" > "Domain management" > "Sync domains" > "Name of the sync domain".
3. Enable the "Allows the use of 'fast forwarding'" option.

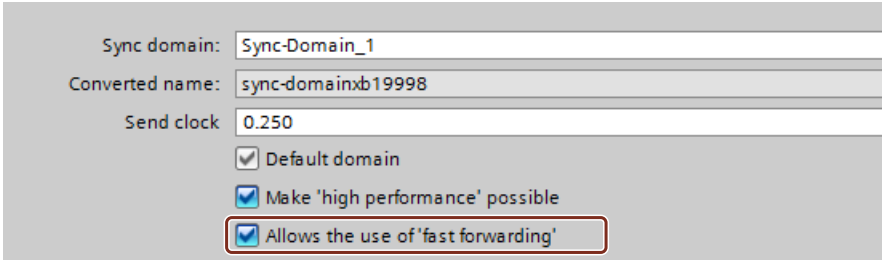


Figure 3-414 Allowing fast forwarding

NOTE

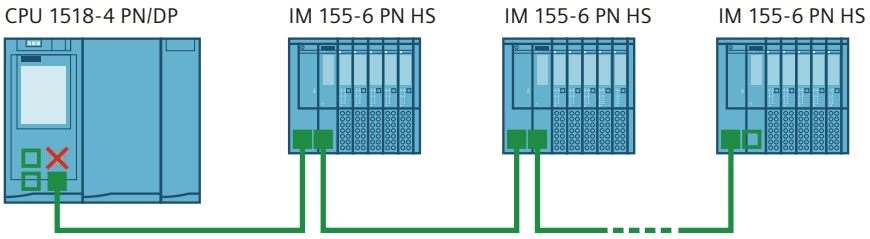
Fast forwarding and IPv6

The operation of fast forwarding in combination with IPv6 is not supported.

As soon as an IO device in the subnet uses an IPv6 address, you must not activate "fast forwarding".

7.6.5 Sample configuration for IRT with high performance

The figure below shows an example configuration with which you can achieve maximum performance.



Port 1 of the X1 interface of the CPU is deactivated.

Port 2 of the X1 interface and the ports of the interface modules on the bus use the following setting: Medium copper, cable length < 20 m or signal delay max. 0.12µs

A programming device connection to the CPU can be established via the interfaces X2 and X3 of the CPU or via the free port at the end of the line.

Figure 3-415 Example configuration for IRT with high performance

Use the following settings for the Sync domain:

- Enable the "Make 'high performance' possible" option.
- Set the send clock to 125 µs.
- Enable the "Allows the use of 'fast forwarding'" option.

Standard Ethernet communication for IRT with high performance

Standard Ethernet communication is still possible even in a PROFINET IO system with high performance. Keep in mind that you first arrange the IRT nodes, as seen from the IO controller, and arrange the standard Ethernet nodes at the end of the line.

With a large volume of data through standard Ethernet communication, it makes sense to reduce the load on your network by separating standard Ethernet communication and cyclic real-time communication. Example: Use the interface X1 for the PROFINET IO communication and a different interface for the standard Ethernet communication.

7.7 Isochronous mode

7.7.1 What is isochronous mode?

Objectives of isochronous operation

PROFINET isochronous mode only works when using PROFINET with IRT.

Data transfer in automation technology is comparable with the transportation of people on public transport. The various road users, such as cars, trucks or buses, use the same traffic routes. This causes delays or bottlenecks when there is an increased volume of traffic. As a result, passengers (PN IOframes) arrive too late at the transfer point and miss their connecting bus (next cycle).

To maintain the specified schedule and reach the stops on their route unhindered, buses need their own lane (PROFINET with IRT) on the road. This lane is reserved exclusively for buses. When the bus schedule (bus clock cycle) is synchronized with the traffic lights (IRT

switch) and additional bus lines (star topology), passengers will specifically transfer to their connecting bus. This achieves optimum time and response behavior.

Just-In-Time

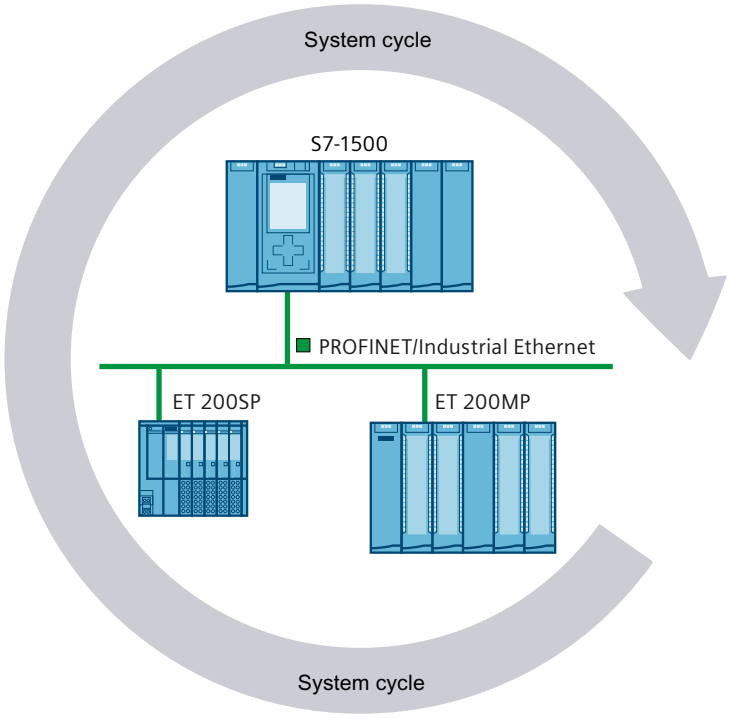


Figure 3-416 System cycle

The fast and reliable response time of a system operating in isochronous mode is due to the fact that all data is provided just-in-time. The basis for this is an equidistant cycle.

The isochronous mode function guarantees synchronization of the following at constant time intervals:

- Signal acquisition and output by the distributed I/O
- Signal transmission via PROFINET IO
- Program execution in the CPU in time with the equidistant PROFINET IO

The result is a system that acquires its input signals, processes them and outputs the output signals at constant time intervals. Isochronous mode guarantees precisely reproducible and defined process response times as well as equidistant and synchronous signal processing for distributed I/O.

Advantages of isochronous mode

The use of isochronous mode allows high-precision control.

- Optimized control loops through constant, calculable dead times
- Determinism, reliable reproducibility of response times
- Consistent (simultaneous) reading in of input data
- Consistent (simultaneous) output of output data

7.7.2 Use of isochronous mode

An isochronous system acquires measured values and process data within a fixed system cycle, processes the signals and outputs them synchronously to the process. Isochronous mode contributes to a high control quality and increased production accuracy. With isochronous mode, the possible fluctuations of process response times are drastically reduced. You make use of the time-assured processing to improve machine cycle times. Even fast processes can be reliably controlled thanks to the precise time reproducibility of all sequences. Shorter cycle times increase the processing speed and help to lower production costs.

In principle, isochronous mode is worthwhile whenever measured values must be acquired synchronously, movements must be coordinated, and process responses must be defined and simultaneously executed, as in the following example. Isochronous mode can thus be used in a wide variety of applications.

Example: Measuring at multiple measurement points with isochronous mode

Automation task
A camshaft production process requires precise measurement of the camshafts for quality assurance purposes.

Feature
For this purpose, a component is needed that can synchronously measure the positions and displacements of the cam during a rotation of the camshaft.

Solution

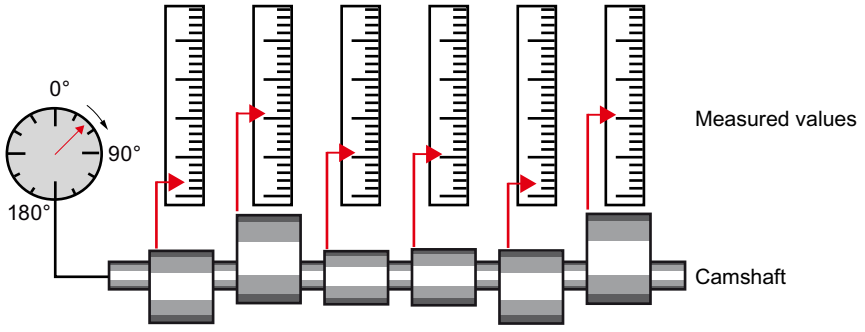


Figure 3-417 Measuring of camshafts

With use of isochronous mode, the measured values are simultaneously acquired at the various measuring points at fixed times. This results in the following workflow:

- Continuously rotate the camshaft
- During continuous rotation, synchronously measure the positions and cam displacements
- Process the next cam shaft

Thus, during a single rotation of the camshaft, all the positions of the camshaft and the associated measured values (red) are measured synchronously. The machine cycle time improves with the same or better measuring accuracy.

Advantage and benefits
The time required for measurement is reduced.

7.7.3 Time sequence of synchronization on PROFINET IO

Introduction

On PROFINET IO, you can isochronously operate I/O modules in distributed I/O systems on a CPU, e.g. in distributed I/O systems ET 200SP, ET 200MP.

Like the I/O modules, the interface modules of the I/O systems must support isochronous mode.

From reading in input data to outputting output data

The basic time sequence of all components involved in synchronization is explained below:

① Measured value acquisition in the process

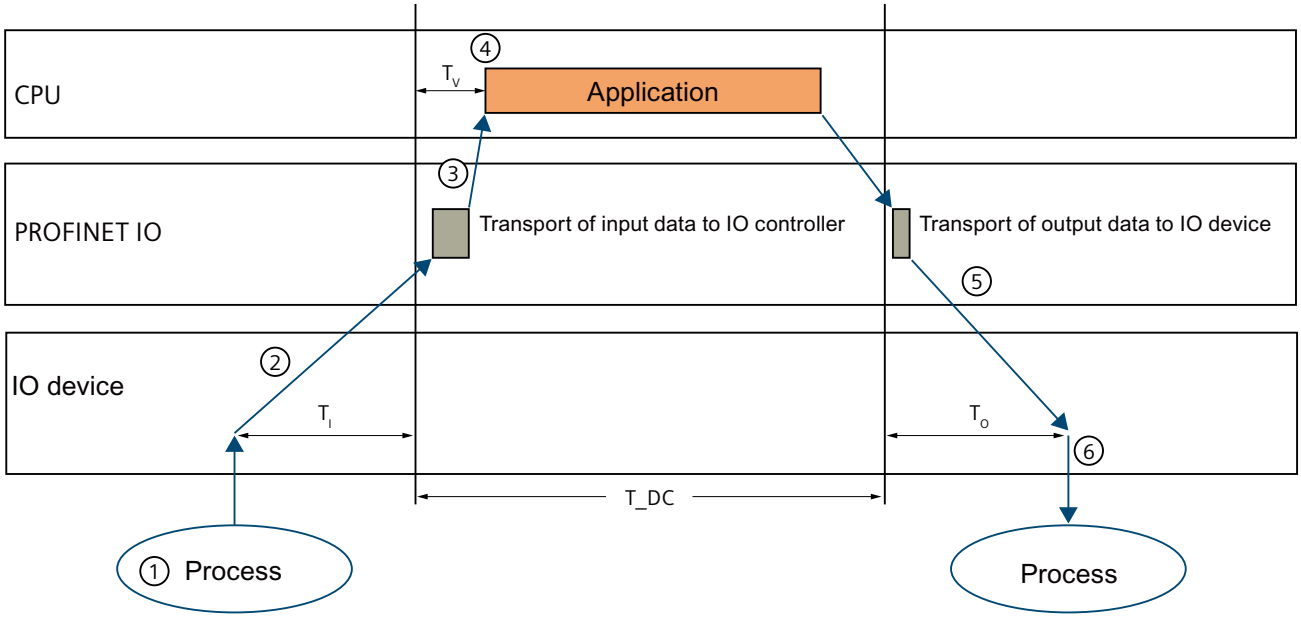
② Isochronous read-in of input data

③ Transport of input data to the IO controller (CPU) via the subnet

④ Further processing in the isochronous application of the CPU

⑤ Transport of output data to the outputting IO device via the subnet

⑥ Isochronous output of output data



T_DC	Data cycle (Time_DataCycle)
T_I	Time for reading in the input data
T_O	Time for outputting the output data
T_V	Configured delay time

Figure 3-418 Time sequence of synchronization on PROFINET IO

To ensure that all input data is ready for transport via the subnet at the next start of the PROFINET IO cycle, the start of the I/O read-in cycle is advanced by the amount of lead time T_I. T_I is the "flashbulb" for the inputs; at this instant, all synchronized inputs are read in. T_I is necessary in order to compensate for analog-to-digital conversion, backplane bus times, and the like. The lead time T_I can be configured by STEP 7 or by you. Let the lead time T_I be

assigned automatically by STEP 7. With the default setting, STEP 7 ensures that a common, minimum T_I is set.

The subnet transports the input data to the IO controller/DP master. The application is started synchronized to the cycle. That is, the isochronous mode interrupt OB is called after a configurable delay time T_V. The user program in the isochronous mode interrupt OB defines the process response and provides the output data in time for the start of the next data cycle. The length of the data cycle (send clock/DP cycle time) is always configured by you.

T_O is the time for the compensation arising from the backplane bus and the digital-to-analog conversion within the IO device/DP slave. T_O is the "flashbulb" for the outputs. The synchronized outputs are output at this time. Time T_O can be configured by STEP 7 or by you. Let time T_O be assigned automatically by STEP 7. STEP 7 automatically calculates a common, minimum T_O.

7.7.4 Configuring isochronous mode

7.7.4.1 Introduction

Configuring at a glance

Setting parameters for isochronous operation of the I/O module
You use the properties of the I/O addresses of the corresponding I/O module to:

- Set isochronous mode for the module.
- Assign the inputs and outputs of the module to a process image partition and an isochronous mode interrupt OB.

  The data of the process image partition is updated synchronously to the assigned OB. Isochronous mode interrupts give you the option of starting programs isochronously with the PROFINET send clock. Isochronous mode interrupts are processed with high priority.

Setting the send clock
The send clock is the shortest possible transmission interval for the data exchange. In isochronous mode, the send clock corresponds to data cycle T_DC.

You set the send clock in the properties of the PROFINET interface of the CPU or in the sync domain.

Setting the application cycle
The application cycle is a multiple of data cycle T_DC. If the runtime of the isochronous mode interrupt OB is short, the application cycle can be identical to the data cycle (= send clock).

You can reduce the application cycle of the isochronous mode interrupt OB relative to the send clock of an isochronous PROFINET IO system. Set an integer multiple of the send clock as the reducing factor.

You use the factor to reduce the CPU utilization by executing the isochronous mode interrupt OB less frequently. You set the application cycle in the properties of the isochronous mode interrupt OB.

Setting the delay time
The delay time is the time between the start of the send clock and the start of the isochronous mode interrupt OB. During this time, the IO controller performs cyclic data exchange with the IO devices.

STEP 7 sets the default delay time in such a way that the isochronous update of the process image partition automatically falls within the execution window of the application cycle.

You set the delay time in the properties of the isochronous mode interrupt OB. A shorter delay time enables you to increase the processing time for your user program in the isochronous mode interrupt OB.

Additional configurations for isochronous mode on PROFINET IO:

- **Setting IRT as the RT class for the interconnected PROFINET interfaces**

  A precondition for isochronous operation on PROFINET IO is IRT communication (Isochronous Real Time Communication). IRT means synchronized data exchange at reserved time intervals.
- **Configuring the topology of the configuration**

  A precondition for IRT communication is the topology configuration. In addition to the reserved bandwidth, the exchange of frames on defined transmission paths is used for further optimization of data communication. For this, the topological information of the configuration is used for planning the communication.
- **Using a sync domain**, you assign the IO devices (sync slaves) to an IO controller (sync master) for the isochronous data exchange.

  A precondition for IRT communication is a synchronization cycle for all PROFINET devices in a sync domain, for distribution of a common time base. With this basic synchronization, synchronous operation of the transmission cycle of the PROFINET devices within a sync domain is achieved.

7.7.4.2 Configuring isochronous mode on PROFINET IO

Introduction

The configuring of isochronous mode for a module is described as IO device in the following based on the ET 200MP distributed I/O system. The procedure described also applies to other distributed I/O systems (e.g., ET 200S or ET 200SP).

The IO controller is an S7-1500 CPU.

Requirements

- The STEP 7 network view is open.
- A S7-1500 CPU has been placed (e.g., CPU 1516-3 PN/DP).
- An IM 155-5 PN HF interface module (ET 200MP) has been placed and networked with the CPU via PROFINET IO.
- All requirements for an IRT configuration are met:
  - The ports of the networked PROFINET interfaces of the CPU and interface module are interconnected (topology configuration).
  - The RT class of the PROFINET interface of the interface module is set to "IRT" (area "Advanced options > Real time settings > Synchronization").
  - The "sync master" and "sync slave" roles are assigned for the PROFINET interfaces of the CPU and interface module (in the properties of a PROFINET interface: "Advanced options > Real time settings > Synchronization > Domain settings" area).

Procedure

To create an isochronous connection between the I/O and user program, follow these steps:

1. Select the IM 155-5 PN HF in the network view of STEP 7. Change to the device view.
2. Insert an I/O module that can be operated isochronously (e.g. DI 16 x 24VDC HF).
3. Go to the "I/O addresses" area in the Inspector window of the selected I/O module.

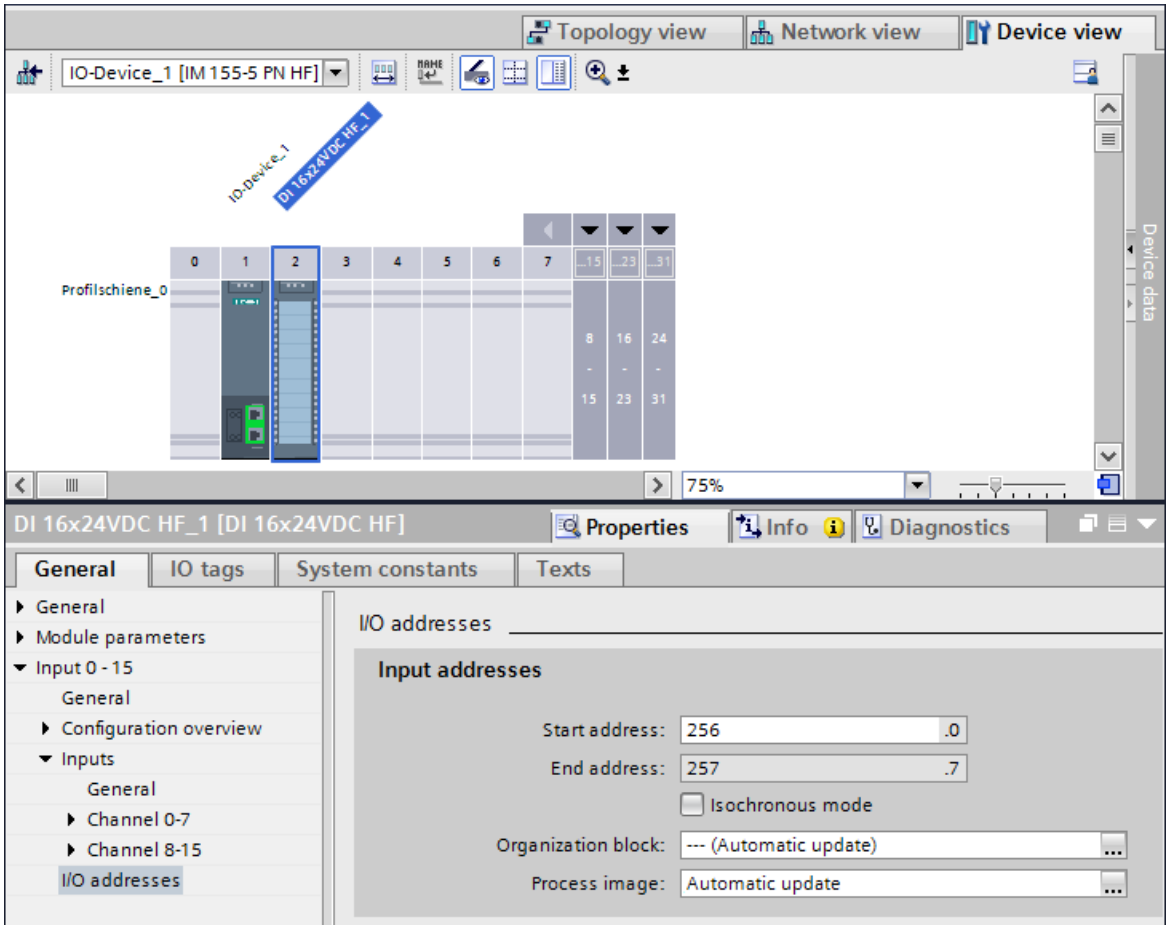


Figure 3-419 Configuring isochronous mode on PROFINET IO

4. Make the following settings in the I/O addresses area:
   - Select the "Isochronous mode" option.
   - Select a process image partition, e.g., process image partition 1.
   - Click the "Organization block" drop-down list. Click the "Add" button or select an existing OB. A dialog box for selecting organization blocks opens.
   - Select the "Synchronous Cycle" OB. Confirm the selection with "OK".

     In the case of automatic number assignment, OB 61 will be generated and opened.

     In the Inspector window, you can continue directly with the setting of the application cycle and delay time (Page 227) in the "Isochronous mode" area and start the programming of the OB in the instruction section.

5. If required, insert additional IO devices in the network view. Adapt the configuration and the settings for the isochronous mode.
6. You want to retrieve information about calculated bandwidths or on adapting the send clock. Select the sync domain in the network view and navigate to the corresponding area of the domain management in the Inspector window.

Reference

You can find examples of parameter assignment and possible settings of isochronous mode for distributed I/O and drives in STEP 7 in this FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109480489).

7.7.4.3 Setting the application cycle and delay time

Requirements

- You have created an isochronous mode configuration in STEP 7.
- You have created an isochronous mode interrupt OB Synchronous Cycle (OB 6x).
- The isochronous mode interrupt OB is open.

Setting the application cycle

The application cycle is a multiple of data cycle T_DC (send clock). You use the application cycle setting to reduce the CPU utilization caused by execution of the isochronous mode interrupt OB. In the following example, the OB is called only after every 2nd data cycle T_DC in the CPU.

To set the application cycle for your isochronous mode application, follow these steps:

1. Open the "Properties" dialog of the isochronous mode interrupt OB under consideration.
2. In the area navigation, click the "Isochronous mode" group .
3. Set the application cycle in "Application cycle (ms)". Open the drop-down list box and select the application cycle. The drop-down list offers multiples of data cycle T_DC as possible values for the application cycle. Data cycle T_DC is set to 2 ms in the following figure.

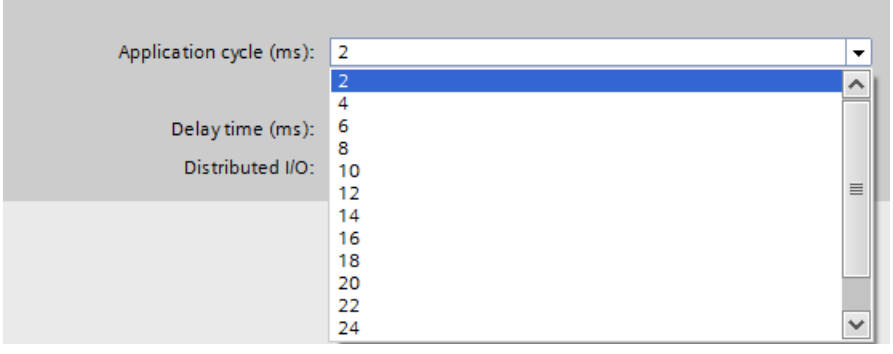


Figure 3-420 Setting the application cycle

Setting the delay time

The delay time is the time between the start of the send clock and the start of the isochronous mode interrupt OB. STEP 7 sets the delay time automatically to the start of the execution window by default. As a result, the isochronous mode update of the process image partition automatically falls within the execution window of the application cycle.

You can also set the delay time manually. A shorter delay time enables you to increase the processing time for your user program in the isochronous mode interrupt OB. If a manual setting is made, note that you must call the "SYNC_PI" and "SYNC_PO" instructions in the execution window of the application cycle.

To set the delay time for your isochronous mode application, follow these steps:

1. Open the "Properties" dialog of the isochronous mode interrupt OB under consideration.
2. In the area navigation, click the "Isochronous mode" group .
3. Clear the "Automatic setting" check box.
4. Enter your desired delay time in "Delay time (ms)".

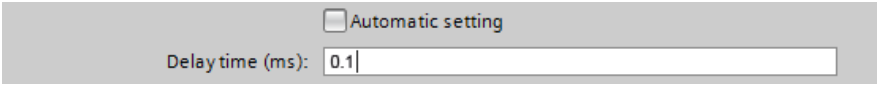


Figure 3-421 Setting the delay time

7.7.5 Programming isochronous mode

7.7.5.1 Basics of Programming

Programming in the isochronous mode interrupt OBs

You program the isochronous section of the program exclusively in the isochronous mode interrupt OBs Synchronous Cycle (OB 6x).

Because the isochronous mode interrupts are processed with high priority, only the time-critical sections of the program should be processed in the isochronous mode interrupt OB. The isochronous mode interrupt OB is called with a configured delay time.

Access to isochronous I/O through call of instructions

You access the isochronous I/O via a process image partition. That is, the addresses of the isochronous modules must be within one process image partition.

You program access to the isochronous IO in isochronous mode interrupt OB Synchronous Cycle (OB 6x) with the SYNC_PI and SYNC_PO instructions.

The isochronous I/O is updated by the call of the "SYNC_PI" and "SYNC_PO" instructions and therefore in the corresponding process image partition.

NOTE

Recommendation: To prevent inconsistent data from being returned to OB 6x, do not use the "DPRD_DAT" and "DPWR_DAT" instructions (direct data access) in the isochronous mode interrupt OB.

The "SYNC_PI" and "SYNC_PO" instructions update the process image partition only within the permitted execution window. The execution window stretches from the end of the cyclic data exchange to the point in time before the end of T_DC at which the outputs can still be copied in time. The data exchange must be started within this time window. If the execution window is violated by the processing of the "SYNC_PI" and "SYNC_PO" instructions, the instructions indicate a corresponding error message.

Program execution models

Depending on the order of the "SYNC_PI" and "SYNC_PO" instruction calls in OB 6x, there are two basic models for the program execution:

- **IPO** model (read **I**nputs - **P**rocessing - write **O**utputs)
- **OIP** model (write **O**utputs - read **I**nputs - **P**rocessing)

7.7.5.2 Program execution according to the IPO model

If the execution time of the isochronous mode interrupt OB is significantly shorter than one data cycle T_DC, use the IPO model. In the IPO model, you do not reduce the data cycle. That is, the application cycle of the isochronous mode interrupt OB is equal to data cycle T_DC.

The IPO model enables the shortest response times.

Programming according to the IPO model in the isochronous mode interrupt OB

For programming according to the IPO model:

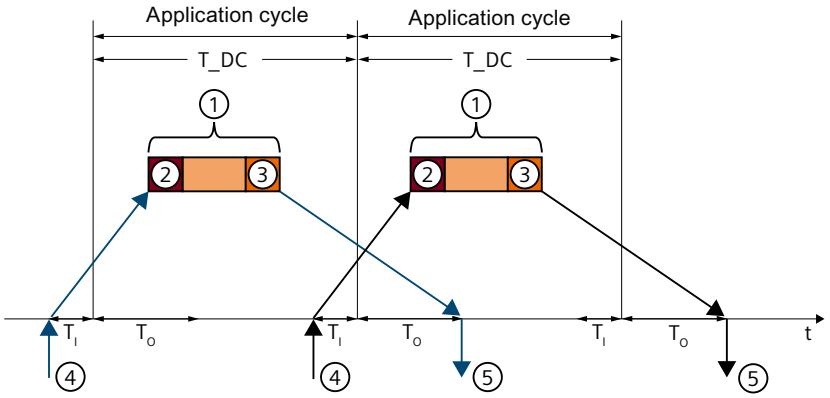
1. Call the SYNC_PI instruction at the start of the isochronous mode interrupt OB.
2. Then call the actual user program.
3. Call the SYNC_PO instruction at the end of the isochronous mode interrupt OB.

Table 3-47 Programming according to the IPO model

Step	Action	Explanation
1	Read in (I)	The SYNC_PI instruction reads in the inputs of the process image partition and provides them to the isochronous mode interrupt OB.
2	Process (P)	You program the actual user program of the isochronous mode interrupt OB.
3	Output (O)	The SYNC_PO instruction outputs the data changed by the user program via the process image partition.

Signal sequence in the IPO model

The following figure shows the signal sequence in the IPO model from the acquisition and the processing in the CPU to the output of the process values:



① Execution of isochronous mode interrupt OB
② "SYNC_PI" instruction
③ "SYNC_PO" instruction
④ Isochronous read-in of process values on I/O module at time T_I
⑤ Isochronous output of process values on I/O module at time T_O

Figure 3-422 Signal sequence in the IPO model

At time T_I the process values are read in isochronously on the I/O. The processing of the data in the IPO model is completed within one data cycle T_DC. The output data is always available on the I/O in the next data cycle T_DC at time T_O.

With the IPO model, there is a constant execution time from the "input terminal" to the "output terminal" of $T_I + T_DC + T_O$.

$T_I + 2 \times T_DC + T_O$ can be guaranteed for the process response time.

7.7.5.3 Program execution according to the OIP model

Use the OIP model in the case of execution cycles of the isochronous mode interrupt OB of different lengths, if the application cycle is greater than data cycle T_DC.

The data exchange with the process is always deterministic in the OIP model, i.e. takes place at a precisely specified time.

Programming according to the OIP model in the isochronous mode interrupt OB

For programming according to the OIP model:

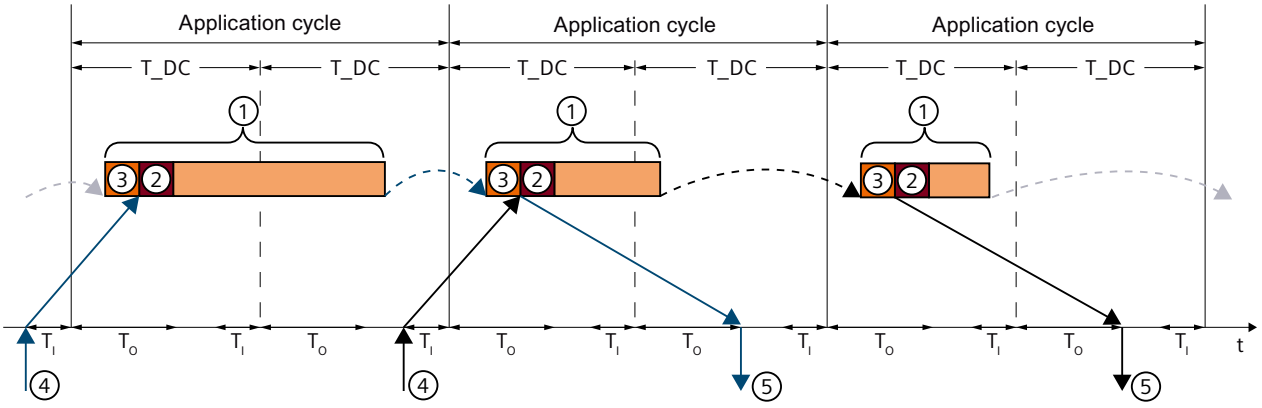
1. Call the SYNC_PO instruction at the start of the isochronous mode interrupt OB.
2. Then call the SYNC_PI instruction.
3. Then call the actual user program.

Table 3-48 Programming according to the OIP model

Step	Action	Explanation
1	Output (O)	The SYNC_PO instruction outputs the data that was changed by the user program in the previous cycle via the outputs of the process image partition.
2	Read in (I)	The SYNC_PI instruction reads in the inputs of the process image partition of the current cycle and provides the inputs to the isochronous mode interrupt OB.
3	Process (P)	You program the actual user program of the isochronous mode interrupt OB.

Signal sequence in the OIP model

The following figure shows the signal sequence in the OIP model from the acquisition of process values and the processing in the CPU to the output of the process values. The application cycle is twice as long as data cycle T_DC in this example.



① Execution of isochronous mode interrupt OB
② "SYNC_PI" instruction
③ "SYNC_PO" instruction
④ Isochronous read-in of process values on I/O module at time T_I
⑤ Isochronous output of process values on I/O module at time T_O

Figure 3-423 Signal sequence in the OIP model

At time T_I the process values are read in isochronously on the I/O. The data is processed over 2 application cycles in the OIP model. The output data is always available on the I/O in the following application cycle at time T_DC + T_O.

With the IPO model, there is a constant execution time from the "input terminal" to the "output terminal" of T_I + application cycle + T_DC + T_O.

T_I + 2 x application cycle + T_DC + T_O can be ensured as the process response time.

7.7.6 Operating multiple PROFINET networks in isochronous mode

7.7.6.1 Useful information on the operation of several PROFINET networks in isochronous mode

Introduction

If several PROFINET interfaces of a S7-1500 CPU support the functionality "PROFINET with IRT", you can operate a separate PROFINET network in IRT mode at these PROFINET interfaces. Each PROFINET network has its own sync domain, for which a separate sync master must be configured. You determine the synchronization roles of the devices and the send clock in the sync domain settings of the PROFINET networks. You can use the following PROFINET interfaces, for example, as the sync master:

- Integrated PROFINET interface, e.g. X1 of the CPU
- PROFINET interface, e.g. X1 of another CPU in the same PROFINET IO system

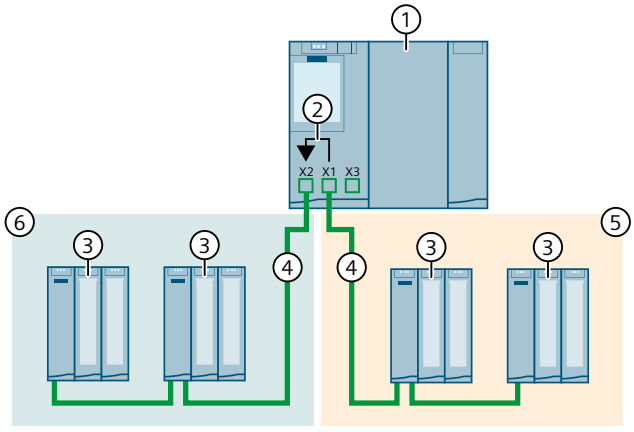
Another CPU within the same PROFINET IO system is also considered to be an I-device that has been directly inserted into the project from the hardware catalog in STEP 7 or as a GSD file.

You can operate the various PROFINET networks for isochronous applications using the following options:

- Independently of each other with separate send clock.
- Coupled/synchronized with synchronized send clock for all PROFINET IO systems

The figure below shows a CPU 1517-3 PN with connected PROFINET networks at the PROFINET interfaces X1 and X2. The PROFINET interfaces X1 and X2 of the CPU are configured as sync master for their sync domains.

The PROFINET interface X2 is coupled or synchronized with the set send clock of the PROFINET interface X1.



① CPU 1517-3 PN
② Coupling/synchronizing the send clock of the PROFINET interface X1
③ IO device, e.g. ET 200MP
④ PROFINET network at PROFINET interface X1 or X2
⑤ Sync domain of the PROFINET network at PROFINET interface X1
⑥ Sync domain of the PROFINET network at PROFINET interface X2

Coupled operation

In coupled operation, you use 2 PROFINET networks for a shared application. One PROFINET network is connected to the PROFINET interface X1 and the other PROFINET network to the PROFINET interface X2 of the CPU. The two PROFINET interfaces X1 and X2 take on the synchronization role sync master for their sync domain.

In coupled operation, one sync master synchronizes the send clock for its sync domain in a 1:1 ratio, based on the send clock of the other sync master. The 1:1 ratio is set by default as soon as 2 PROFINET networks are operated in isochronous mode.

As the PROFINET networks operate with a coupled send clock, the shared application requires only one isochronous mode interrupt OB (OB 61).

Synchronized operation

In synchronized operation, you use the two PROFINET networks for different applications. Also in this case, the two PROFINET interfaces X1 and X2 take on the synchronization role sync master for their sync domain.

In synchronized operation, a sync master adjusts the send clock for its sync domain proportionally, based on the send clock of the other sync master. The maximum selectable ratio depends on the following factors:

- The default value of the send clock to which the PROFINET interface should synchronize.
- Selected PROFINET interface on the CPU
- Supported send clocks of the devices connected to the PROFINET networks.

Due to the synchronized send clock in a 1 ratio, the send clocks in the two PROFINET networks differ. You need a separate isochronous mode interrupt OB for each send clock. The isochronous mode interrupt OBs 61 to 64 are available in STEP 7.

7.7.6.2 Configuring the synchronization of the send clocks of PROFINET interfaces

Requirements

- STEP 7 as of V20
- The CPU must support the PROFINET functionality "PROFINET with IRT" at the PROFINETinterfaces (X1 and X2). For this reason, use one of the following CPUs:
  - CPU 1517(F)-3 PN
  - CPU 1518(F)-3 PN
  - CPU 1516T(F)-3 PN
  - CPU 1517T(F)-3 PN
  - CPU 1518T(F)-3 PN
- A STEP 7 project is open.
- One of the CPUs mentioned above has been configured.
- A PROFINET network has been configured on each of the PROFINET interfaces X1 and X2 of the CPU.
- STEP 7 displays the network view.

Procedure - Configuring synchronization roles and send clock

To configure the synchronization roles and the send clock in a sync domain in STEP 7, proceed as follows:

1. Select the desired PROFINET network.
2. Navigate in the Inspector window to "PROFINET subnet > Domain management > Sync domains".
3. Make the following settings in the "Devices > I/O devices" area:
   – Assign the synchronization role "Sync Master" to the PROFINET interface of the CPU.
   – Select the RT class "IRT
   " for the required IO devices. The synchronization role changes from "unsynchronized" to "sync slave."
4. Select a suitable send clock from the selection menu in the "Sync domain" area. By default, the send clock is set to a time of 1,000 ms.

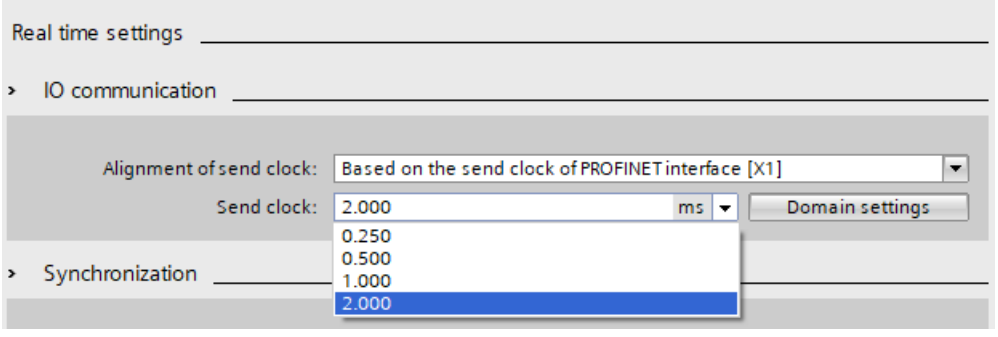
Result: You have configured the sync domain of the PROFINET network.

If you want to operate another PROFINET network with IRT at an S7-1500 CPU, then repeat steps 1 to 4 for the other PROFINET network.

Procedure - Synchronizing the send clock with another PROFINET interface

To synchronize the send clock with another PROFINET interface of the CPU, proceed as follows:

1. At the CPU, select the PROFINET interface, e.g. X2, to be synchronized based on the send clock of another integrated PROFINET interface.
2. In the Inspector window, navigate to "Advanced options > Real time settings > Synchronization".
3. Assign the synchronization role "Sync Master" to the PROFINET interface.
4. In the Inspector window, navigate to "Advanced options > Real time settings > IO communication".
5. In the selection menu next to "Alignment of send clock", select the entry "Based on the send clock of the PROFINET interface [X1]".
   STEP 7 adopts by default the send clock of the specifying PROFINET interface.
6. Depending on the application, select another possible send clock from the selection menu next to "send clock".



Result: The PROFINET interface X2 is coupled or synchronized with the set send clock of the PROFINET interface X1.

Alternatively, you can also configure the PROFINET interface X2 as the source for the shared send clock and synchronize the send clock of the PROFINET interface X1 to it.

If you change the default value for the send clock, you have to check the send clock settings of the PROFINET interfaces synchronized to it. The displayed send clock is displayed against a red background if the adopted or selected send clock is not supported by the synchronized PROFINET interface. In this case, click on the selection menu next to "Send clock" and select a valid value.

7.7.6.3 Operating several CPUs in isochronous mode

Introduction

As of STEP 7 V20 you can operate an isochronous application in a CPU with more than one PROFINET network (isochronous coupling of several PROFINET networks). For this, the CPU must support the PROFINET functionality "PROFINET with IRT" at both PROFINET interfaces (X1 and X2) In this case, you can synchronize the send clock of the sync domain of one PROFINET network with another PROFINET network. Consequently, the send clock starts simultaneously, and the application cycle is also synchronized.

Similarly, you can operate multiple CPUs and their connected PROFINET networks in isochronous mode. For this, at a PROFINET interface, one CPU takes over the send clock of the sync domain from the leading PROFINET network. The other PROFINET interface of the CPU synchronizes the adopted send clock for the sync domain of its PROFINET network. During synchronization, the adopted send clock is coupled to the other PROFINET interface in a 1:1 ratio by default. Alternatively, you synchronize the send clock proportionally to the other PROFINET interface.

Synchronization roles during adoption and synchronization of the send clock

Assign one of the following synchronization roles to the PROFINET interface in the leading PROFINET network:

- Sync master:
  The PROFINET interface uses your local send clock.
- Sync slave:
  The PROFINET interface uses the send clock of the PROFINET interface of a further CPU (sync master) in the same PROFINET network.

Assign the synchronization role "sync master" to the synchronizing PROFINET interfaces of the CPUs. In this case, the synchronization of the send clock must be based on the other PROFINET interface of the CPU. This configuration will be referred to as "controlled sync master" in the following sections.

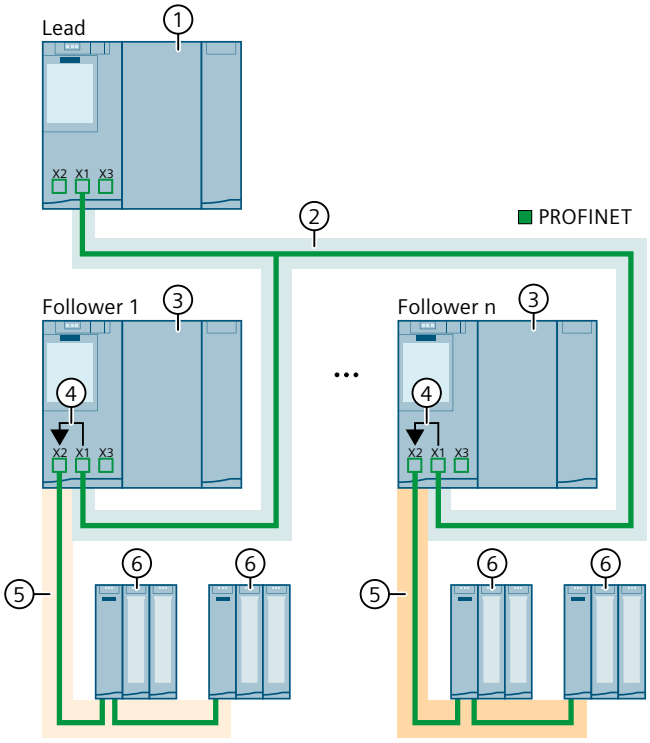
If both PROFINET interfaces of a CPU are configured as sync masters with a local send clock, no synchronization of the connected PROFINET networks will occur.

If you configure both PROFINET interfaces of a CPU as controlled sync master, STEP 7 will display an error message.

Example of the synchronization process

The PROFINET interfaces X1 of the CPUs "Lead" and "Follower" are located in the sync domain of the leading PROFINET network. The PROFINET interface X1 of the "lead" CPU is configured as the sync master with a local send clock in the sync domain. The PROFINET interfaces X1 of the "follower" CPUs are configured as sync slave in the sync domain and are synchronized to the "lead" CPU.

The PROFINET interfaces X2 of the "follower" CPUs are configured as controlled sync master and couple/synchronize the send clock for the sync domains of their connected PROFINET networks.



① S7-1500 CPU, PROFINET interface X1 configured as sync master
② Leading sync domain
③ S7-1500 CPU, PROFINET interface X1 configured as sync slave, PROFINET interface X2 configured as controlled sync master
④ Coupling/synchronizing the send clock: In the example, the send clock adjustment of PROFINET interface X2 is based on the send clock of PROFINET interface X1.
⑤ Coupled/synchronized sync domain
⑥ IO device, e.g. ET 200MP

Figure 3-424 Example of the synchronization process

Handling controlled sync masters

A sync slave always automatically synchronizes to the send clock of the sync master. If the sync master fails, a substitute clock of the same length is automatically generated at the sync slave.

The controlled sync master then synchronizes itself to the send clock of the sync slave. A controlled sync master synchronizes itself to the send clock of the sync domain of the leading IRT PROFINET IO system using one of the following options:

- Automatically:
  As soon as the controlled sync master detects a send clock, it synchronizes automatically to this cycle. This is the default response. You cannot influence this response.
- Manually:
  You determine the time of synchronization in the user program and can thus take suitable precautionary measures, e.g. deactivate devices and thus avoid system failures due to the synchronization process.
  The controlled sync master only synchronizes to the send clock when a valid send clock is detected and the corresponding instruction is called up as a start signal in the user program.

If you want to use manual synchronization on a controlled sync master, you must configure the controlling PROFINET interface as a sync slave. A controlling PROFINET interface that is configured as a sync master always generates a valid cycle. Synchronization is therefore not lost.

The instructions required to control and monitor synchronization are described in the following sections.

More information

Information on the exchange of data between the CPUs "Lead" and "Follower" is available in the section Direct data exchange (Page 247).

You can find information on cross-project isochronous mode in the section Operating multiple projects isochronously (Page 240).

7.7.6.4 Programming manual synchronization

Introduction

If a controlled sync master synchronizes to a PROFINET interface configured as a sync slave, you can also specify the time of synchronization in the user program. Define additional precautionary measures to avoid system failures caused by the synchronization process.

To specify manual synchronization in the user program, STEP 7 as of V20 contains the following instructions:

- GetIOSystemSync
- InitIOSystemSync
- StartIOSystemSync

Use these instructions to check the synchronization status and start the synchronization process. You can find these instructions under "Extended instructions > Distributed I/O".

The following sections describe the instructions and show the procedure for a manual synchronization process.

Determine type of synchronization

Use the InitIOSystemSync instruction to determine the type of synchronization. At the input mode, specify whether synchronization should take place manually or automatically. If InitIOSystemSync is not called, automatic synchronization is set by default.

You can find information on the parameters of the instructions in the STEP 7 online help.

Determine status of synchronization

The GetIOSystemSync instruction informs you about the status of synchronization. The SyncMode output displays the type of synchronization that was selected with the InitIOSystemSync instruction. The SyncStatus output displays the status of synchronization. This includes whether a send clock has been detected or whether a send clock is still being awaited.

You can find information on the parameters of the instructions in the STEP 7 online help.

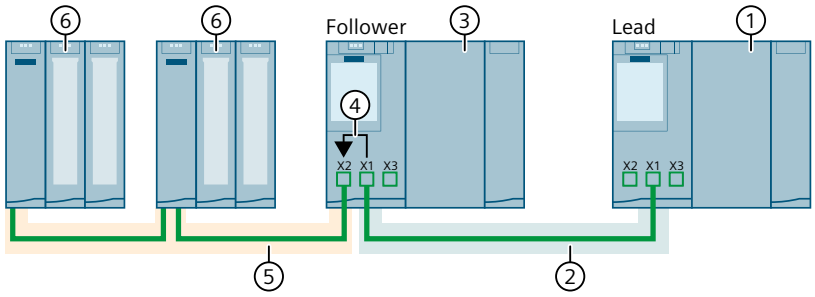
Start synchronization

If you call the StartIOSystemSync instruction in the user program and all requirements are met, synchronization starts. The requirements include, for example, the correct configuration of the PROFINET interfaces. In addition, the GetIOSystemSync instruction must signal at the outputs that manual synchronization has been selected and a valid send clock has been detected.

You can find information on the parameters of the instructions in the STEP 7 online help.

Configuration example of manual synchronization

The figure below shows a configuration example where you can use manual synchronization. The PROFINET interface X1 is configured as the sync master at the "lead" CPU. The sync master uses the local send clock. The PROFINET interface X1 is configured as the sync slave at the "follower" CPU. The sync slave is in the same sync domain of the PROFINET network as the sync master and synchronizes to the send clock. The PROFINET interface X2 of the "follower" CPU is configured as the controlled sync master. The controlled sync master only starts the synchronization to the send clock of the PROFINET interface X1 for the sync domain of its connected PROFINET network once all requirements have been met.



① S7-1500 CPU, PROFINET interface X1 configured as sync master
② Sync domain of the leading PROFINET network
③ S7-1500 CPU, PROFINET interface X2 configured as controlled sync master
④ Coupling/synchronizing the send clock of the PROFINET interface X1
⑤ Sync domain of the coupled/synchronized PROFINET network
⑥ IO device, e.g. ET 200MP

Figure 3-425 Configuration example of manual synchronization

Manual synchronization procedure

The figure below shows the manual synchronization procedure. The instructions and the associated input/output parameters are processed by the user program in the "follower" CPU. If manual synchronization was selected at InitIOSystemSync, the PROFINET interfaces remain synchronized until the connection to the sync master is interrupted. The GetIOSystemSync instruction immediately indicates a connection abort at the output SyncStatus. The StartSystemSync instruction outputs the value "0" at the Ret_Val output and starts manual synchronization only when the following conditions are met:

- The GetIOSystemSync instruction indicates at the output SyncStatus that a send clock has been detected.
- The requirements for starting synchronization manually have been met.

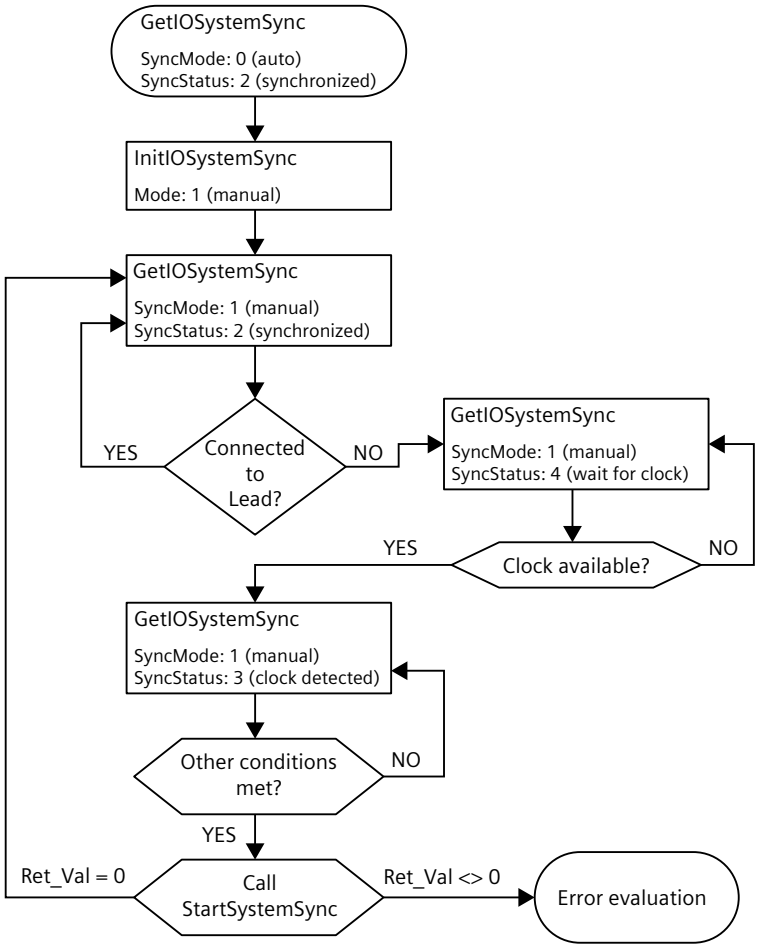


Figure 3-426 Manual synchronization procedure

7.7.7 Operating multiple projects isochronously

With IRT isochronous mode across several projects, you can transfer IRT synchronization from one project to other projects. This allows two CPUs to exchange data isochronously, even though each CPU is used in a separate project. This allows you to, for example, delimit the responsibilities of individual plant parts and create clearly defined interfaces.

To implement cross-project IRT clock synchronization, use one of the following devices:

- PN/PN coupler as of FW version V6.0:
  A PN/PN coupler can connect two subnets isochronously with each other, each of which you use in a separate project. You can use several PN/PN couplers within a subnet.
- Isochronous I-device with an S7-1500 CPU as of FW version V4.1:
  If the CPU supports the "PROFINET with IRT" functionality at several PROFINET interfaces, you can configure the CPU as an isochronous I-device in a separate project. The PROFINET interface configured as an I-device is used for isochronous data exchange with a higher-level IO controller. The other PROFINET interface can synchronize with the I-device interface and operate connected IO devices isochronously.
  In another project, import the I-device as a GSD file and assign the I-device to a higher-level IO controller.

Basics of configuration

In the first project, use the desired device from the hardware catalog and adapt the configuration. Then export the configured device as a GSD file. The exported GSD file is used in other projects as a substitute for the configured device from the first project.

You can read how to implement IRT clock synchronization across several projects with a PN/PN coupler in the Synchronous operation functions (https://support.industry.siemens.com/cs/ww/en/view/109974350) Function Manual.

The following sections describe the cross-project IRT clock synchronization with an S7-1500 CPU as I-device.

7.7.7.1 Cross-project clock synchronization with an I-device

If you want to implement cross-project clock synchronization with an S7-1500 CPU, use an S7-1500 CPU as of FW version V4.1. The CPU must support the "PROFINET with IRT" functionality on several PROFINET interfaces. A PROFINET interface (I-device), e.g. X2 is used for isochronous data exchange with the higher-level IO controller. The other PROFINET interface, e.g. X1 can couple/synchronize to the send clock and use the send clock for its connected PROFINET IO system.

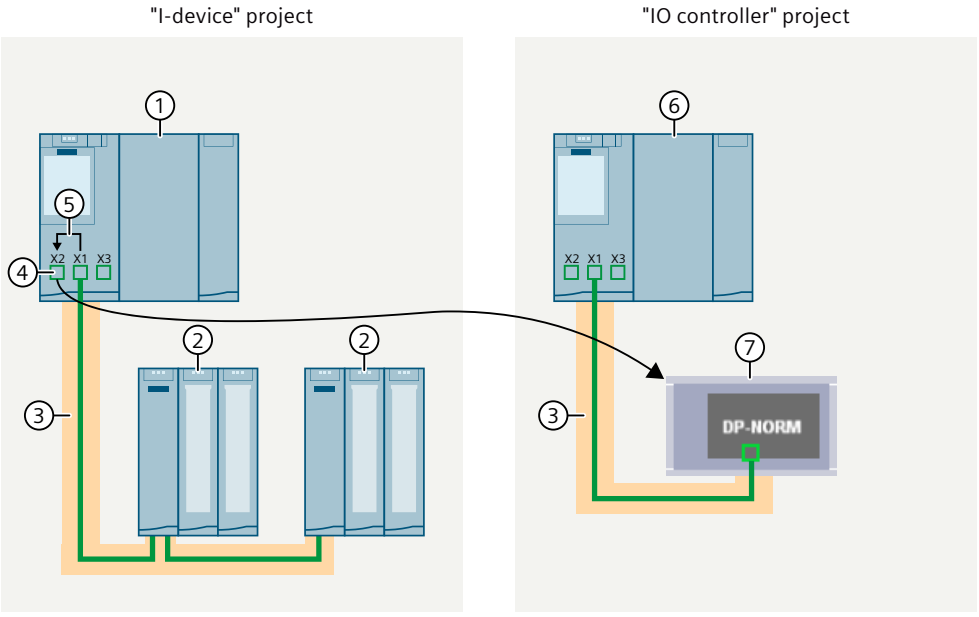
NOTE

Operating a PROFINET interface as an I-device with IRT in isochronous mode
If you configure a PROFINET interface as an I-device with IRT in isochronous mode, this PROFINET interface cannot be an IO controller for IO devices with IRT. IO devices with RT are possible on this PROFINET interface.

Create the following projects in STEP 7 for cross-project clock synchronization with an S7-1500 CPU:

- "I-device" project:
  In this project, you configure an isochronous I-device with a fixed send clock and isochronous applications. To do this, use a PROFINET interface, e.g. X2 an S7-1500 CPU from the hardware catalog.
  If required, you can configure the synchronization of the send clock for both PROFINET interfaces. In this case, the PROFINET interface without I-device functionality, e.g. X1, can synchronize the send clock as a controlled sync master for a lower-level PROFINET IO system.
  You export the configured I-device as a GSD file. The GSD file serves as a substitute for the configured I-device in other projects.
- "IO controller" project:
  In this project, you install the GSD file exported from the "I-device" project. Use the GSD file in this project as a substitute for the I-device on a higher-level IO controller from the hardware catalog.
  An isochronously configured I-device requires clock synchronization in the IO controller. Therefore, in the sync domain settings, select the value for the send clock that was also set in the I-device.

The following figure shows the interaction between the "I-device" project and the "IO controller" project.



① CPU 1517-3 PN with connected isochronous PROFINET IO system on the PROFINET interface X1.
② IO device, e.g. ET 200MP
③ Sync domain
④ PROFINET interface X2, configured as an isochronous I-device.
⑤ Coupling/synchronizing the send clock of the PROFINET interface X1 (optional)
⑥ IO controller, e.g. CPU 1517-3 PN
⑦ Imported GSD file of the PROFINET interface X2 from the "I-device" project

Figure 3-427 Cross-project clock synchronization with an I-device

The following sections describe the configuration procedures in the "I-device" and "IO controller" projects.

Procedure - "I-device" project

In the "I-device" project, you configure a PROFINET interface, e.g. X2 of the desired CPU as an isochronous I-device. Optionally configure the synchronization of the send clock for the other PROFINET interface without I-device functionality.
You can find information on configuring I-devices in the section Configuring the I-device (Page 129). You can find out how to synchronize the PROFINET interfaces of a CPU in the section Configuring the synchronization of the send clocks of PROFINET interfaces (Page 233).

To use isochronous mode on the I-device, you must enable the option 'Parameter assignment of PN interface by higher-level IO controller' when configuring the I-device. Once you have configured your I-device and synchronized the PROFINET interfaces, configure the clock synchronization for various projects on the I-device as follows:

1. In the network view of STEP 7, select the PROFINET interface configured as an I-device, e.g. X2 of the CPU.
2. Optional, to avoid address conflicts in other projects:
   - In the Inspector window, navigate to the "General > Ethernet addresses" area.
   - In the "Internet Protocol Version 4 (IPv4)" area, select the "IP address is set directly in the device" option.
   - In the "PROFINET" area, activate the "PROFINET device name is set directly at the device" check box.
3. In the Inspector window, navigate to "General > Operating mode > Isochronous mode"
4. Select the "Isochronous mode" check box.
5. Configure the desired transfer areas for isochronous mode as follows:
   - Select a transfer area in the Inspector window under "General > Operating mode > I-device communication", e.g. "Transfer area_1"
     The Inspector window shows the selected transfer area.
   - Select the "Isochronous mode" check box.
   - Select or generate an isochronous mode interrupt OB for the transfer area, e.g. OB 61.

– Select the process image for the transfer area, e.g. PIP 1.

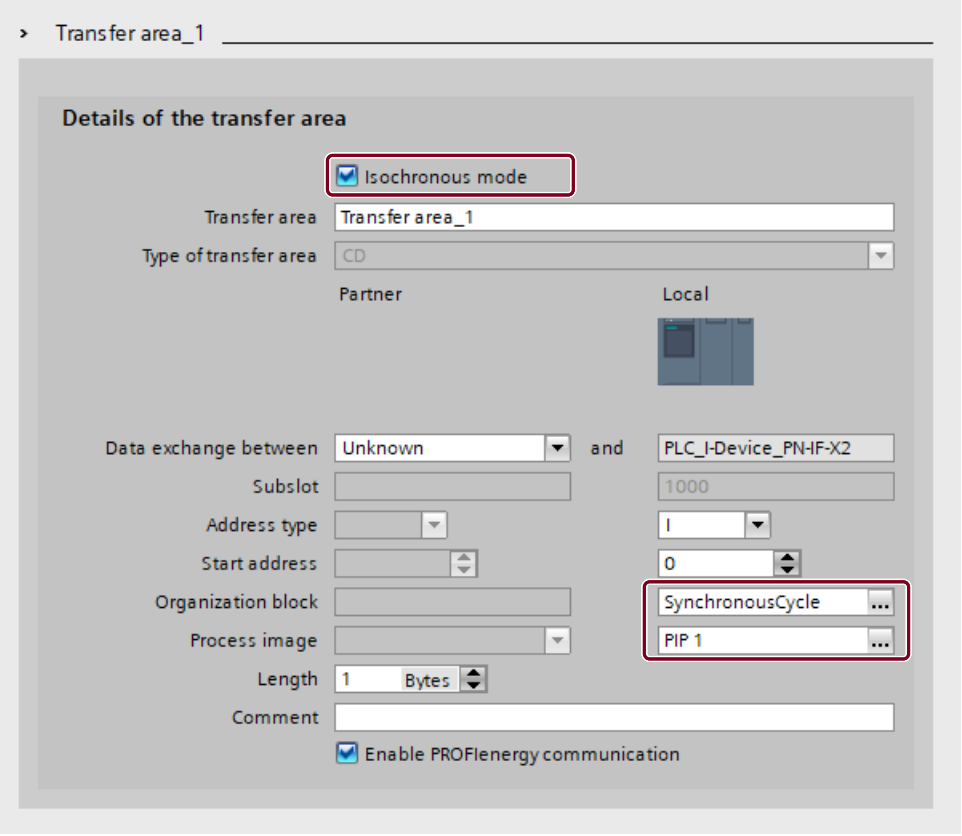


Figure 3-428 Configuring isochronous transfer range on the I-device

6. Repeat step 5 for each additional transfer area that you want to use isochronous mode.
7. In the Inspector window, go to "General > Advanced options > Real time settings".
8. Select the desired send clock.
   For a PROFINET interface that is configured as an I-device, you cannot change the "Alignment of send clock" option.
9. Compile the CPU configured as an I-device.
   The export as GSD file only works immediately after the compiling process. If you change the configuration, you need to compile the CPU configured as an I-device again.
   The "Export" button in the "Operating mode > I-device communication > Export device description file (GSD)" area can be selected.
10. Click the "Export" button
    The export dialog opens.
11. Assign a name for the I-device proxy as well as a description and a storage location (path) in the fields provided.
12. Click the "Export" button to complete the process.

Result: You have configured the I-device for isochronous mode in various projects and exported it as a GSD file.

Procedure - "IO controller" project

In the "IO controller" project, use the previously configured isochronous I-device as a GSD file on a higher-level IO controller.

To assign the imported I-device to a higher-level IO controller and configure the clock synchronization, proceed as follows:

1. Install the GSD file exported from the "I-device" project in STEP 7.
2. Add an IO controller (e.g. CPU 515-2 PN) from the hardware catalog in the network view using drag-and-drop.
3. Add the imported I-device from the hardware catalog using drag-and-drop.
   You can find information on the imported I-device under "Other field devices > PROFINET IO > PLCs & CPs > Siemens Aktiengesellschaft"
4. Connect the PROFINET interface of the I-device to the desired PROFINET interface of the IO controller.
5. Select the PROFINET network.
6. In the Inspector window, navigate to "PROFINET subnet > Domain management > Sync domains".
7. Make the following settings in the "Devices > IO devices" area:
   - Assign the "Sync master" synchronization role to the PROFINET interface of the IO controller.
   - Select the RT class "IRT" for the I-device.
     The synchronization role changes from "Unsynchronized" to "Sync Slave".
8. In the "Sync domain" area, select the same send clock that you selected in the I-device configuration.
9. Switch to the device view of the I-device.
10. Configure the isochronous transfer areas as follows:
    - Select a transfer area in the "Device overview" area, e.g. "Transfer area_1".
    - In the Inspector window, navigate to the "General > I/O addresses" area.
    - Select or generate an isochronous mode interrupt OB for the transfer area, e.g. OB 61.

– Select the process image for the transfer area, e.g. PIP 1.

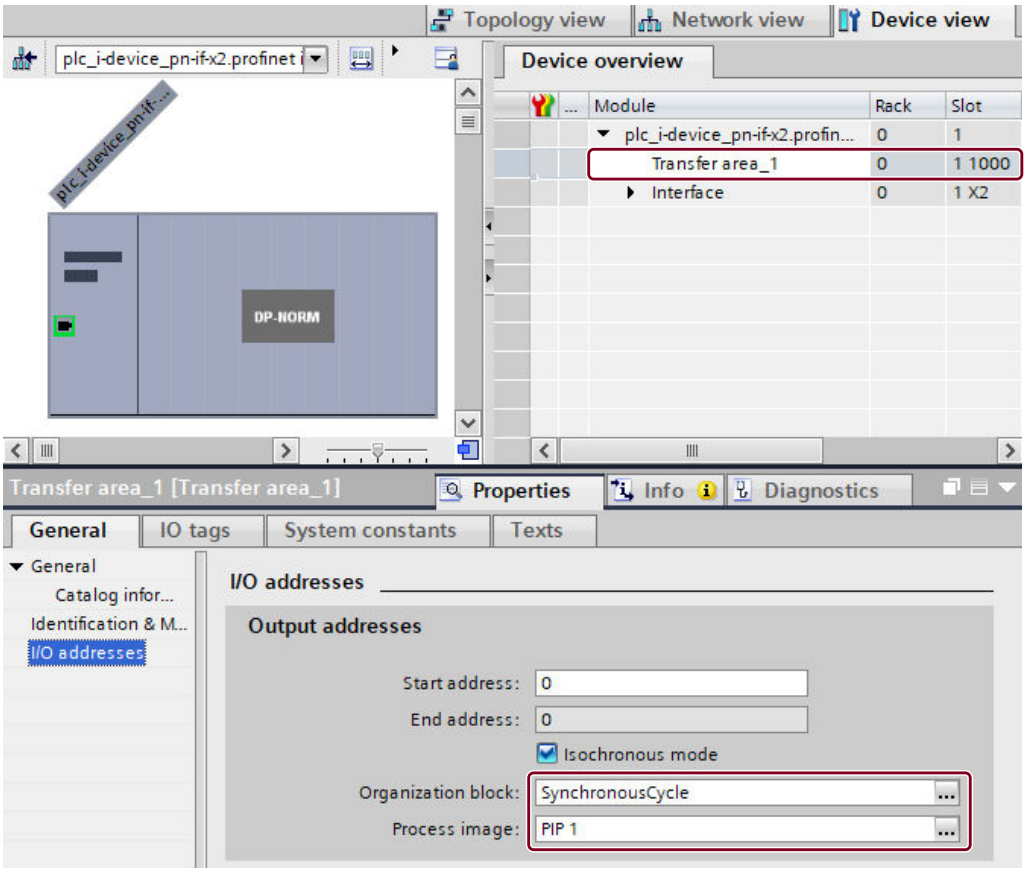


Figure 3-429 Configuring isochronous transfer range on the imported I-device

11. Repeat step 10 for each additional transfer area that you want to use isochronous mode.
12. Change to the topology view.
13. Configure the topology between the IO controller and I-device.

Result: You have assigned the imported I-device to a higher-level IO controller and configured the clock synchronization.

Set the same send clock in all projects

The send clock set in the I-device ("I-device" project) must match the send clock of the higher-level IO controller ("IO controller" project).

If you want to change the send clock at a later date, you do not need to export and import the I-device again. To change the send clock, proceed as follows:

1. Change the send clock in the I-device project.
2. In the I-device project, adjust the time for the application cycle in the isochronous mode interrupt OB.
3. Load the changes to the I-device CPU.

4. Change the send clock in the IO controller project.
5. In the IO controller project, adjust the time for the application cycle in the isochronous mode interrupt OB.
6. Load the changes into the higher-level IO controller.

Result: You have changed the send clock and loaded it into the I-device and the higher-level IO controller.

7.8 Direct data exchange

7.8.1 Introduction

This section describes the direct data exchange function.

Principle of operation

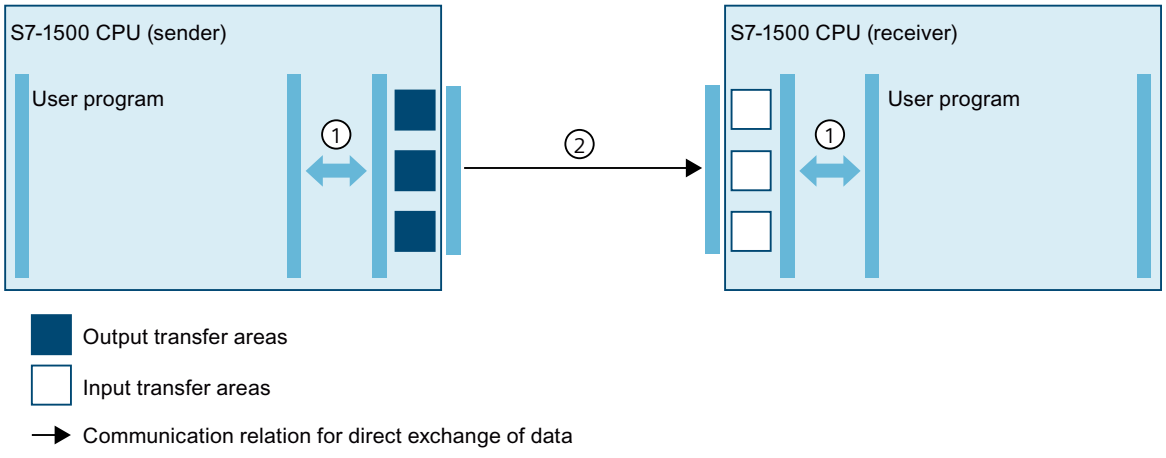
Starting with firmware version V2.8, the S7-1500 CPU supports direct data exchange (cross data traffic) with other S7-1500 CPUs.

In the case of direct data exchange, an S7-1500 CPU provides cyclic user data from the I/O area to one or more partners. The direct data exchange is based on PROFINET with IRT and isochronous mode.

The data exchange takes place via transfer areas.

Direct data exchange between two S7-1500 CPUs (1:1)

The figure below shows the direct data exchange between two S7-1500 CPUs. The output transfer areas of the sending S7-1500 CPU correspond to the input transfer areas of the receiving S7-1500 CPU.



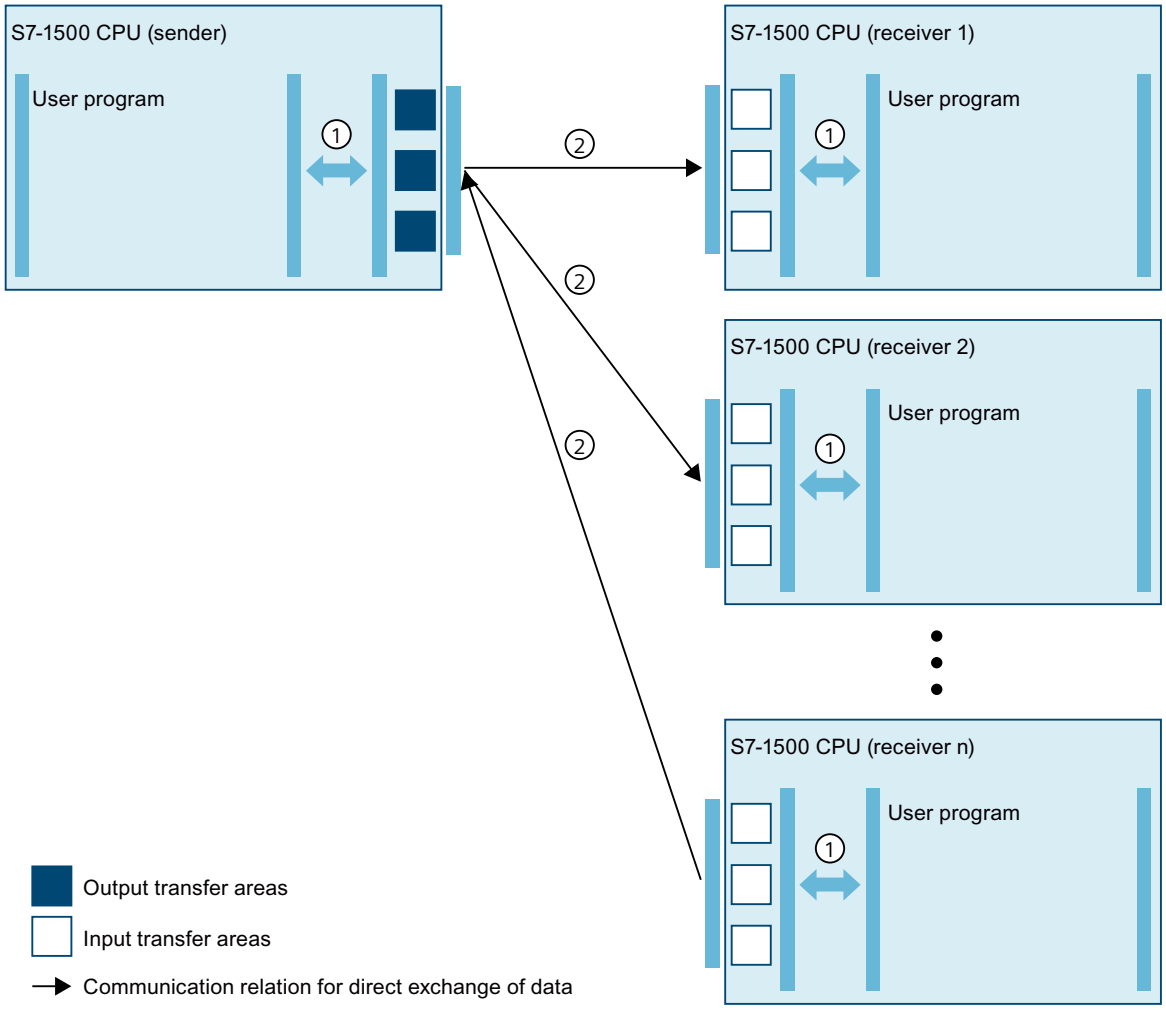
① Transfer relation between the user program and the transfer area. The user program and the transfer areas exchange input and output data via this path.

② Communication relation for direct data exchange You configure the communication relations in STEP 7. You create transfer areas for direct data exchange in the properties of the communication relations.

Figure 3-430 Direct data exchange between two S7-1500 CPUs (1:1)

Direct data exchange with multiple receivers (1:n)

The following figure shows the direct data exchange with multiple S7-1500 CPUs. In this case, the sending S7-1500 CPU provides the data of its output transfer areas to multiple S7-1500 CPUs. Each receiving S7-1500 CPU has its own input transfer areas.



① Transfer relation between the user program and the transfer area. The user program and the transfer areas exchange input and output data via this path.

② Communication relation for direct data exchange You configure the communication relations in STEP 7. You create transfer areas for direct data exchange in the properties of the communication relations.

Figure 3-431 Direct data exchange with multiple receivers (1:n)

Applications

- Deterministic, isochronous I/O communication between multiple S7-1500 CPUs

Properties of direct data exchange

- Always isochronous
- Support of MRPD for MRP configuration
- No acyclic data exchange via PROFINET data record mechanisms
- No PROFINET alarms
- Configuration limits:
  - Maximum data length for direct data exchange 3075 bytes including user data qualifier
  - Maximum data length for a transfer area: 1024 bytes without user data qualifier
  - Maximum number of transfer areas of sender: 128
  - Maximum number of transfer areas of receiver: 512, distributed among a maximum of 64 receivable PROFINET frames and thus up to 64 sender CPUs

Diagnostics options of the receiver

Operating state change of sender:

- When the sender goes from RUN to STOP, the receiver behaves as follows:
  - The "SYNC_PI" and "SYNC_PO" instructions return an error message in parameter RET_VAL during synchronization of the process image.
  - With direct I/O access to the input transfer areas of the direct data exchange, OB 122 "I/O access error" is called, if present.
  - Incoming diagnostic message "I/O data failure in hardware component"
- When the sender goes from STOP to RUN, the receiver behaves as follows:
  - Call of OB 83 "Pull/plug interrupt" for input transfer areas of the direct data exchange
  - Up until the call of OB 83, OB 122 is called if present.
  - Outgoing diagnostic message "User data failure of hardware component"

Station failure/station recovery of the sender:

- When the sender fails, e.g. due to a bus interruption, the receiver behaves as follows:
  - Call of OB86 "Rack failure"
  - The "SYNC_PI" and "SYNC_PO" instructions return an error message in parameter RET_VAL during synchronization of the process image.
  - With direct I/O access to the input transfer areas of the direct data exchange, OB 122 "I/O access error" is called, if present.
- When the sender recovers after a station failure, e.g. because the bus connection is re-established, the receiver behaves as follows:
  - Call of OB86 "Rack failure"

7.8.2 Configuring direct data exchange between two S7-1500 CPUs

The procedure for configuring direct data exchange between two IO controllers is described below.

First, you create the communication relation for direct data exchange. You then configure transfer areas for the connection.

Requirements

- STEP 7 V16 or higher
- Two S7-1500 CPUs firmware version V2.8 or higher
- IRT is configured:
  - Both CPUs are in one sync domain.
  - One CPU is the sync master, and the other CPU is the sync slave.
  - Ports are interconnected.

Setting up the communication relation for direct data exchange

To set up the communication relation for direct data exchange between two S7-1500 CPUs, follow these steps:

1. Select the PROFINET interface X1 of the sending S7-1500 CPU.
2. Change to the table view of the network view, tab "I/O communication".
   The PROFINET interface X1 of the CPU is shown in the "Partner 1" column.
3. In the "Partner 2" column at "<Drop or select the device here>", select the PROFINET interface of the communication partner from the drop-down list as the connection partner.
   Note the communication direction:
   - ←: Communication partner is sender
   - →: Communication partner is receiver

The communication relation for direct data exchange between the two S7-1500 CPUs is set up.

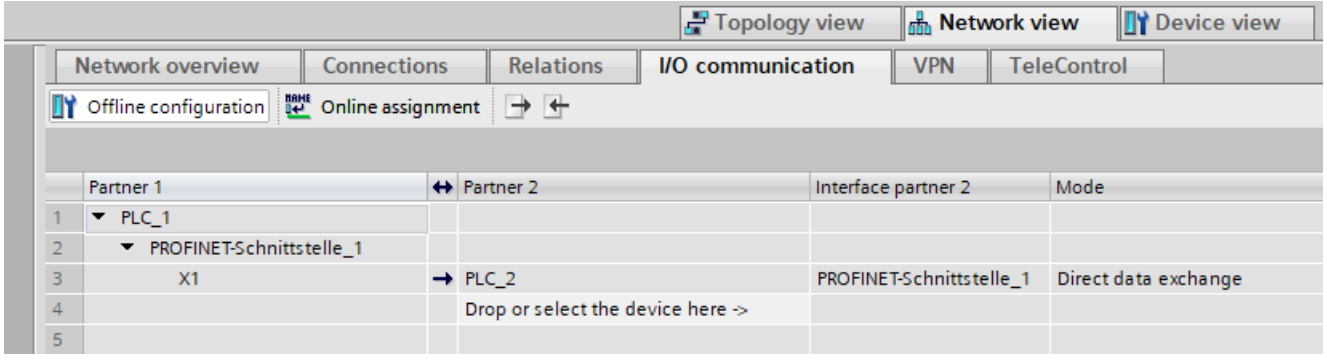


Figure 3-432 Communication relation for direct data exchange

Configuring transfer areas for direct data exchange

To configure a transfer area for direct data exchange, follow these steps:

1. Select the communication relation for direct data exchange.

	Partner 1		Partner 2	Interface partner 2	Mode
1	PLC_1				
2	PROFINET-Schnittstelle_1				
3	X1	→	PLC_2	PROFINET-Schnittstelle_1	Direct data exchange
4			Drop or select the device here ->		
5					

Figure 3-433 Communication relation for direct data exchange

2. Navigate to the properties of the communication relation to "General" > "Direct data exchange" > "Transfer areas".
3. Create a new transfer area by double-clicking on "<Add new>". Assign a meaningful name for the transfer area.

A transfer area for direct data exchange is created.

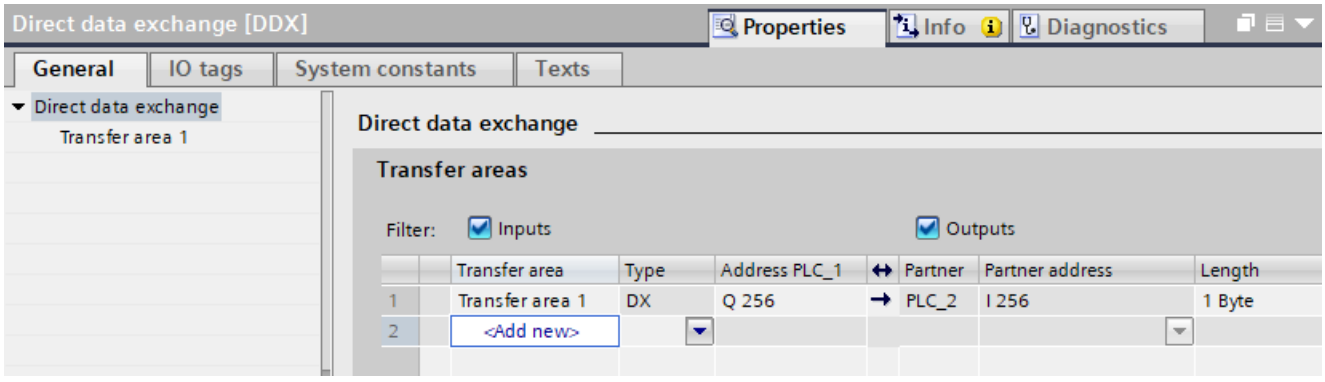


Figure 3-434 Transfer area for direct data exchange

The communication direction of the transfer area is specified by the communication relation. You cannot change the communication direction of the transfer area.

Editing the transfer area

Set the properties of the transfer area under "General" > "Direct data exchange" > "Name of transfer area" > "Detail of the transfer area".

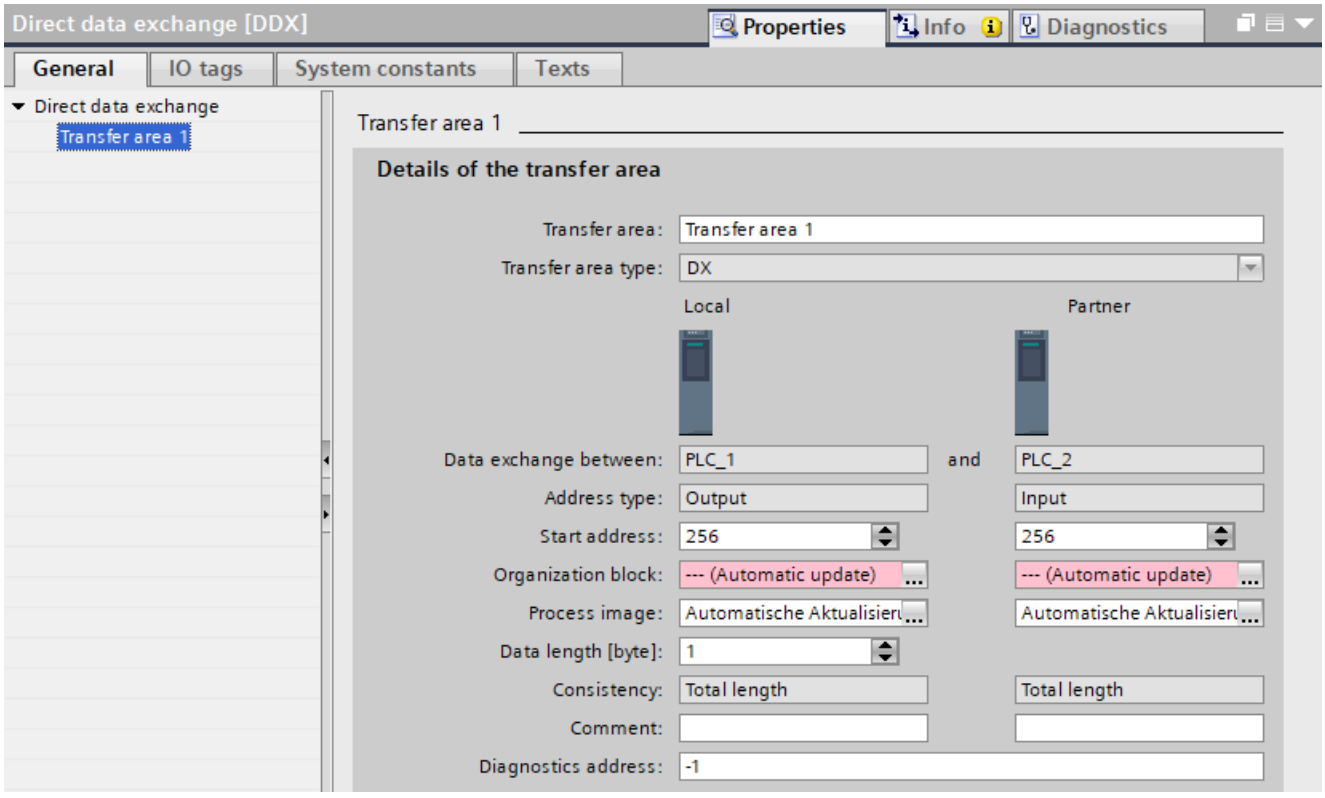


Figure 3-435 Properties of the transfer area

Table 3-49 Overview of the settings of the transfer area

Parameter	Local	Partner
Start address	Set the start address of the input or output transfer areas in the local CPU.	Set the start address of the input or output transfer areas in the partner CPU.
Organization block	Assign the transfer area to an isochronous mode interrupt OB or the "MC-Servo" OB.	Assign the transfer area to an isochronous mode interrupt OB or the "MC-Servo" OB.
Process image	Select a process image partition, e.g. PIP 1. If you have assigned "MC-Servo" as the organization block, STEP 7 automatically sets "PIP OB Servo" as the process image.	Select a process image partition, e.g. PIP 1. If you have assigned "MC-Servo" as the organization block, STEP 7 automatically sets "PIP OB Servo" as the process image.
Data length [bytes]	Set the size of the transfer area.	-

Downloading the configuration to devices

Rules:

- Download the configuration to all CPUs involved.
- If you make changes to the configuration of the direct data exchange, download these changes to all CPUs involved.

7.8.3 Configuring direct data exchange between multiple IO controllers

The procedure for configuring direct data exchange between multiple S7-1500 CPUs is described below.

First, you set up the communication relations for direct data exchange. You then configure transfer areas for the communication relations.

Requirements

- STEP 7 V16 or higher
- S7-1500 CPUs firmware version V2.8 or higher
- IRT is configured:
  - All CPUs are in one sync domain.
  - One CPU is the sync master, and the other CPUs are sync slaves.
  - Ports are interconnected.

Setting up the communication relations for direct data exchange

To set up the connection for direct data exchange between multiple S7-1500 CPUs, follow these steps:

1. Select the PROFINET interface X1 of the sending CPU.
2. Change to the table view of the network view, "I/O communication" tab.
   The PROFINET interface X1 of the CPU is shown in the "Partner 1" column.
3. In the "Partner 2" column at "<Drop or select the device here>", select the PROFINET interface of the communication partner from the drop-down list as the connection partner.
   Note the transfer direction:
   - ←: Connection partner is sender
   - →: Connection partner is receiver

   The connection for direct data exchange between the two S7-1500 CPUs is set up.
4. Repeat step 3 for every other receiving IO controller.

The connections for direct data exchange between the sending CPU and the receiving CPUs are set up.

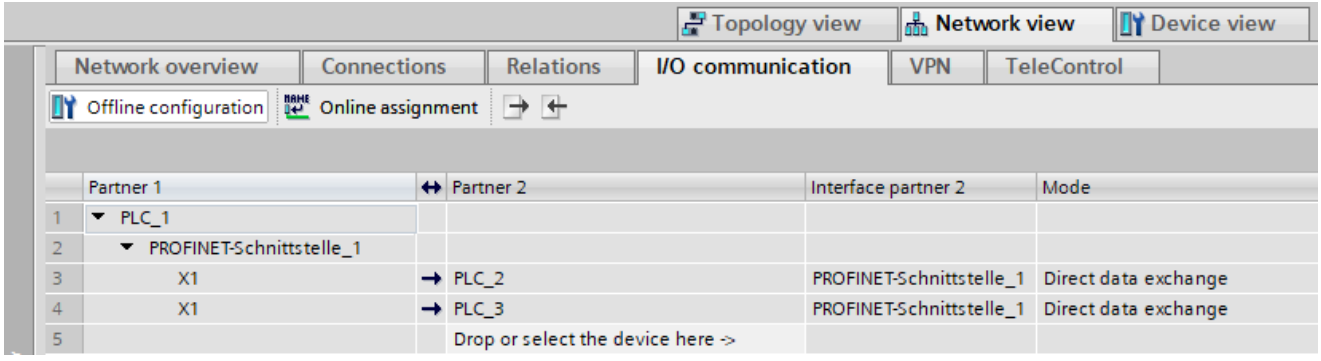
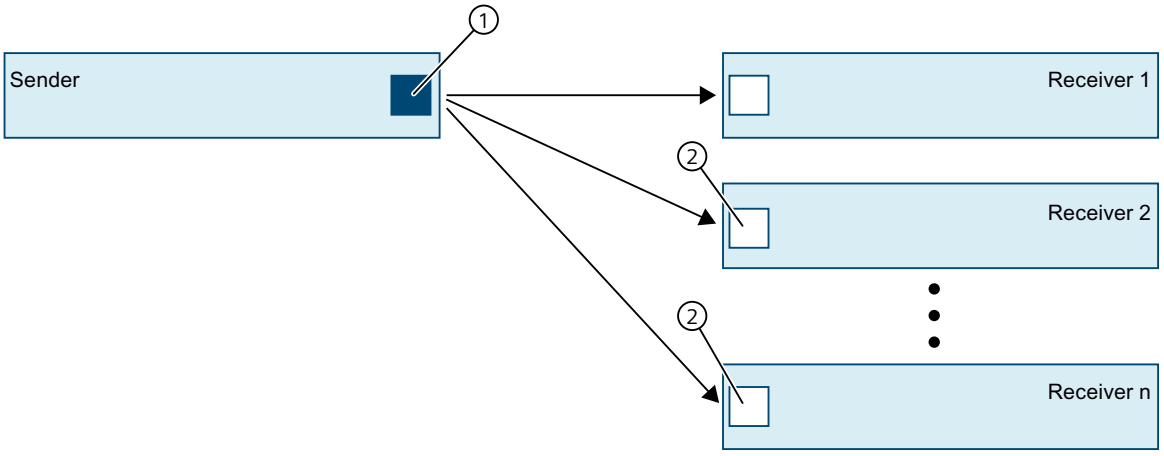


Figure 3-436 Connection for direct data exchange with multiple S7-1500 CPUs

Configuring transfer areas for direct data exchange

The following graphic shows the order for configuration of the transfer areas.



① First, you configure the transfer area between the sender and one receiver. You configure this transfer area at the PROFINET interface of the sender.

② You then configure the transfer areas between the sender and the other receivers. You configure these transfer areas at the PROFINET interfaces of the receivers.

Figure 3-437 Order of configuration of transfer areas in the case of multiple receivers

To configure a transfer area for direct data exchange, follow these steps:

1. Select the PROFINET interface X1 of the sending CPU and change to the table view, "I/O communication" tab.
2. In the table view of the network view, select a communication relation for direct data exchange between the sender and receiver 1.
3. Navigate to the properties of the I/O connection to "General" > "Direct data exchange" > "Transfer areas".
4. Create a new transfer area by double-clicking on "<Add new>". Assign a meaningful name for the transfer area.

   A transfer area for direct data exchange between the sender and receiver 1 is configured.

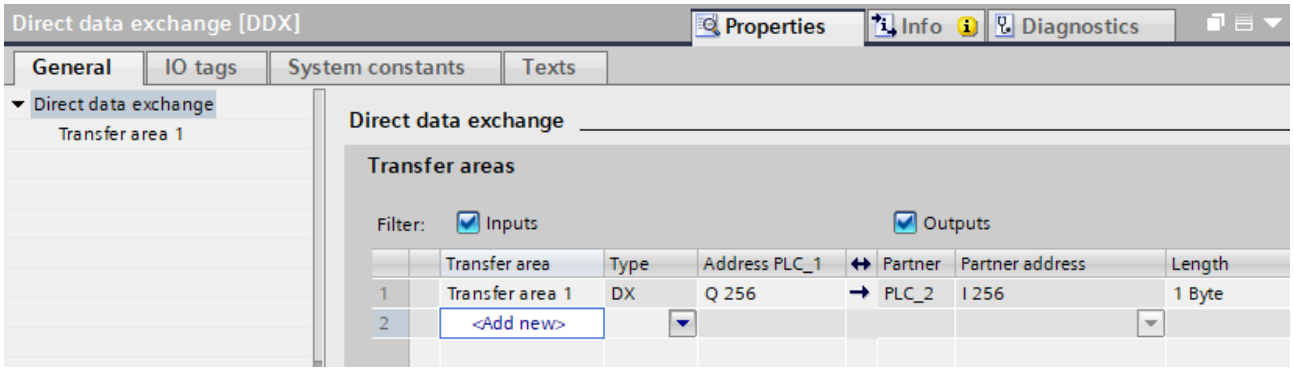
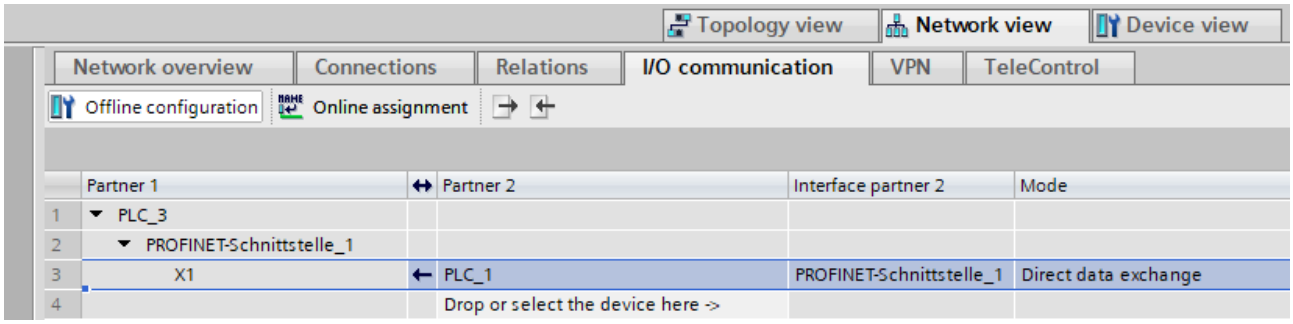


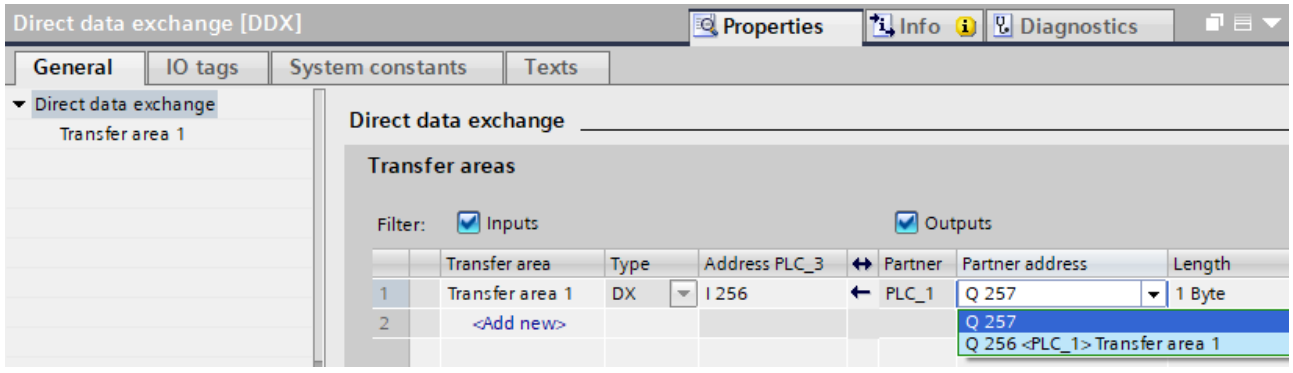
Figure 3-438 Transfer area for direct data exchange

5. Now, select the PROFINET interface of a receiver for which a transfer area is not yet set up, e.g. receiver 2.

6. Change to the table view of the network view to "I/O communication"
   The communication relation for direct data exchange with the sender is displayed.



7. Select the communication relation.
8. Navigate to the properties to "General" > "Direct data exchange" > "Transfer areas".
9. Create a new transfer area by double-clicking on "<Add new>". Assign a meaningful name for the transfer area.
   A transfer area for direct data exchange is configured.
10. Select the transfer area.
11. For "Partner address", select the existing address area in the sender as the output transfer area.



A transfer area for direct data exchange between receiver 2 and the sender is configured.

Editing the transfer area

Set the properties of the transfer area under "General" > "Direct data exchange" > "Name of transfer area" > "Detail of the transfer area".

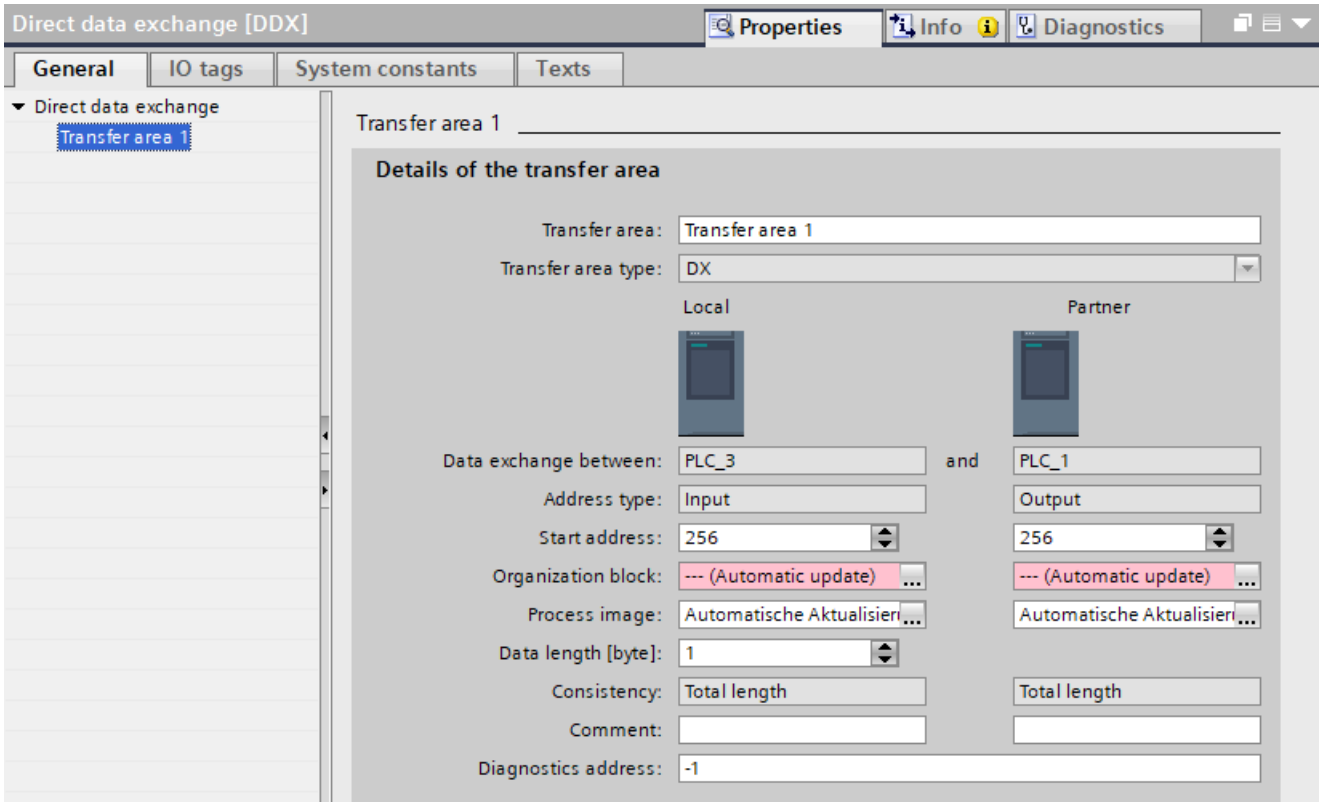


Figure 3-441 Properties of the transfer area

Table 3-50 Overview of the settings of the transfer area

Parameter	Local	Partner
Start address	Set the start address of the input or output transfer areas in the local CPU.	Set the start address of the input or output transfer areas in the partner CPU.
Organization block	Assign the transfer area to an isochronous mode interrupt OB or the "MC-Servo" OB.	Assign the transfer area to an isochronous mode interrupt OB or the "MC-Servo" OB.
Process image	Select a process image partition, e.g. PIP 1. If you have assigned "MC-Servo" as the organization block, STEP 7 automatically sets "PIP OB Servo" as the process image.	Select a process image partition, e.g. PIP 1. If you have assigned "MC-Servo" as the organization block, STEP 7 automatically sets "PIP OB Servo" as the process image.
Data length [bytes]	Set the size of the transfer area.	-

Downloading the configuration to the device

Rules:

- Download the configuration to all CPUs involved.
- If you make changes to the configuration of the direct data exchange, download these changes to all CPUs involved.

7.9 Device replacement without exchangeable medium

Definition

IO devices which have no slot for exchangeable medium (e.g. ET 200SP, ET 200MP) or IO devices which support the PROFINET functionality "Device replacement without exchangeable medium/PG" can be replaced without having an exchangeable medium with saved device names inserted and without having to assign the device name with the PG. The new IO device is given a device name by the IO controller and not by the exchangeable medium or the PG.

To assign the device name, the IO controller uses the configured topology and the neighborhood relations established from the IO devices.

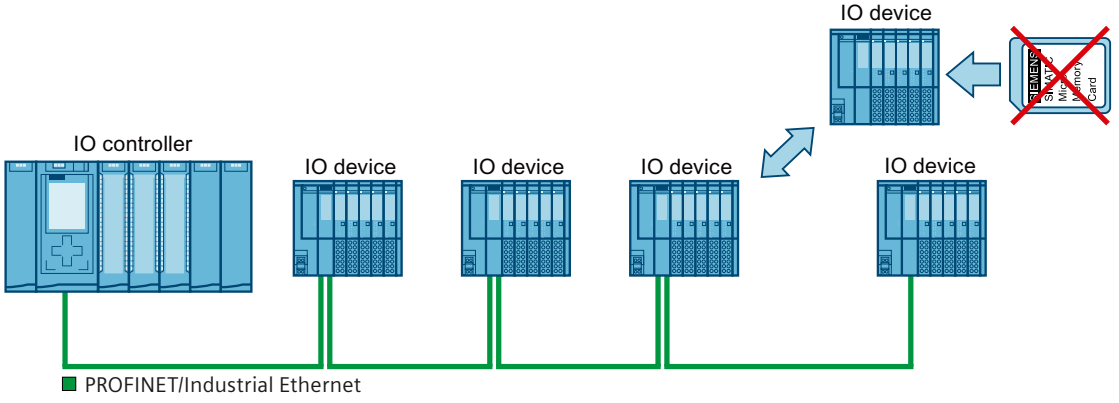


Figure 3-442 Device replacement without exchangeable medium

NOTE

When you exchange a device, make sure that the PROFINET cable is again inserted into the correct port, as it is configured in STEP 7.
Otherwise, the device names can be assigned incorrectly.

Advantages

With the Device replacement without exchangeable medium/PG PROFINET functionality, you can profit from the following advantages:

- After the replacement of the IO device, it automatically obtains its device name from the IO controller. You no longer have to assign device names with the PG or exchangeable medium.
- You can save on the storage medium for the IO device that replaces the removed one.
- Simple device name allocation with series machines that have the same configuration and set topology. It is no longer necessary to assign device names via exchangeable medium/PG.

Which devices support device replacement without exchangeable medium?

An overview of the devices that support the "Device replacement without exchangeable medium" function is provided in this FAQ (https://support.industry.siemens.com/cs/ww/en/view/36752540).

7.9.1 Device replacement without exchangeable medium/PG function

Neighborhood

Neighborhood is the physical relationship between two ports of adjacent PROFINET devices. A PROFINET device is connected in this case through one of its ports over a physical Ethernet line to a specific port of the second PROFINET device in close proximity (neighbors).

Both terminal devices, for example, IO controllers and IO devices with a port, and network components, for example, switches, IO controllers and IO devices with multiple ports, are considered PROFINET devices.

Failure and replacement of an IO device

The following example describes device replacement without exchangeable medium in the case of failure of an IO device.

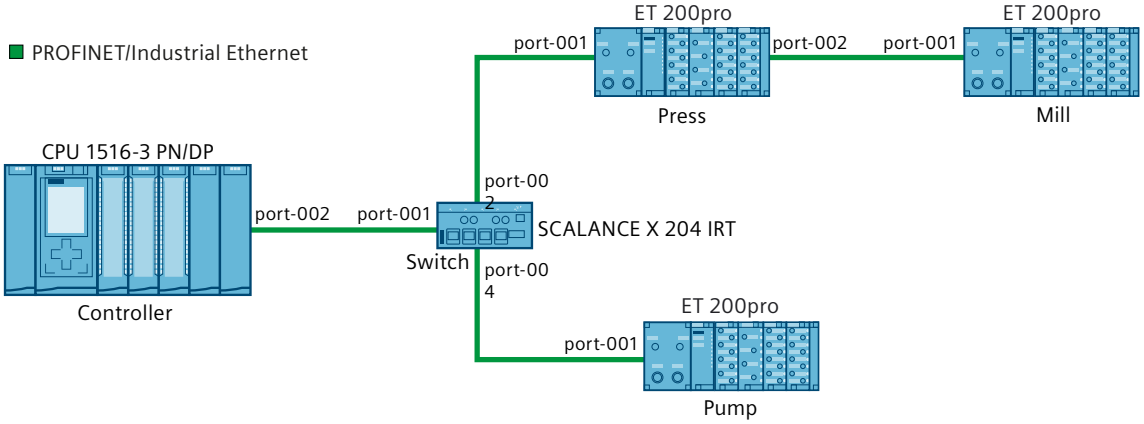


Figure 3-443 Example configuration of device replacement without exchangeable medium

For the device replacement, the following information is available to the IO controller:

PROFINET device	Device alias
Controller	"port-001.Switch"
Switch	"port-002.Controller", "port-001.Press", "port-001.Pump"
Press	"port-002.Switch", "port-001.Mill"
Mill	"port-002.Press"
Pump	"port-004.Switch"

The IO device with the device name "Mill" fails in this example:

Requirement

The PROFINET device replacing the removed one has no device name.

Principles of name assignment

The failure of the "Mill" IO device is considered here.

1. The IO controller queries the device name of the replaced IO device.
2. The IO controller detects that the IO device with the device alias "port-002.Press" does not have a device name.
3. The IO controller assigns the device name "Mill" to the replaced IO device via the device alias "port-002.Press" of the failed IO devices.

NOTE

If you insert a device with the Device replacement without exchangeable medium/PG PROFINET functionality at a different location than the configuration, a different device name is then assigned to the device.

Reset a wrongly inserted device to delivery state before you use it again.

7.9.2 Replacing an IO device without exchangeable medium

Introduction

Replacement of IO devices is sometimes frequently required in automation systems. The IO devices are generally assigned a device name by either inserting an exchangeable medium or via the programming device. The CPU identifies the IO device by using these device names.

Under certain circumstances, replacing an IO device can be done without inserting an exchangeable medium or without the PG.

Requirements

- The topology of the PROFINET IO system with the respective IO devices must be configured.

  By configuring the topology, the neighbor relationships of all the PROFINET devices located in the PROFINET IO system are announced to the PROFINET IO system or the IO controller. From the neighbor relationships specified by the set topology and the actual neighbor relationships established by the real PROFINET devices, the IO controller can identify the replaced IO device without a name and assign to it the configured name and the IP address and then again list it in the user data traffic.
- The affected IO devices in the automation system must support device replacement without exchangeable medium.

  If the individual IO devices in the automation system do not support device replacement without exchangeable medium, a corresponding alarm is output for the IO device.

NOTE

Use only new IO devices as replacements or restore configured IO devices to their delivery state.

Activating/deactivating device replacement without exchangeable medium

The "Device replacement without exchangeable medium" function is activated in the IO controller by default.

To deactivate device replacement without exchangeable medium, follow these steps:

1. In the device or network view of the STEP 7, select the PROFINET interface in the corresponding IO controller.
2. In the interface properties under "Advanced options > Interface options", clear the "Support device replacement without exchangeable medium" check box.

To reactivate device replacement without exchangeable medium, you must select the "Support device replacement without exchangeable medium" check box again.

7.9.3 Permit overwriting of PROFINET device name

With the option "Permit overwriting of PROFINET device names of all assigned IO devices", you can overwrite PROFINET device names of IO devices. This option reduces the effort during automatic commissioning, for example, when replacing a device.

Requirements

- IO controller supports the "Permit overwriting of device names of all assigned IO devices" option, for example CPU 1215C DC/DC/DC as of firmware version 4.0

How the "Permit overwriting of PROFINET device names of all assigned IO devices" option works

The IO controller (CPU) can overwrite the PROFINET device names of IO devices in the IO system when the "Permit overwriting of PROFINET device names of all assigned IO devices" option is enabled.

Multiple use IO systems can only be operated when this option is enabled. The IO controller checks prior to overwriting if the type of the IO device matches the configured type.

If the option is not selected, the IO controller cannot overwrite the device names of the IO devices. In this case, you must manually assign the PROFINET device name on the IO device if the PROFINET device name changes in the configuration or when a device is replaced, or delete the device names of the IO devices prior to an automatic commissioning.

Response during commissioning

Select the option "Permit overwriting of PROFINET device names of all assigned IO devices" only if the following requirements are fulfilled:

- All the configured IO devices are available.
- All IO devices are wired correctly in accordance with the topology configuration.
- No IO device is jumpered.

If configured IO devices are missing or are jumpered (partial commissioning), do not use the option.

You can also use the option for standard machine projects in which you adjust the configuration later via ReconfigIOSystem. Note that the valid configuration is always the one that was transferred to the IO controller in the control data record using the ReconfigIOSystem Mode:=2 instruction. As soon as you enable the reconfiguration with ReconfigIOSystem Mode:=3, the PROFINET device names are overwritten as defined in the data record.

⚠ CAUTION

Error at partial commissioning
If device names are assigned incorrectly during partial commissioning or incorrect wiring, these have to be deleted manually after a correction of the wiring in order to attain correct assignment of the device names.

Behavior during operation

As soon as you replace a device, the new device is overwritten with the configured PROFINET device name.

The PROFINET device name is not overwritten when the MAC address of the IO device is already actively being used in the project.

⚠ WARNING

Wrong PROFINET device name

When the "Permit overwriting of PROFINET device names of all assigned IO devices" option is enabled, incorrectly connected devices can be assigned an incorrect PROFINET device name from the configuration.

Depending on the connected I/O, there is risk of death, severe injuries or damage caused by malfunctions.

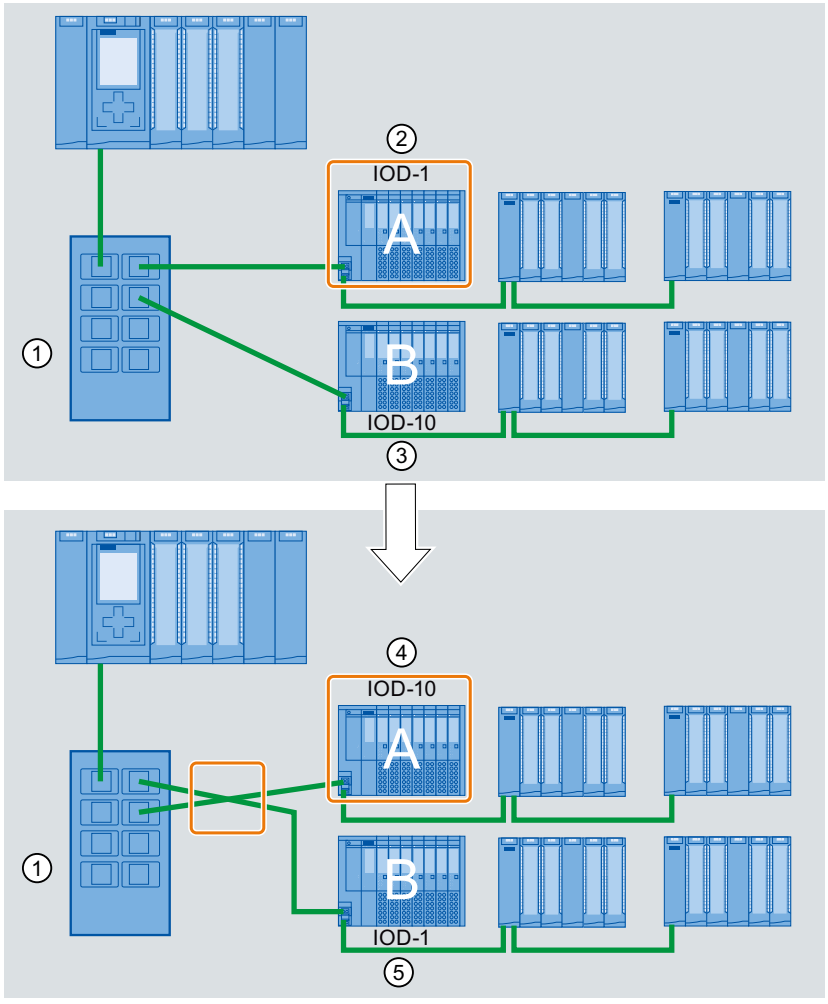
To rule out any danger, check whether the suitable replacement device has been connected in case of a device replacement and whether the port interconnection matches the configured preset topology.

Typical source of danger

When replacing an IO device ("standard case"), it is almost guaranteed that the replaced device will be connected according to the configured port interconnection.

The figure below shows a scenario whereby the connections of two identical PROFINET cables are swapped at two switch ports. Because the IO controller assigns the device names according to the preset topology, the incorrect connection of the devices has serious effects on the naming.

Due to the control of different actuators, the plant could become hazardous in this case.



① Switch with connected PROFINET cables
② Device A, device name "IOD-1": controls motor 1
③ Device B, device name "IOD-10": controls motor 10
④ Device A controls motor 10!
⑤ Device B controls motor 1!

Procedure

Proceed as follows to change the "Permit overwriting of PROFINET device names of all assigned IO devices" option:

1. Select the PROFINET interface of the CPU for which you want to change the option in the network view or in the device view.
2. Select the area "Advanced options", section "Interface options".
3. Change the option.

7.10 Standard machine projects

Introduction

Standard machine projects are STEP 7 projects that use a set of innovative functions allowing simple configuration and commissioning of flexible automation solutions for standard machines or for machines with a modular structure.

A hardware configuration consisting of an IO controller and any number of connected IO devices represents a "PROFINET IO system master". This master is configured with a maximum configuration based on a template from which various options can be derived for different standard machines, for example with different configuration variants of the IO system.

Greater flexibility at all levels

Standard machine projects have the following central characteristics:

- Different variants of a standard machine can be loaded from precisely one project with an engineered maximum configuration (IO system options). The standard machine project covers all variants (options) of the IO system.
- An IO system option can be integrated in an existing network locally using simple tools.

Flexibility is provided in more ways than one:

- With suitable configuration, adaptation of the IP address parameters of the IO controller is possible locally using simple tools. This allows a standard machine to be integrated in different plants with little effort or to be included in a network several times.
  IO systems with this property are known as **multiple use IO systems**.
- With suitable configuration and programming, different setups of IO system options can be operated locally that differ in terms of the selection of IO devices used or in terms of the arrangement of the IO devices.
  Since the specific configuration of the IO system is controlled by the user program, this is known as **configuration control for IO systems**.
- Independently of the functions described above, with suitable configuration and programming, you can use different station options of central devices or distributed I/O devices in one project. The devices can be different in terms of the selection and arrangement of the modules.
  Since the concrete configuration of the station is controlled by the user program, this is also known as **configuration control at the device layer**.

Application examples

You can find application examples for configuration control at the device layer, configuration control for IO systems and multiple-use IO systems on the Internet (https://support.industry.siemens.com/cs/ww/en/view/29430270).

Additional information

For more information on multiple use IO systems, refer to section Multiple use IO systems (Page 265).

For more information on the configuration control for IO systems, refer to section Configuration control for IO systems (Page 273).

For more information on configuration control, refer to the system manual S7-1500, ET 200MP (http://support.automation.siemens.com/WW/view/en/59191792).

7.10.1 Multiple use IO systems

7.10.1.1 What you should know about multiple use IO systems

Multiple use automation solutions

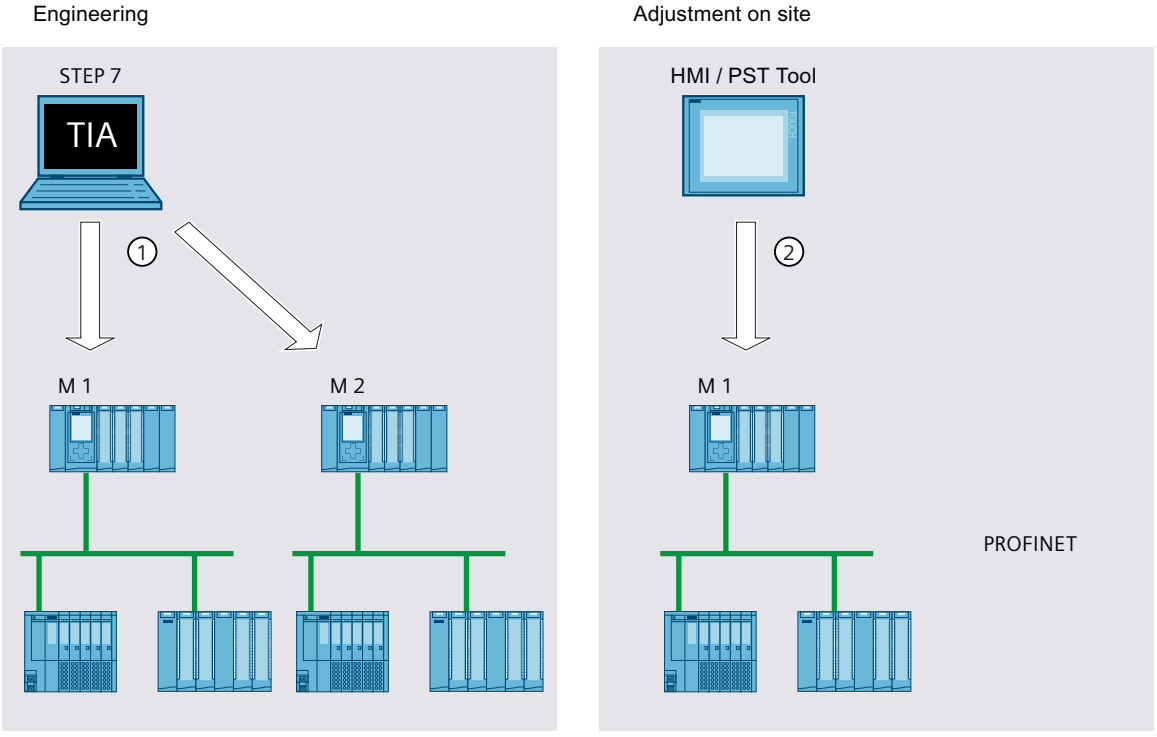
For a flexible reusable automation solution as is the case with series machines, the following use cases are typical:

- The machine (and therefore also the PROFINET IO system) is used more than once by the customers.
- The machine is used in different plants by various customers.

For this to be possible, the automation solution must meet the following requirements:

- A project (configuration and program) can be loaded on various machines of the same type without changes.
- Only a few easy adaptations need to be performed locally to integrate the machine into an existing network infrastructure.

The following figure shows how an automation solution with a multiple use IO system is loaded on different automation systems and then one automation system is adapted to the existing network infrastructure locally.



① Load configuration with multiple use IO system
② Set IP address and device name locally on the IO controller

Figure 3-444 "Multiple use IO system" principle

Principle

The automation components for a machine include a PROFINET IO system, consisting of an IO controller (PROFINET interface of a CPU) and the IO devices assigned to it.

With the "Multiple use IO system" setting for the IO system, you turn a STEP 7 project into a "Standard machine project".

The "Multiple use IO system" setting triggers various settings and checks of the configuration by STEP 7. The settings ensure that the IO system is self-contained and there are no dependencies on components outside the IO system.

Requirements

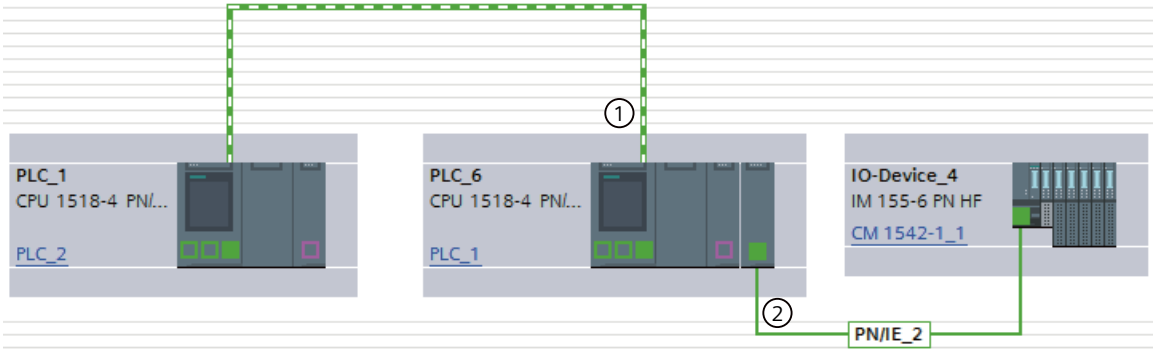
- STEP 7 as of V13
- The IO controller supports the "Multiple use IO system" function, for example a CPU 1512SP-1 PN as of firmware version 1.6.

Rules

The following rules apply to a multiple use IO system:

- No IO device can be configured as shared device.
- The ports of the devices must be interconnected.
  Devices for which no port interconnection is configured, for example, interface module IM 154-6 IWLAN (ET 200pro PN), cannot be operated with STEP 7 V13 as IO devices on a multiple use IO system.
- If an IO device in a multiple use IO system is an I-device (CPU as an "intelligent" IO device):
  - If the I-device has a lower-level IO system, this I-device cannot be connected to the same PROFINET interface as the higher-level IO controller.

    Note: If the I-device is configured using a PROFINET GSD, STEP 7 cannot check for compliance with this rule. In this case, you are responsible for ensuring compliance with the rule.



① I-device in multiple use IO system. The PROFINET interface is operated as IO device. No other IO system is connected here.

② A lower-level IO system on the I-device is connected to another PROFINET interface.

Figure 3-445 Example configuration for "Multiple use IO system" with I-device

  - The PROFINET interface of the I-device must be set to "Parameter assignment of PN interface by higher-level controller".
- If MRP (Media Redundancy Protocol) is configured:
  - All IO devices on the multiple use IO system must belong to the same MRP domain.
- If IRT (Isochronous Real Time) is configured:
  - All IO devices in multiple use IO systems must belong to the same sync domain.
  - The sync domain must not include any other IO devices.
- IE/PB Links cannot be operated as an IO device in a multiple use IO system with STEP 7 V13.

Configuration

You specify whether or not a configuration can be used multiple times in the properties of the IO system.

All other parameter settings for the configured devices are then set automatically by STEP 7 and checked during compilation.

Boundary conditions

To prevent a standard machine project from having dependencies on other devices outside of the machine, observe the following:

- A standard machine project consists of an IO controller and the corresponding IO devices. You should therefore configure only one CPU as IO controller and the corresponding IO devices in the standard machine project.
- Do not use connection configured at both ends for the communication. Instead, use only a connection configured at one end or unspecified connections if necessary.

  Background: To configure the communication in a STEP 7 project, it is always possible to set the IP address parameters in the project. For multiple use IO systems, however, this strategy is not possible since the IP address parameters of the IO controller and the assigned IO devices are assigned locally. At the time of the configuration, the IP address parameters are therefore unknown.

  If you nevertheless want to configure communication with devices on PROFINET, for example with a central coordinator, you can only use communications mechanisms that allow dynamic assignment of the IP address parameters in the user program.

  Example: Open User Communication

  If, for example, the device is configured as an active end point (initiator of the connection), the IP address parameters can be stored, for example, in a data block. You then supply the data block with the currently valid IP address parameters during commissioning. For this dynamic type of IP address parameter assignment, there is no system support; in other words, if you change the configuration of the system, the IP address parameters are not automatically adapted.

  You will find a description of handling instructions for Open User Communication under this keyword in the STEP 7 online help.

7.10.1.2 Configuring multiple use IO systems

Requirements

- STEP 7 as of V13
- The IO controller supports the "Multiple use IO system" function, for example a CPU 1512SP-1 PN as of firmware version 1.6.

Procedure

The configuration of a series machine using an S7-1500-CPU as an example is described below.

To create a standard machine project, follow these steps:

1. Create a project.
2. Configure a CPU as the IO controller, for example a CPU 1518-4 PN/DP as of firmware version 1.5.
3. Configure the required IO devices and assign the IO devices to the IO controller.
4. Configure the port interconnection between the devices.

5. Select the IO system so that you can edit the properties in the inspector window.
6. Select the "Multiple use IO system" check box in the "General" area of the inspector window.

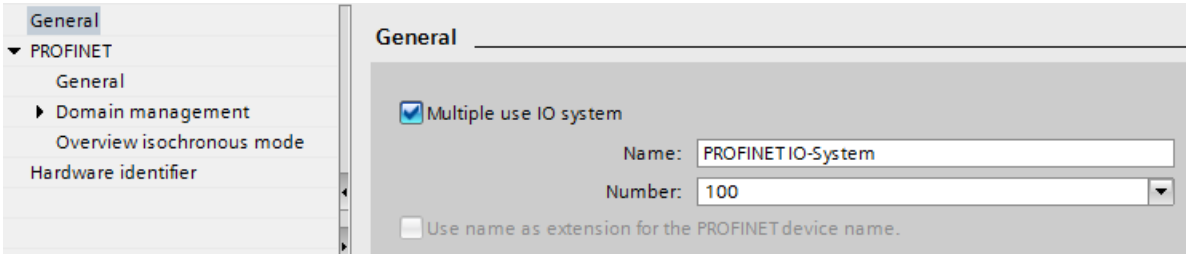


Figure 3-446 Activate "Multiple use IO system"

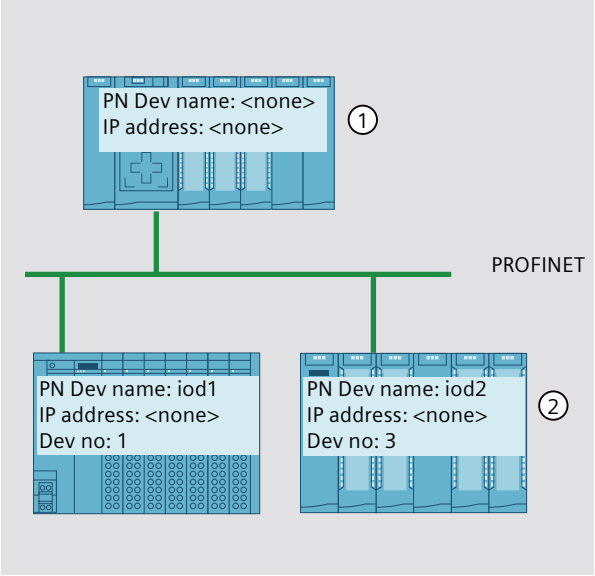
Result: The following settings are made by STEP 7:

- The device name of the IO controller (CPU) in the standard machine project is set to "PROFINET device name is set directly at the device". The IO controller (CPU) has no PROFINET device name initially.
- The IP protocol of the IO controller (CPU) is set to "IP address is set directly at the device". The CPU has no IP address initially.
- The "Support device replacement without exchangeable medium" option is selected automatically. This option enables automatic commissioning. A commissioning engineer does not have to assign device names to the IO devices locally. The IO controller assigns the device name and IP address to the IO devices based on the preset topology and other settings during startup.
- The device name of the IO devices is set to "Generate PROFINET device name automatically" (from the configured name of the IO device).
- The IP protocol of the IO devices is set to "IP address is set by the IO controller during runtime". The IO devices have no IP address initially. If an IO device is not a typical distributed I/O system (e.g., ET 200 systems), but rather another device such as an HMI device, change the option to "IP address is set directly at the device"; see below.
- The device number for the IO devices is automatically assigned and is used locally for making the IP address unique.

The option "Permit overwriting of PROFINET device name" must be selected (CPU parameters, properties of the PROFINET interface, Ethernet addresses area) so that the IO controller can adapt the device name later at the operator.

This option is disabled by default.

The following figure shows the above-described settings for the IP address and PROFINET device name.



① After the configuration is loaded from the standard machine project, the IO controller has no device name and no IP address.

② Following loading, the IO devices have a device name and a device number but no IP address.

Figure 3-447 Settings for the IP address and the PROFINET device name

How an IO device obtains an IP address locally

Below, you will find an explanation of the "IP address is set by the IO controller during runtime" and "IP address is set directly at the device" options, which can generally be configured for a multiple use IO system.

If you have set the "Multiple use IO system" option for the IO system, STEP 7 automatically sets the "IP address is set by the IO controller during runtime" option for the IO devices.

In this case, the IO controller assigns the IO device an IP address that results from the locally assigned IP address of the IO controller (see next section). This option is appropriate if the IO device is a field device, e.g., ET 200MP, ET 200SP, ET 200AL, or another distributed I/O system.

If the IO device is not a "standard" field device, for example, an HMI device for a Windows operating system, the "IP address is set by the IO controller during runtime" option described above does not work. In this case, choose the "IP address is set directly at the device" option. You must then assign the IP address to the device locally and take steps to ensure that this address is suitable for the IP addresses of the other IO devices and the IP address of the IO controller.

7.10.1.3 Adapt multiple use IO systems locally

A few steps are needed to adapt the machine that was loaded with the standard machine project.

Only the device name and IP address of the IO controller must be adapted locally. The device names and IP addresses of the IO devices result from these adaptations. In this example, the effects of local settings are described for two specific machine modules.

The local settings are possible, for example, with the CPU display and commissioning tools such as Primary Setup Tool (PST) or PRONETA. You do not need a programming device with STEP 7 to make these settings, even though it is possible to do so.

Requirement

- The machine was loaded with a standard machine project (see Configuring multiple use IO systems (Page 268)).
- The display is ready for operation and the desired tool for assigning the IP address and device name is available (e.g., PST Tool, STEP 7).
- The ports of the IO controller and IO devices are interconnected according to the configuration.

Procedure

Observe the boundary conditions and instructions for commissioning an S7-1500. For more information on commissioning an S7-1500 CPU, refer to the system manual S7-1500, ET 200MP (http://support.automation.siemens.com/WW/view/en/59191792).

To adapt a standard machine locally, follow these steps:

1. Integrate the machine into the network.
2. Connect the device for assigning the IP address and device name to the CPU, for example a PG/PC with the appropriate software.
3. Assign the desired device name and IP address to the IO controller.

NOTE

Remove DCP write protection when assigning via PG/PC

If write protection is enabled for DCP (Discovery Configuration Protocol), you cannot change the device name and IP address via PG/PC.

You can find information on assigning in the section Assigning a device name and IP address (Page 60). You can find information on handling DCP in the section PROFINET Security Class 1 (Page 36).

4. Start up the CPU.

The IO controller then assigns the adapted PROFINET device name and a unique IP address to the IO devices.

The following rules apply to the assignment:

- The device names of the IO devices are formed by chaining together the following name components, separated by a period:
  <configured name of the IO device from the standard machine project>.<name of the associated IO controller set on the device>
- The IP addresses of the IO devices result from the locally configured IP address of the associated IO controller and the device number (sum).

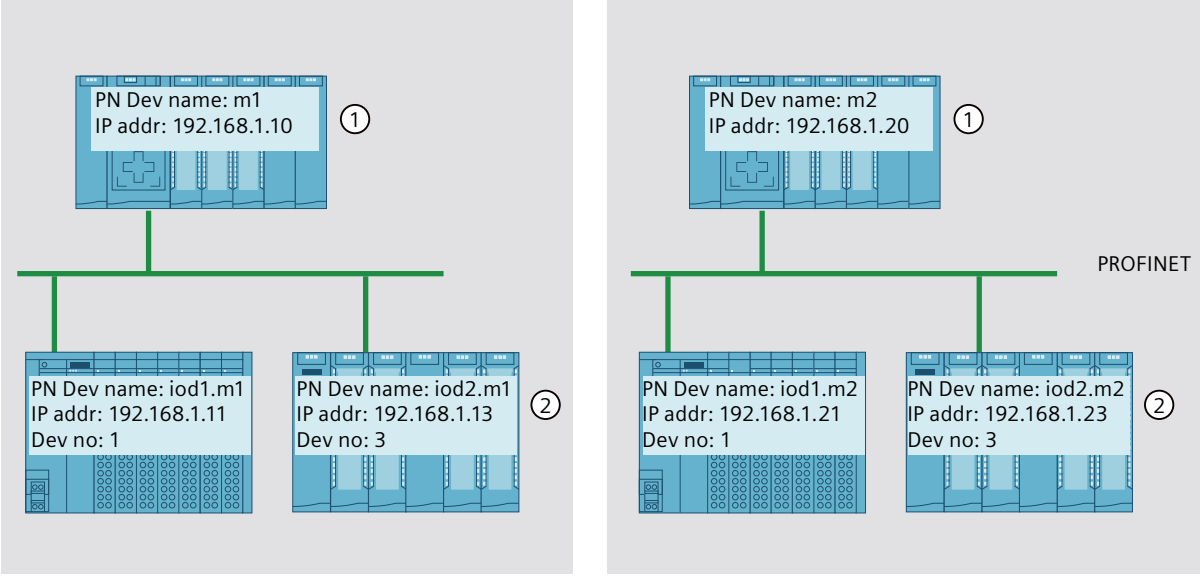
NOTE

Make sure that duplicate IP addresses cannot be created on the subnet during the assignment. The IO controller does not assign a new IP address in this case.

In the following figure, the device name "m1" and the IP address 192.168.1.10 have been assigned to the IO controller of the first machine.

The device name "m2" and the IP address 192.168.1.20 has been assigned for the second machine.

Refer to the figure for the resulting device names and IP addresses.



① Set device name and IP address on the IO controller

② After startup, the IO devices have an updated device name (<configured device name>.<device name of IO controller>) and an adapted IP address (= <IP address of IO controller> + <device number>)

Figure 3-448 Example of the assignment of IP addresses and device names at "Multiple use IO system"

See also

Configuring multiple use IO systems (Page 268)

7.10.2 Configuration control for IO systems

7.10.2.1 Information about configuration control of IO systems

Configuration control of IO systems makes it possible to generate several concrete versions of a standard machine from a standard machine project.

You are given the flexibility to vary the configuration of an IO system for a specific application as long as the real configuration can be derived from the set configuration. The configured configuration therefore represents the superset of all real configurations that can be derived from it.

The following figure shows an example of how two IO systems with a different number of IO devices arise from one standard machine project.

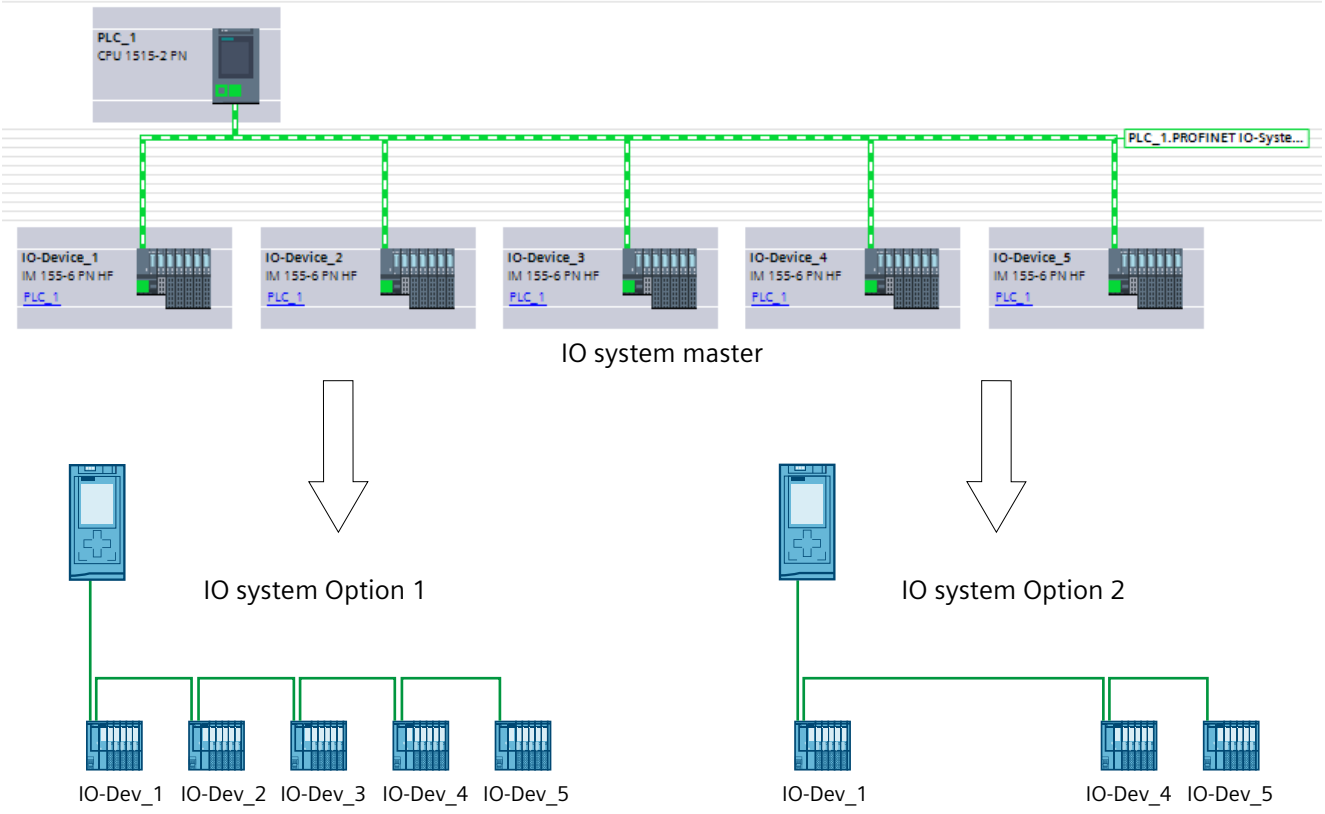


Figure 3-449 Example of configuration control for PROFINET IO systems

In the following sections, you find a description of how to configure and program a PROFINET IO system to commission, for example, a standard machine on-site without using configuration software.

Concept

The principle of configuration control is already known at the device level for the flexible use of submodules/modules ("option handling"). Different configurations can be derived from one engineering project both for central as well as for distributed I/O.

With S7-1500 CPUs as of firmware version V1.7, this principle can also be applied at the IO system level. You have the option of omitting, adding or changing the order of stations (IO devices) of a PROFINET IO system in a specific plant.

Configuration control for devices and configuration control for IO systems can be combined; the functions are independent of each other.

It is possible to operate variants deviating from a maximum configuration of an IO system. In a standard machine project, you can prepare a kit of IO devices which can be flexibly customized for various configurations using configuration control.

The following variations are available:

- Variation of the number of IO devices involved

  You include optional IO devices for the configuration control in the configuration by transferring a suitable data record with the required configuration in the user program.
- Variation of the order of IO devices involved

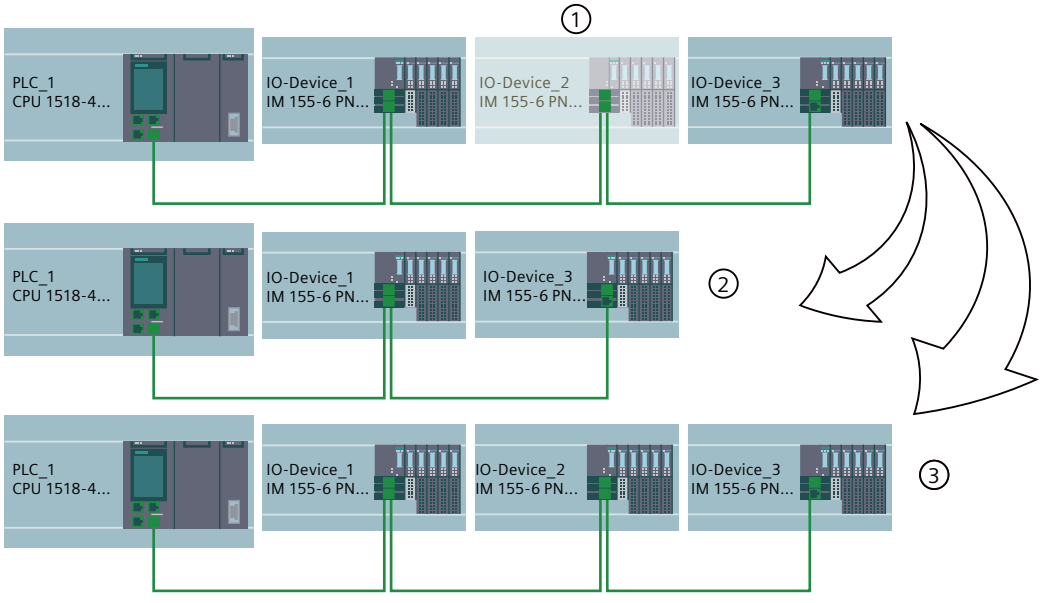
  You adapt the port interconnection of the IO devices to the topology being used by transferring a suitable data record with the required topology in the user program.

The following figure shows how you serve two different configurations with an IO device marked as optional in the network view of STEP 7.

- Configuration without the optional IO device:

  In this case, you use the instruction "ReconfigIOSystem" to transfer a data record to the PROFINET interface containing the information that no optional IO device is to be included in the configuration.
- Configuration with the optional IO device:

  In this case, you use the instruction "ReconfigIOSystem" to transfer a data record to the PROFINET interface adding the optional IO device to the configuration.



① Determined through parameter assignment: IO Device_2 is optional IO device
② Configuration without the optional IO device
③ Configuration with the optional IO device

Figure 3-450 Example configuration with "Optional IO device" and the associated configuration options

Summary: The procedure in principle

The following phases are distinguished when it comes to the implementation of a standard machine concept:

1. Engineering phase: Creating a standard machine project and loading into specific machine or plant:
   - Completely configuring all IO devices (options) ever required in a specific machine or plant
   - Configuring as optional those IO devices that will be omitted in specific machines or plants
   - Preparing user program (see Configuring flexible order of IO devices (Page 282)) with the possibility of selecting on-site the actually existing configuration via switch or HMI device
2. Commissioning phase: Preparing specific machine or plant for operation:
   - Integrating machine or plant in the on-site network (see Adapt multiple use IO systems locally (Page 271))
   - Selecting the currently existing configuration of the IO system via configured option

7.10.2.2 Configuring IO devices as optional

Requirements

- IO controller supports configuration control for IO systems, for example CPU 1516-3 PN/DP as of firmware version 1.7
- STEP 7 V13 SP1 or higher
- The rules (Page 287) for the establishment and operation of a standard machine project have been considered.

Port interconnection

As of STEP 7 V15.1, port interconnection is not necessary for optional IO devices.

A port interconnection between the devices of the IO system that you want to customize with the user program is mandatory in the following cases.

- You have configured IRT.
- You have configured MRP.
- You are using STEP 7 <= V15.

Procedure

To configure an IO device as optional IO device, proceed as follows:

1. Create a project.
2. Configure an S7-1500 CPU firmware version V1.7 or higher as IO controller.
3. Configure the required IO devices and assign the IO devices to the IO controller.
4. Select the IO device you want to mark as optional.

5. Select the area "PROFINET interface [X1]" > Advanced options".
6. Enable the "Optional IO device" option.

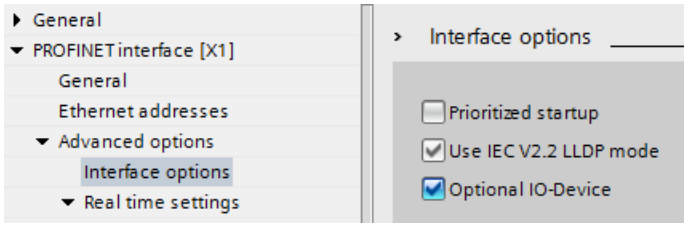


Figure 3-451 Configure the IO device as an optional IO device

7. Repeat steps 4 to 6 for all IO devices to be configured as optional.
8. Load the configuration onto the CPU.

Result: Once this configuration is loaded, the system behavior is as follows:

- The CPU is prepared for the configuration control of the IO system.
- All IO devices are disabled.
- Irrespective of whether you customize the configuration with the user program (adding optional IO devices) or make no changes to the loaded configuration: You must call the instruction "ReconfigIOSystem" in the user program and notify the current configuration to the system!

  The system will not be operational without calling the instruction "ReconfigIOSystem".

  For further information on the proceeding see Enabling optional IO devices in the program (Page 276).

Fast parameter assignment in the "IO communication" table

You can also specify whether or not an IO device is optional in the "IO communication" tab.

In an additional "Optional IO device" column, a selectable check box is available for each IO device that indicates whether or not an IO device is optional. Here, you can adjust the setting centrally.

7.10.2.3 Enabling optional IO devices in the program

Requirements

- IO controller supports configuration control for IO systems, for example CPU 1516-3 PN/DP as of firmware version 1.7
- STEP 7 V13 SP1 or higher
- At least one IO device was configured as optional IO device.
- The rules (Page 287) for the establishment and operation of a standard machine project have been considered.

Procedure

Observe the information on and rules for commissioning in the documentation for SIMATIC S7-1500, for the ET 200SP CPUs and for the CPU 1516pro-2 PN.

The following description of the proceeding only includes steps required to understand the program-controlled activation of an optional IO device.

To activate or deactivate IO devices, follow these steps:

1. Create a data record "CTRLREC" for the instruction "ReconfigIOSystem". You can find information on the structure of the data record in the STEP 7 online help.
2. Call the instruction "ReconfigIOSystem" and select MODE 1 to deactivate all IO devices.

   If you set the CPU to STOP or POWER OFF state in order to modify the plant in this status (for example to add an optional IO device), explicit deactivation using "ReconfigIOSystem" with mode 1 is not necessary. In this case, i.e. following a STOP-RUN transition and following a POWER-OFF > POWER-ON transition, all IO devices are deactivated automatically.
3. When you have brought the plant to a safe status that allows restructuring without any danger:

   Put the plant together according to your intended application. Add the required optional IO devices at the points at which you planned this in the configuration (observe the order!) or remove optional IO devices that you no longer require.
4. Network the IO devices.
5. Startup the S7-1500 system and call again the instruction "ReconfigIOSystem". Select MODE 2 to transfer the data record CTRLREC.
6. Following successful transfer of the data record, call again the instruction "ReconfigIOSystem". Select MODE 3 to activate all IO devices forming part of the current configuration.

   Result: The CPU **activates** the following IO devices:
   - All IO devices that you have not set as optional IO devices.
   - All optional IO devices listed in the control data record (CTRLREC).

   The following IO devices remain **disabled**:
   - Docking units (IO devices changing during operation).
   - Optional IO devices that are not listed in the control data record.

NOTE

Call the instruction "ReconfigIOSystem" for all values of the parameter MODE with the same control data record (CTRLREC)!

If you use different data records for the values of the MODE parameter, this results in an inconsistent customization of the configuration and thus to rather incomprehensible error messages.

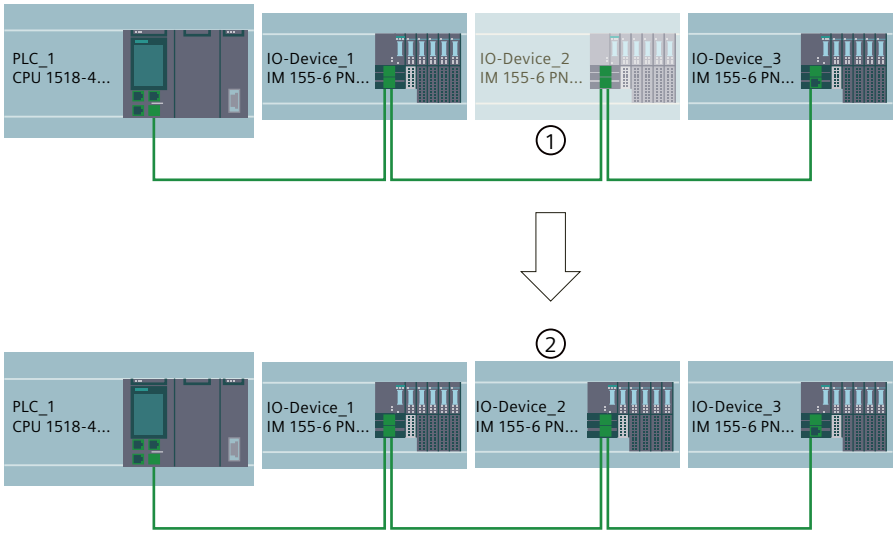
Example: Data record structure for the activation of an IO device

The IO device "IO-Device_2" is to be activated as the only IO device in the user program.

To do this, you only require the hardware identifier of "IO-Device_2".

Recommendation: Use the system constants of the hardware identifiers instead of the absolute values as shown in this example. With this procedure, the content of the DB is not influenced by changes to the hardware identifiers as the result of changes to the configuration.

The data record is to be stored in a data block and to be transmitted to the PROFINET interface of the IO controller in the user program using the instruction "ReconfigIOSystem".



① IO device_2 is configured as optional IO device.

② Once the data record is transmitted and the configuration is activated using the instruction "ReconfigIOSystem" IO device_2 is included in the configuration and participates in the data exchange with the IO controller.

Figure 3-452 Example: Activating an optional IO device

Creating data block

In this example, the control data record is created in a data block. The data block is structured as follows:

Line 2: Array definition: Array of type Word with 4 elements. Array of Word is permitted as the data type.

Line 3: Version of the data record (currently: V1.0).

Line 4: Number of optional IO devices to be activated (here: 1).

Line 5: List of the hardware identifiers of the IO devices, inserted here as system constants.

Line 6: Number of port interconnections that are set in the user program (here: 0).

Line 7: Additional data records (optional)

myCTRLREC

	Name	Data type	Start value	Comment
1	Static			
2	ArrMachineConfig0	Array[0..3] of Word		Array for one optional IO device
3	ArrMachineConfig0[0]	Word	16#0100	
4	ArrMachineConfig0[1]	Word	16#0001	
5	ArrMachineConfig0[2]	Word	"IO-Device_2~IODevice"	
6	ArrMachineConfig0[3]	Word	16#0000	
7	ArrMachineConfig1	Array[0..8] of Word		

Figure 3-453 Data block with control records

Parameter MODE of instruction "ReconfigIOSystem"

You control how the "ReconfigIOSystem" instruction works with the MODE parameter.
The following values are possible for the MODE input parameter:

MODE	Description
1	All IO devices of the IO system can be disabled by calling the instruction with MODE 1. The "ReconfigIOSystem" instruction uses the "D_ACT_DP" instruction internally. "ReconfigIOSystem" returns errors that are detected by D_ACT_DP in the following output parameters: • STATUS (error code) • ERR_INFO (hardware identifier of the IO device causing the error). In STATUS and ERR_INFO, the CPU enters the last determined error/HW identifier and in so doing overwrites an existing error code. For this reason, additional errors can be present besides the entered error.
2	For controlling the actual configuration of the IO system, the instruction transfers the data record to the PROFINET interface, which is addressed with LADDR block parameter (HW identifier of the PROFINET interface).
3	All non-optional IO devices in the IO system and optional IO devices that are listed in the control data record CTRLREC are enabled. The optional IO devices that are **not** listed in the CTRLREC data record remain disabled. If IO devices that are part of docking units (alternating IO devices in operation) are listed in the CTRLREC control data record, the PN IO system reacts as follows: • IO devices of the docking units remain disabled when ReconfigIOSystem is called with MODE 3. This reaction corresponds to the reaction of a configuration without configuration-controlled IO devices. IO devices of docking units are disabled by default and must be enabled in the user program. For more information on docking units, refer to the section Docking systems (Page 291).

Rules for the call sequence of "ReconfigIOSystem"

- Always supply the instruction "ReconfigIOSystem" with the same control data record (CTRLREC input parameter)!
- Call sequence following POWER OFF -> POWER ON transition:
  - ReconfigIOSystem call with MODE 1 (optional).
  - ReconfigIOSystem call with MODE 2 (mandatory, even without previous reconfiguration!).
  - ReconfigIOSystem call with MODE 3 (mandatory).
- Call sequence following STOP > RUN transition:
  - ReconfigIOSystem call with MODE 1 (optional).
  - ReconfigIOSystem call with MODE 2 (mandatory, even when configuration was modified in STOP state). Otherwise not required).
  - ReconfigIOSystem call with MODE 3 (mandatory).
- Call sequence for reconfiguration in RUN state:
  - ReconfigIOSystem call with MODE 1 (mandatory).
  - ReconfigIOSystem call with MODE 2 (mandatory).
  - ReconfigIOSystem call with MODE 3 (mandatory).

Explanations and recommendations concerning the rules

- If you do not list an IO device to be configured as optional IO device in the control data record or data block resp. this IO device does not form part of the configuration and does not take part in data exchange with the CPU.
- If you do not activate any optional IO device at all and work with the loaded configuration without reconfiguration, you still have to follow the proceeding described in the above section and transmit the control data record to the CPU.

  The control data record has the simple structure with the following tags:
  - Version (High Byte =1, Low Byte = 0)
  - Number of optional devices to be activated = 0
  - Number of port interconnections that are set in the user program = 0
- Following a STOP > RUN transition and following a POWER-OFF > POWER-ON transition, all IO devices are deactivated automatically. For this reason, no ReconfigIOSystem call with MODE 1 is required for configuration control to function properly.

  If you use your project as a universally valid sample for programming the configuration control, we still recommend to perform the ReconfigIOSystem call with MODE 1 prior to any reconfiguration. This way, the sample can also be used for reconfigurations in RUN mode.
- Commissioning extensive I/O systems (more than 8 optional IO devices) while using IRT at the same time:

  To keep the startup times short when activating the optional IO devices (ReconfigIOSystem, mode 3), note the following tip: Check the device numbers of the IO devices. The device numbers should follow the topological interconnection starting at the IO controller in ascending order. The further an IO device is from the IO controller topologically, in other words the more IO devices there are between the IO controller and the IO device in question, the higher the device number should be.

You set the device numbers in the "Ethernet addresses - PROFINET" area in the Inspector window with the PROFINET interface selected.

Example of the assignment of device numbers with a linear topology:

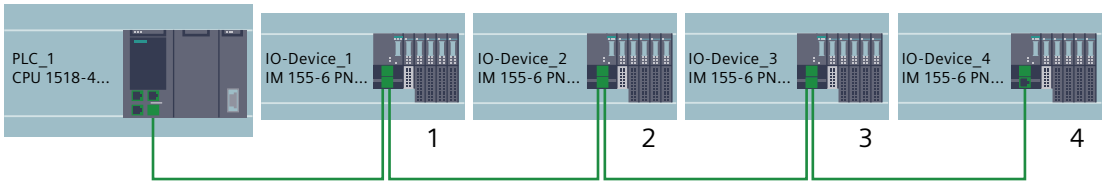


Figure 3-454 Example: Device numbers in a line topology

- The CPU processes the instruction "ReconfigIOSystem" to transfer the control data record asynchronously.

  For this reason, you must call "ReconfigIOSystem" in a loop repeatedly when calling the instruction in the startup program until the output parameter "BUSY" or "DONE" indicate that the data record has been transferred.

  Tip: To program the loop, use the SCL programming language with the instruction REPEAT ... UNTIL.

```
REPEAT
    "ReconfigIOSystem"(REQ := "start_config_ctrl",
                       MODE := 1,
                       LADDR := 64,
                       CTRLREC := "myCTRLREC".ArrMachineConfig0,
                       DONE => "conf_DONE",
                       BUSY => "conf_BUSY",
                       ERROR => "conf_ERROR",
                       STATUS => "conf_STATUS");
UNTIL NOT "conf_BUSY"
END_REPEAT;
```

Additional information

For information on the basic structure of the data record and on using the instruction "ReconfigIOSystem" see the STEP 7 online help.

See also

Configuring IO devices as optional (Page 275)

7.10.2.4 Configuring flexible order of IO devices

The following section shows how you can create the conditions required to change the order of IO devices in a PROFINET IO system.

This function is also supported with optional IO devices. For simplicity, a maximum configuration without optional IO devices is shown below.

Concept

A typical application for a standard machine project consists of composing an entire plant from a set of various plant units which only differ with respect to the different arrangement of the units, e.g. in the case of transport systems. Each plant unit consists of a functional unit of mechanics (rails or conveyor belts) and electrics (power supply, IO device with IO modules, sensors, actuators, motors, PROFINET port for data exchange with central control ...).

The following figure shows how, simply by exchanging two rail segments, a new transport system is created that is adapted with an upstream points to the local conditions.

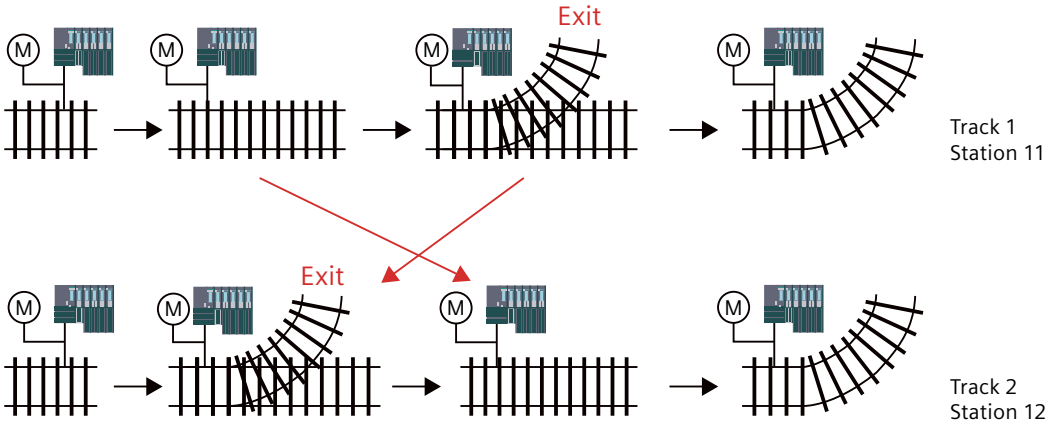


Figure 3-455 Example: Changing the arrangement of IO devices

From the automation viewpoint, no change in the project is required for the flexible adjustment of the PROFINET configuration.

The order of the IO devices is determined by the port interconnection. For each IO device, you define in the port properties the partner port and thus the neighboring device connected at the respective local port. If the partner port is to be defined by the user program, the option "Partner set by user program" is to be selected as partner port.

The figure below shows the initial configuration of the transport system shown above, which is to permit the order of the connected IO devices to be changed via the user program. In the example, the order of IO-Device_2 and IO-Device_3 is to be controlled via the user program.

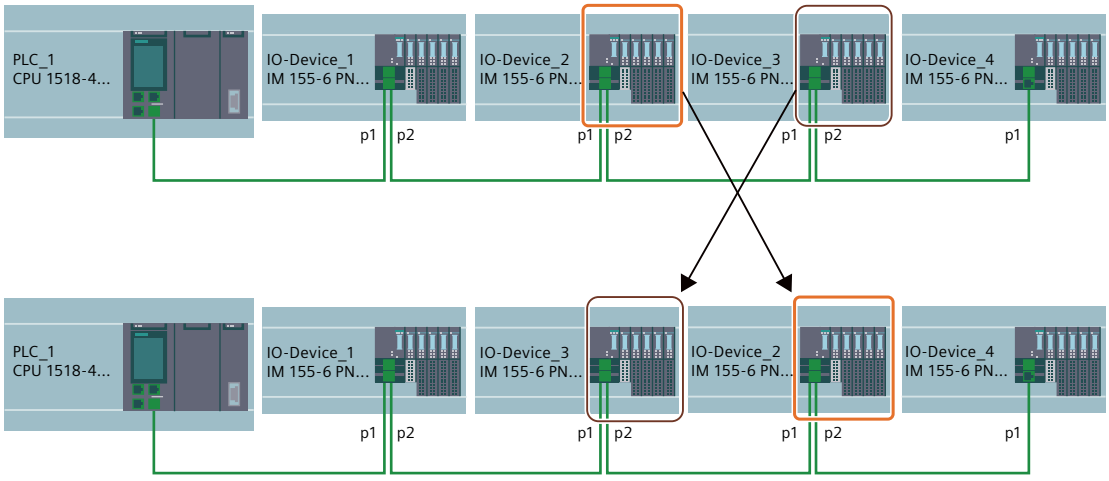


Figure 3-456 Example configuration: Configuring flexible order of IO devices

To determine how the partner port settings are to be selected, you must note for each device and each port of a device which partner can be interconnected.

- If the partner is always the same in the different configurations provided, you select the partner port for this partner.
- If the partners vary in the different configurations, you select "Setting partner by user program".

For the example in the figure above, the following port settings result:

Device	Local port	Partner port setting	Explanation
PLC_1	p1	p1 (IO device_1)	Partner of PLC_1 at port 1 is IO device_1 (always)
IO device_1	p1	p1 (PLC_1)	Partner of IO device_1 at port 1 is PLC_1 (always)
IO device_1	p2	Partner is set by user program	Partner of IO device_1 at port 2 is either IO device_2 or IO device_3 => Setting partner by user program
IO device_2	p1	Partner is set by user program	Partner of IO device_2 at port 1 is either IO device_1 or IO device_3 => Setting partner by user program
IO device_2	p2	Partner is set by user program	Partner of IO device_2 at port 2 is either IO device_3 or IO device_4 => Setting partner by user program
IO device_3	p1	Partner is set by user program	Partner of IO device_3 at port 1 is either IO device_2 or IO device_1 => Setting partner by user program

Device	Local port	Partner port setting	Explanation
IO device_3	p2	Partner is set by user program	Partner of IO device_3 at port 2 is either IO device_4 or IO device_2 => Setting partner by user program
IO device_4	p1	Partner is set by user program	Partner of IO device_4 at port 1 is either IO device_3 or IO device_2 => Setting partner by user program
IO device_4	p2	Any partner	No partner planned at port 2

Requirement

- IO controller supports configuration control for IO systems, for example CPU 1515-2 PN as of firmware version 1.7
- STEP 7 V13 SP1 or higher
- The rules (Page 287) for the establishment and operation of a standard machine project have been considered.

Procedure

To set the partner port for a program controlled interconnection, proceed as follows:

1. Select the PROFINET interface of the device (IO controller or IO device) whose port you want to set.
2. In the properties of the PROFINET interface, select the area "Port interconnection" (Extended options > Port [...] > Port interconnection).
3. From the drop-down list, select "Setting partner by user program" as partner port.
4. Repeat steps 1 to 3 for each port to be interconnected via the user program.

See also

Customizing arrangement of IO devices in the program (Page 284)

7.10.2.5 Customizing arrangement of IO devices in the program

Requirements

- IO controller supports configuration control for IO systems, for example CPU 1516pro-2 PN as of firmware version 1.7 as an IO controller
- STEP 7 V13 SP1
- At least one partner port was configured as "Partner set by user program".
- The rules (Page 287) for the establishment and operation of a standard machine project have been considered.

Procedure

The proceedings corresponds to the proceeding for activating optional IO devices.

Only the structure of the data record must be extended for the program-controlled assignment of the ports. The extension is described in the following sections.

Example: Data record structure for the assignment of partner ports

For the data record structure, you need the HW identifications of the ports.

The data record is to be stored in a data block and to be transmitted to the PROFINET interface of the IO controller in the user program using the instruction "ReconfigIOSystem".

As the input parameter RECORD of the instruction "ReconfigIOSystem" is of the VARIANT data type, you first have to create a data type for the data block.

In the following sections, you find a description of the structure of the PLC data type as well as of the structure of the data block based on this type.

Selecting derived configuration

For the following selected configuration it is shown below what the data record must look like so that the IO devices are interconnected in the planned order by the user program.

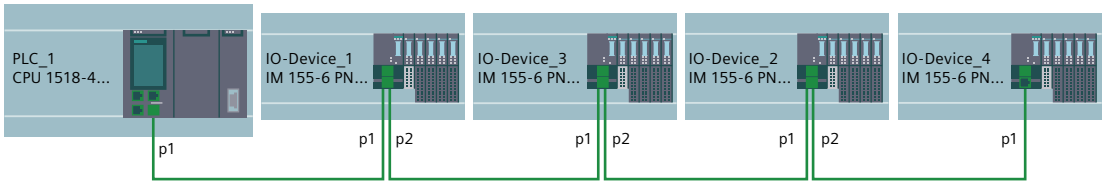


Figure 3-457 Example configuration: Customizing arrangement of IO devices in the user program

This example is based on the flexible configuration from the previous section (Page 282) with the settings for the respective partner ports described there.

The partner ports in the specific derived configuration have been defined so that it is possible to name the HW identifications of the ports involved.

The following table only contains those devices whose ports can be defined by the user program. Only these devices are relevant for the data record structure.

Device	Local port	Partner port setting	Partner port of the selected configuration
IO device_1	p2 = Port 2 HW identifier: 251	Partner is set by user program	Port 1 of IO device_3 HW identifier: 261
IO device_2	p1 = Port 1 HW identifier: 281	Partner is set by user program	Port 2 of IO device_3 HW identifier: 291
IO device_2	p2 = Port 2 HW identifier: 311	Partner is set by user program	Port 1 of IO device_4 HW identifier: 321

Creating data block

For the derived configuration, the structure of the data block "DB-IO-SYSTEM-Port-Interconnections" is explained as an example.

This data block is used when calling the instruction "ReconfigIOSystem" at input parameter "CTRLREC".

Instead of the absolute values for the hardware identifiers of the ports, the system constants of the hardware identifiers are used here.

The data block is structured as follows:

Line 2: Declaration of an Array of Word (only this data type is possible).

Line 3: Version of the control data record: V1.0.

Line 4: Number of optional IO devices: 0.

Line 5: Number of specified port interconnections: 3.

Line 6: Port interconnection 1, local port.

Line 7: Port interconnection 1, partner port.

Line 8: Port interconnection 2, local port.

Line 9: Port interconnection 2, partner port

Line 10: Port interconnection 3, local port.

Line 11: Port interconnection 3, partner port.

IO-SYSTEM-Port-Interconnections

	Name	Datentyp	Startwert	Kommentar
1	Static			
2	ArrMachineConfig	Array[0..8] of Word		data record for port interconn settings
3	ArrMachineConfig[0]	Word	16#0100	
4	ArrMachineConfig[1]	Word	16#0000	
5	ArrMachineConfig[2]	Word	16#0003	
6	ArrMachineConfig[3]	Word	"IO_device_1~PROFINET_interface~Port_2"	
7	ArrMachineConfig[4]	Word	"IO_device_3~PROFINET_interface~Port_1"	
8	ArrMachineConfig[5]	Word	"IO_device_2~PROFINET_interface~Port_1"	
9	ArrMachineConfig[6]	Word	"IO_device_3~PROFINET_interface~Port_2"	
10	ArrMachineConfig[7]	Word	"IO_device_2~PROFINET_interface~Port_2"	
11	ArrMachineConfig[8]	Word	"IO_device_4~PROFINET_interface~Port_1"	

Figure 3-458 Data block with data record for port interconnections

Interconnection not listed in data block

If the partner port was configured as "Setting partner by user program" in the port properties and this port is not listed in the data record or data block resp., then the CPU sets this port to the setting "any partner". If no data record is transmitted at all, the CPU sets this "any partner" setting for all program-controlled assignments.

Additional information

For information on the basic structure of the data record and on using the instruction "ReconfigIOSystem" see the STEP 7 online help.

7.10.2.6 System behavior and rules

Below, you find a description of how an IO system whose configuration is controlled by the user program behaves in operation.

In addition, rules and restrictions are listed here which must be considered when configuring the maximum structure of the configuration in a standard machine project.

System behavior

- System diagnostics:
  If an optional IO device is deactivated, the IO device is displayed as "deactivated" from the system diagnostics viewpoint (online view or Online & Diagnostics).
- Topology view:
  Offline view: As configured. No interconnection is shown for ports with partner ports configured as "Setting partner by user program".
  Online view: Ports and interconnections with deactivated IO devices are shown in a different shade of green as error-free ports and interconnections of activated IO devices.
- Representation in the Web server:
  The names of devices are shown as configured (Properties > General > Project information).
  The assigned PROFINET device name for the CPU is shown on the "Communication" website, at the "Parameter" tab.
  IP address parameters: Currently assigned IP address parameters are shown on the site "Module state".
  Topology: The current topology resulting from any customizations via user program is shown in the Web server. IO devices configured as optional are shown as "deactivated" IO devices in the Web server.

Rules

The rules for standard machine projects as described here (Page 265) apply.

For configuration-controlled IO systems, the following additional rules apply:

- When configuring MRP (Media Redundancy Protocol):
  The ports configured as ring ports must not be interlinked via user program.
  However, devices with ring ports (devices of an MRP domain) can be optional IO devices.
- When configuring docking stations (= IO devices changing during operation):
  Neither the docking station nor the first IO device of a docking unit may be optional IO devices.
  The ports of the docking units must not be interlinked via user program.
- When configuring IRT:
  The order of synchronized IO devices ("IRT devices") must be defined by the configuration and must not be changed in the different variants of a standard machine. For this reason, the ports of the IRT devices must not be interlinked via user program.
  However, you have the possibility to configure IRT devices primarily as optional IO devices.

You also have the option to interconnect, by user program, RT devices that are, for example, separated from this line by a switchport (see figure).

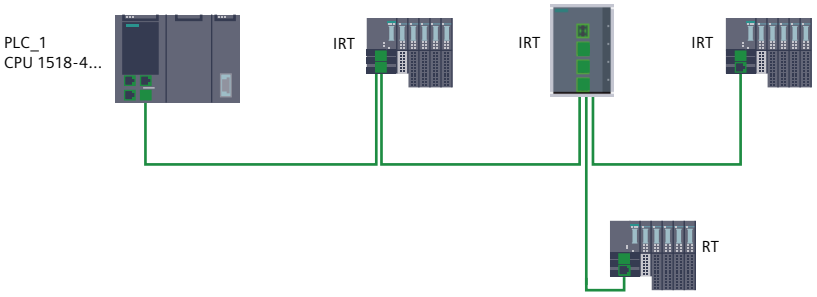


Figure 3-459 Example: Configuration control for IO systems with separated RT device

7.11 Saving energy with PROFIenergy

Saving energy with PROFIenergy

PROFIenergy is a PROFINET-based data interface for switching off consumers centrally and with full coordination during pause times regardless of the manufacturer or device type. Through this, the process should only be provided with the energy that is absolutely required. The majority of the energy is saved by the process; the PROFINET device itself only contributes a few watts of savings potential.

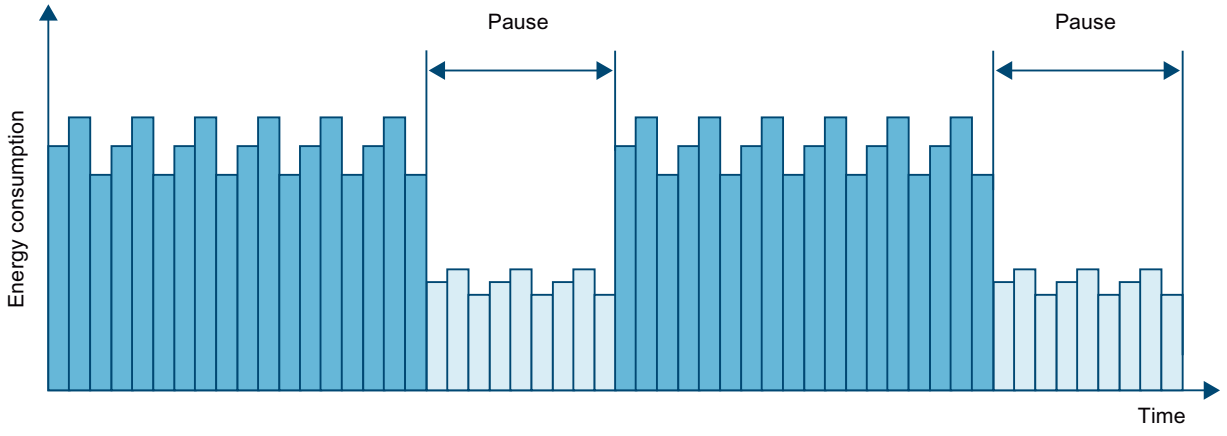


Figure 3-460 Energy savings during pauses with PROFIenergy

Basic information

In order to use the PROFIenergy functionality, the existing IO controller has to be "upgraded" to a so-called "PROFIenergy controller" by means of a function block in the PROFINET IO system and at least one PROFIenergy-capable IO device ("PROFIenergy device") has to exist. The PROFIenergy commands (for example to start or end a pause) are sent by the "PROFIenergy controller" to the individual "PROFIenergy devices". Each "PROFIenergy device" decides individually how it responds to the PROFIenergy command (response is device- and manufacturer-specific).

No additional hardware is needed; the PROFIenergy commands are directly interpreted by the PROFINET devices.

Principle of operation

At the beginning and end of pauses, the system manager enables or disables the pause function of the system; then the IO controller sends the PROFIenergy command "Start_Pause"/"End_Pause" to the PROFINET devices. The device interprets the contents of the PROFIenergy command and switches off or back on.

Through other PROFIenergy functions, device information can be accessed during pauses. The user can use this information in order to optimally time the transfer of the "Start_Pause"/"End_Pause" command.

PROFIenergy instructions for IO controllers

Two instructions are needed for controlling and monitoring the PROFIenergy functions.

The instruction PE_START_END allows you to easily activate and deactivate the idle state of PROFINET devices. This occurs by means of an incoming edge or outgoing edge. The instruction PE_START_END provides a simple interface for implementing the PROFIenergy commands Start_Pause and End_Pause.

The instruction PE_CMD allows you to transmit all PROFIenergy commands, including Start_Pause and End_Pause. The other commands can be used, for example, to query the current status of the PROFINET device or the behavior during the pauses. The instruction PE_CMD is a convenient means for handling all PROFIenergy functions.

PROFIenergy instruction for I-devices

The instruction PE_I_DEV allows you to also implement PROFIenergy on I-devices. The instruction receives PROFIenergy commands on the I-device and forwards these to the user program for execution. After executing the command, the user program calls the PE_I_DEV instruction again in order to send the acknowledgment to the IO controller. For these replies, each command offers you a helper instruction that supplies the reply data to the instruction.

The instructions can be found in the "Instructions" task card of the STEP 7 program editor.

Configuration and programming

The functions can be comfortably integrated into existing systems. No configuration is required for the use of PROFIenergy. However, amendments to the user program are required:

- Before the "Start_Pause" command, you must ensure that your system is brought into a condition that is suitable for a pause.
- A sequential control system for the beginning of the pause of the devices and for the punctual restarting of the device on break must be programmed (depending on the required startup times that the respective PROFINET device demands).

- The error messages of the PE_CMD instruction must be evaluated, and the required reaction must be programmed (for example, cancellation or continuation of further commands on lower-level PROFINET devices).

NOTE

In the case of the ET 200S distributed I/O system, you have to configure the application of PROFIenergy in STEP 7. You configure PROFIenergy by selecting the "Use energy saving for this potential group" check box in the PM-E DC24V/8A RO power module.
If you want to use PROFIenergy for an I-device, you have to configure this in STEP 7. Information about configuring PROFIenergy for an I-device is available in the section Configuring PROFIenergy with I-devices (Page 141).

Application examples

- SIMATIC S7 library for simple configuration of PROFIenergy.
  The application example is available here (https://support.industry.siemens.com/cs/ww/en/view/109478388).
- Application guide for implementation of shutdown concepts with PROFIenergy.
  The application example is available here (https://support.industry.siemens.com/cs/ww/en/view/96837137).
- Saving energy with SIMATIC S7 PROFIenergy with I-device
  The application example is available here (https://support.industry.siemens.com/cs/ww/en/view/41986454).

7.12 Docking systems

Using alternating IO devices ("alternating partners") during operation in a docking station

The following figure shows an automation cell with a docking station and several docking units.

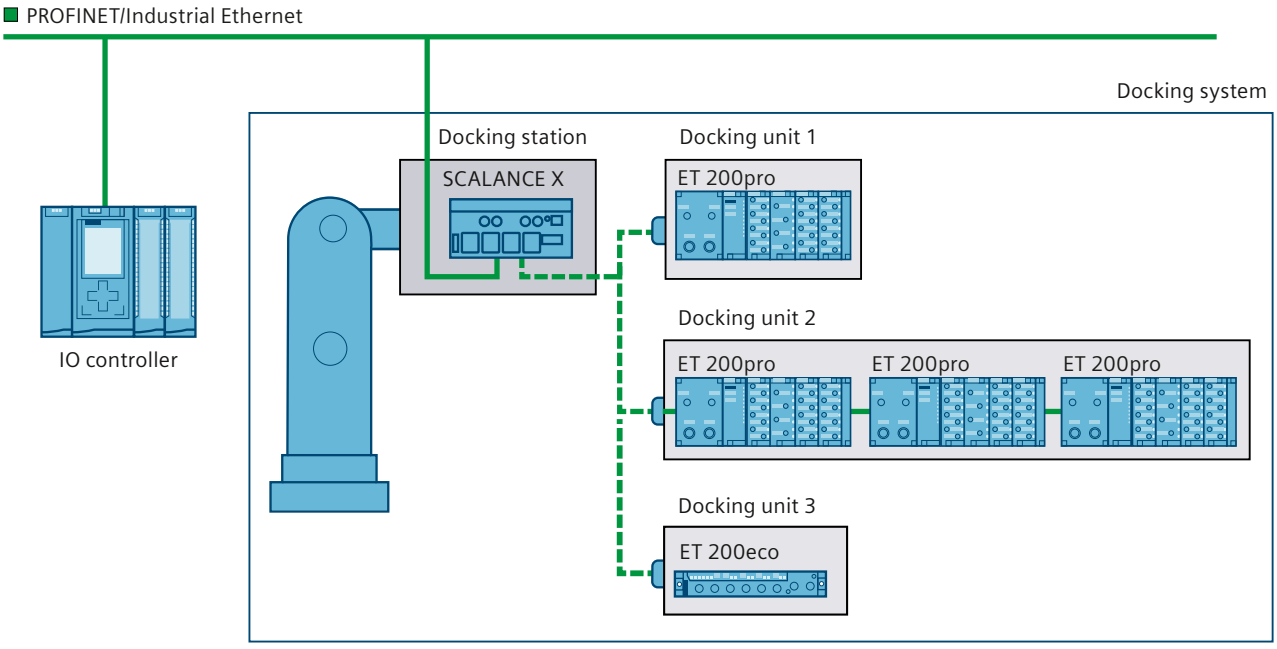


Figure 3-461 Alternating IO devices (partner ports) in a docking system

Area of application for alternating IO devices during operation

You can use the PROFINET function "Alternating IO devices during operation" ("alternating partners"), for the tool changeover for robots, for example. Typical tools include:

- Welding guns
- Positioning tools for manufacturing parts

Requirements for interconnecting alternating partner ports during operation

You can interconnect IO devices with alternating partner ports during operation in the following situations:

- The alternating IO device (docking unit) has no IRT communication configured.
- The PROFINET interface is connected to the Ethernet subnet.
- The PROFINET devices support topology configuration.

- The IO controller, the alternating IO devices (docking unit) and the switch (docking station) on which the alternating IO devices are to be operated support this feature.

NOTE

Unique IP address
Each docking unit of a docking system must be configured with a unique IP address in a shared project and operated on the same IO controller as all other docking units of the system.

Applicative conditions

The following points should be observed when implementing a docking system with alternating IO devices during operation:

- The IO devices of all docking units must be deactivated by default in the configuration.
- At any time, only one docking unit can be active, i.e., only the IO devices of one docking unit can be activated. All IO devices of other docking units must be deactivated or become deactivated before the IO devices of a docking unit can be activated. You activate an IO device with the "D_ACT_DP" instruction.
- A physical connection to this docking unit and its IO devices must be created in order to activate a docking unit. The IO devices are then switched on (power on). At the same time, all the IO devices of this docking unit must be activated in the user program with the "D_ACT_DP" instruction.

NOTE

Automatic deactivation in "Startup" mode of the CPU
If the CPU is in "Startup" mode, IO devices of a docking system that alternate during operation are deactivated automatically.

- After the feedback "IO device activated", you can access the IO device by means of direct I/O access.

- Call the "D_ACT_DP" instruction to activate and deactivate the IO device as close as possible to the start of the OB 1 cycle.

NOTE

Number of alternating IO devices during operation ("alternating partner port") - number of docking units

If you wish to achieve the shortest possible tool changeover times, you must observe the following points that are dependent on the CPU or the CP that is being used:

– Only those IO devices that have been configured with the PROFINET function "Prioritized startup" can start up in an optimized fashion. The number of IO devices with configuration for this PROFINET function is restricted.
– Only a limited number of IO devices can be activated at the same time. This number depends on the available "D_ACT_DP" resources. A docking unit should not contain more than the corresponding number of IO devices. If more IO devices are operated in a docking unit, the IO devices must be activated one after the other, which takes correspondingly longer.

Example: An S7-CPU 1516-3 PN/DP can operate a maximum of 32 IO devices with prioritized startup and can simultaneously activate 8 IO devices by means of "D_ACT_DP". Therefore, for a scheduled optimum use, a docking unit should include no more than 8 IO devices and no more than 32 IO devices should be used in all the alternating docking units.

7.12.1 Configuring docking systems

Configuring docking systems

The possible connections to the individual IO devices must be configured in STEP 7.

Procedure in STEP 7

1. Configure your system as usual, but do not yet configure the topological interconnections of the individual PROFINET devices.
2. Navigate to the "Topology view" tab.
3. Select the port which you want to operate with alternating partners during operation.
4. Navigate to the "Properties" tab of the inspector window and select "Port interconnection" in the area navigation.
5. Under "Partner port", select the "Alternative partners" option.

6. Select the desired partner ports: To do this, click "<Add alternative partners... and choose a partner port. Repeat this process until all required partner ports are connected.

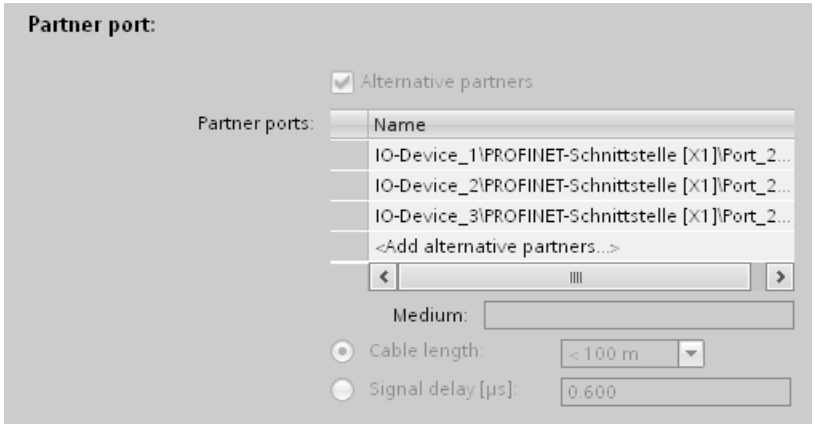


Figure 3-462 Configuring docking systems in STEP 7

Tip: You can also use drag-and-drop operation to connect alternative partner ports in the topology view.

Result

You have interconnected the respective port with one or more alternating IO devices. The connections with the individual alternating partner ports during operation are shown in the topology view by a green, dashed line.

Multiple IO devices as a docking unit ("Alternating partner port")

A docking unit may also consist of several IO devices connected in series. If you use IO devices connected in series as a docking unit, ensure that the topology of the IO devices is configured. A docking unit consisting of two IO devices connected in series (Tool_3_1 and Tool_3_2) is shown at the bottom right in the figure below.

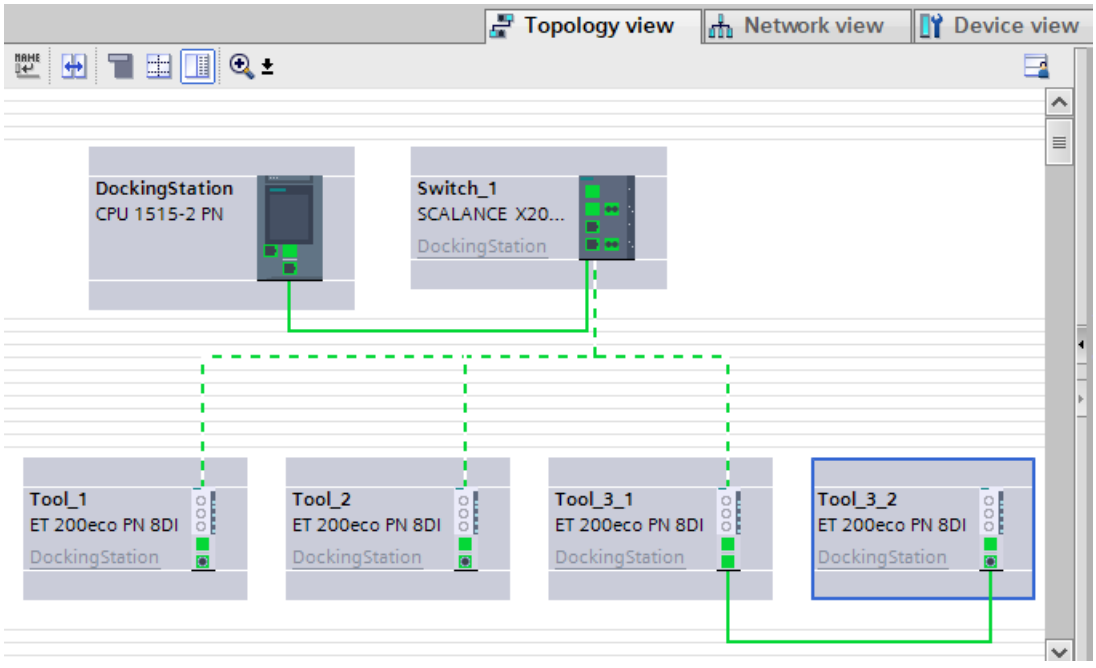


Figure 3-463 Docking system in the topology view of STEP 7

Restriction in the interconnection

The interconnection with a partner port is not possible in the following cases:

- The partner port does not have a suitable type of cable. In this case, a media convertor from the catalog must be inserted.
- The partner port is blocked (deactivated).
- The two ports that are to be interconnected belong to the same interface (it is only possible to interconnect the ports from different interfaces in a station).
- The two ports that are to be interconnected belong to different Ethernet subnets.

Deleting interconnections

Select the port of the alternating partner and remove the interconnection with the "Remove" button.

7.13 Accelerating startup

7.13.1 Options for accelerating the startup of IO devices

Reducing the startup time of IO devices

The time needed for the startup of IO devices depends on various factors and can be reduced in different ways.

You can achieve a significant reduction in the startup time using the "Prioritized startup" PROFINET function.

To further reduce the startup times, use the following measures in addition to the "Prioritized startup":

- Optimize the port settings
- Optimize the cabling of the ports
- Perform measures in the user program (for docking systems only)

These measures will accelerate the startup of IO devices even without "Prioritized startup". However, you can only achieve the fastest startup times of about 500 ms by combining all the measures with "Prioritized startup".

NOTE

Startup time up to 8 s

In the following situation, despite prioritized startup, a startup time of up to 8 s may occur: On a docking point, multiple physical IO devices dock as an IO device with identical device names and identical IP configurations (for example, docking point for automatic transport system).

Dependencies

The length of the startup time for an IO device (distributed I/O) with the "Prioritized startup" PROFINET function depends on the following factors:

- IO devices (distributed I/O)
- IO structure of the IO device (distributed I/O)
- Modules of the IO device (distributed I/O)
- IO controller
- Switch
- Port setting
- Cabling

- Configured RT class of the IO device

NOTE

Startup time and RT class of the IO device
An IO device with IRT communication requires longer than an IO device with RT communication for the accelerated startup.
The longer startup for IRT is due to the necessity of synchronizing the IO device before the communication can be set up.

NOTE

IWLAN and prioritized startup
PROFINET devices which are connected via access points to PROFINET IO do not support the "Prioritized startup" PROFINET function.

7.13.2 Prioritized startup

Definition

Prioritized startup denotes the PROFINET functionality for accelerating the startup of IO devices in a PROFINET IO system with RT and IRT communication. It reduces the time that the correspondingly configured IO devices require in order to return to cyclic user data exchange in the following cases:

- After the power supply has returned
- After a station has returned
- After activation of IO devices

⚠ WARNING

Data exchange despite multiple use IP addresses/device names in PROFINET IO system
To achieve higher ramp-up times, the IO controller checks the uniqueness of device name of IP address parallel to the device ramp-up. In the case of incorrect or double assignment of device name or IP address, a short-time data exchange is possible until the IO controller reacts to the error. In this time the IO controller can exchange IO data with the false device. During commissioning, ensure that no IP addresses / device names are assigned multiple times in the PROFINET IO system.

Advantages

The PROFINET functionality "prioritized startup" enables PROFINET IO applications in which machine parts or tools and their IO devices have been permanently replaced. Waiting times of several seconds between the scheduled processes of the restart are reduced to a minimum by this optimization. This accelerates the production process with alternating IO devices (PROFINET functionality "docking systems"), e.g. in tool changer applications, and enables a greater throughput in production.

The PROFINET functionality "prioritized startup" also offers a considerable increase in performance for applications where a quick startup time of the IO devices after "power on" or after station failure / station return is required, or when activating IO devices.

Area of application

You can use prioritized startup, for example, for changing tools for robots in the automotive industry. Typical tools are, for example:

- Welding guns
- Positioning tools for the manufacture of car body parts

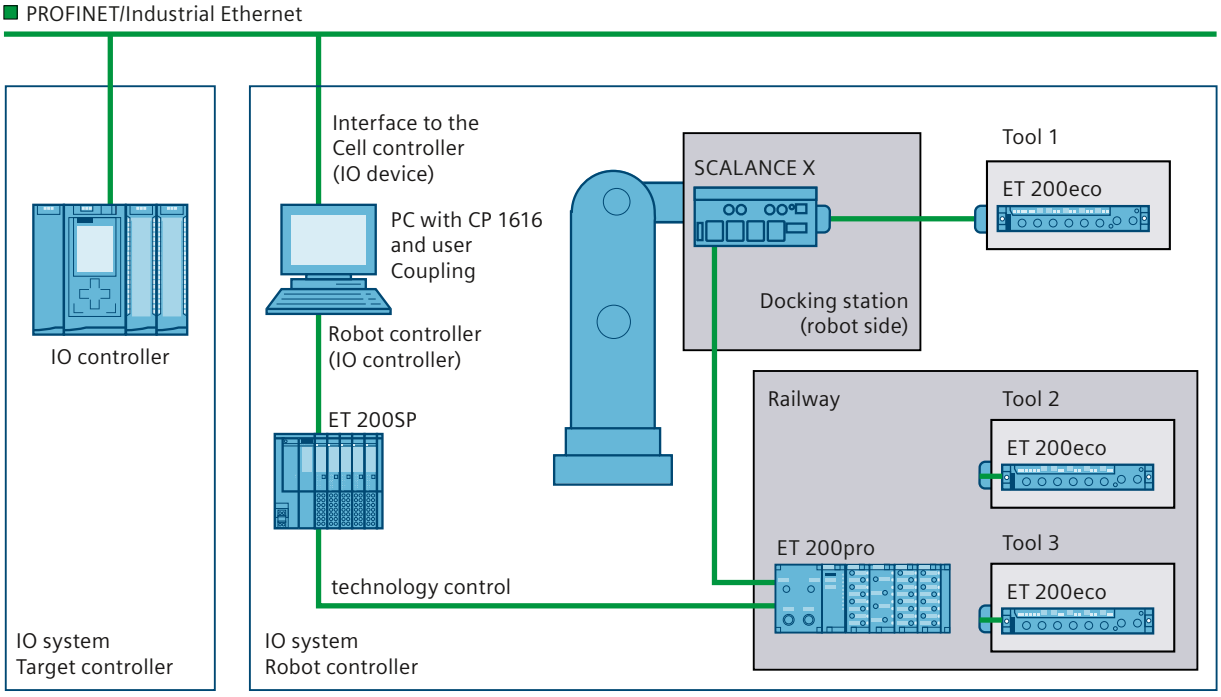


Figure 3-464 Example configuration of a tool changer: Tools 1-3 configured with "Prioritized startup".

7.13.3 Configuring prioritized startup

Requirements

You can enable the "Prioritized startup" PROFINET function for the IO devices (distributed I/O) only in the following cases:

- The IO controller used can prioritize selected IO devices during startup.
- The IO device used supports prioritization.

Procedure

1. Select the IO device in the network view or device view for which you wish to accelerate startup.
2. Open the IO device properties in the Inspector window.
3. Select "PROFINET interface > Advanced options > Interface options".
4. Select the "Prioritized startup" check box.

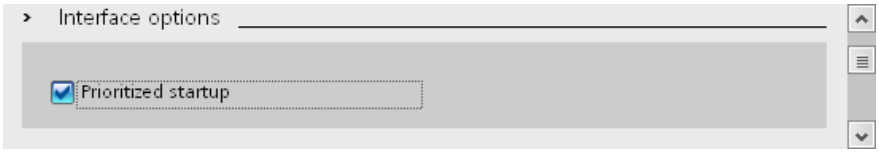


Figure 3-465 Configuring prioritized startup in STEP 7

5. Download the configuration to the IO controller.

NOTE

Prioritized startup after a startup for the first time
A prioritized startup of the IO device is always available to you after the first configuration of this IO device in the very first startup of the PROFINET IO system. Even in the case of spare parts or a reset to factory settings, the first startup is a standard startup for the respective configured IO devices.

NOTE

Number of IO devices (distributed I/O) with prioritized startup
You can only start up a maximum number of IO devices with the "Prioritized startup" PROFINET functionality within one PROFINET IO system. This maximum number depends on the IO controller used.

7.13.4 Optimize the port settings

Optimizing port settings on the IO device and IO controller

The transfer medium and the duplex option are checked during startup of the IO device in the case of copper cabling.

These checks require time, but with specific presets of these options you can save the time the check requires. Make certain that the settings made correspond to the actual conditions (using the correct cables).

Optimizing port settings for accelerated startup

To optimize port settings for accelerated startup, follow these steps:

1. Select the ports of the IO controller or the partner port of the corresponding IO device.
2. Navigate to "Port options > Connection" in the Inspector window. Select the setting "TP 100 Mbps full duplex" under "Transmission rate/duplex"

3. Clear the "Enable autonegotiation" check box.

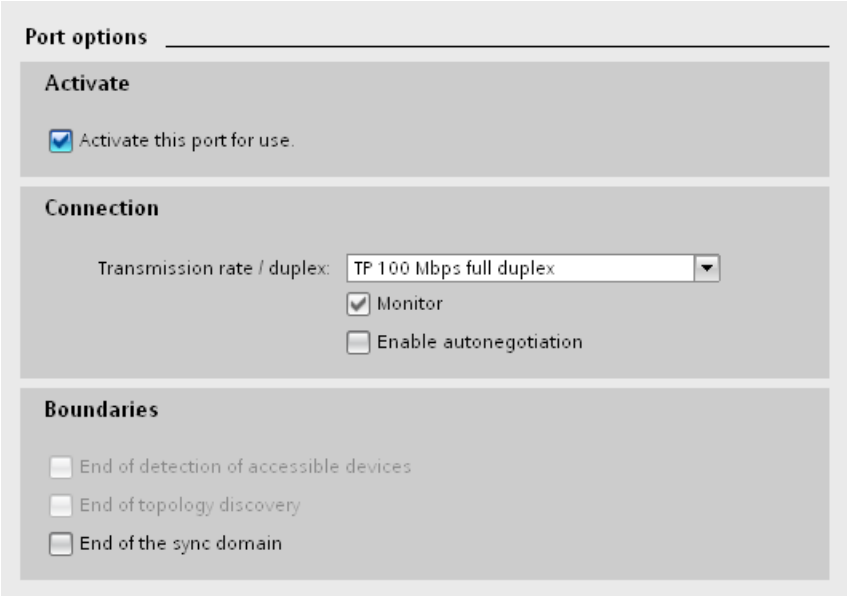


Figure 3-466 Optimizing port settings for accelerated startup in STEP 7

These settings are automatically applied during topology configuration for the partner port.

7.13.5 Optimize the cabling of the ports

Requirements

You have made the following settings for the port in question to reduce the startup time of the IO device:

- Fixed transmission rate
- Autonegotiation deactivated

The time for negotiating the transmission rate during startup is saved.

If you have disabled autonegotiation, you must observe the cabling rules.

Properties of ports

PROFINET devices have the following two types of ports:

Type of port	PROFINET devices
Switch port with crossed pin assignment	For IO devices: Port 2 For S7-CPUs with two ports: Ports 1 and 2
Terminal device port with normal pin assignment	For IO devices: Port 1 For S7-CPUs with one port: Port 1

Crossed pin assignment means that the pin assignment for the ports for sending and receiving between the respective PROFINET devices is inverted internally.

Validity of the cabling rules

The cabling rules described in the following paragraph apply exclusively for the situation in which you have specified a fixed port setting in STEP 7.

Rules for cabling

You can connect several IO devices in series using patch cables. To do this, connect port 2 of the IO device (distributed I/O) with port 1 of the next IO device. The following graphic provides an example with two IO devices.

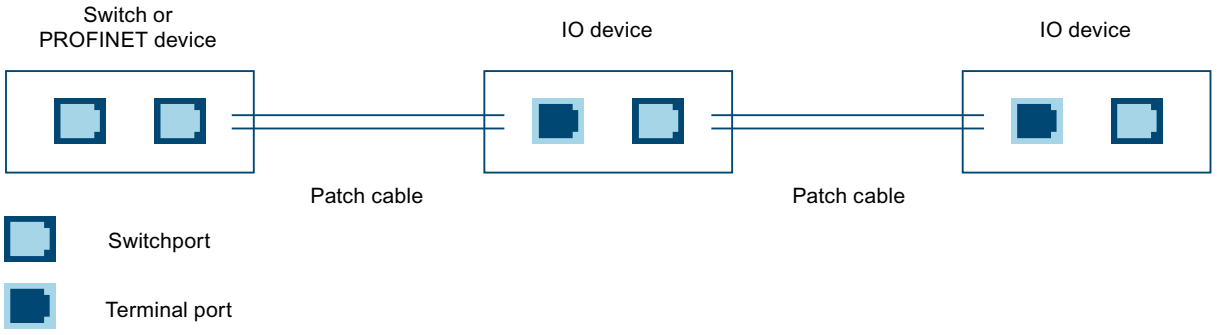


Figure 3-467 Optimized cabling for accelerated startup

7.13.6 Measures in the user program

Introduction

You can make certain changes in the user program to accelerate the startup for IO devices of docking systems that alternate during operation.

Making the required changes to the user program

To accelerate the startup by making changes to the user program, follow these steps:

1. Call the "D_ACT_DP" instruction to activate and deactivate the IO device at the start of the OB 1 cycle.

   If the IO device is replaced, the device that is no longer required must be deactivated and the new device must be activated.
2. If you control the "Power ON" command of the IO devices via the application, then start the activation of the IO devices via the corresponding call of the "D_ACT_DP" instruction as near to the same time as possible. The IO device has to be physically connected for this.
3. You access the IO device using direct access commands after the "D_ACT_DP" instruction has provided the feedback "IO device activated".

7.14 Dealing with timeouts while exchanging data

7.14.1 Terminating communication relation during faults

The prerequisite for data exchange between an IO controller and an IO device is an existing communication relation (Application Relation, AR).

In a communication relation, data is transmitted cyclically and acyclically. If a protocol error or a timeout is detected during acyclic data record communication (e.g. program instructions "RDREC" or "WRREC", or reading of a diagnostic data record), the IO controller terminates the communication relation. In this case, the IO controller assumes that a communication error has occurred. This also ends the cyclic IO data exchange. The error code is returned as a static error in the instruction to the data record transfer. The error is indicated in the diagnostics buffer of the IO controller as the event "IO device failure - Timeout in acyclic PROFINET services".

Possible causes for a termination of the communication relation include:

- A high network load
- Too many ARP telegrams (Address Resolution Protocol).
- Too many UDP frames (User Datagram Protocol).
- Erroneous RPC calls (Remote Procedure Call).

Maintain communication relation

If you can tolerate timeouts during the data record communication from the point of view of your application and no negative repercussions are to be feared, you can change the described default behavior. If, for example, timeouts occur during the data record communication, the communication relation is still preserved. Cyclic IO data exchange continues.
A data exchange error is then signaled as a temporary error (status code: 16#DE80_C300 or 16#DF80_C300) in the instruction for data record transfer.

Starting from STEP 7 V19, you have two options for enabling maintenance of the communication relation. Depending on the FW version of the S7-1500 CPU used, you can enable maintenance as follows:

- S7-1500 CPU as of FW version V3.1:
  - You can configure the maintenance in the CPU properties.
  - You can transfer a data record 0xB072 to an integrated PROFINET interface of the S7-1500 CPU.
- S7-1500 CPU as of FW version V3.0: You can transfer a data record 0xB072 to an integrated PROFINET interface of the S7-1500 CPU.

You must enable maintenance of the communication relation separately for each required PROFINET interface:

- When configuring in the CPU properties, you must enable maintenance for each required PROFINET interface separately.
- When transferring a data record 0xB072, you must transfer this data record separately to each required PROFINET interface.

You will find the various procedures for maintaining the communication relation in the sections below.

Maintaining the communication relation in S7-1500 R/H systems

For S7-1500 R/H CPUs, enable maintenance of the communication relation as described above. However, the S7-1500 R/H system does not synchronize all changes automatically. Therefore you must make the following changes:

- Enable in the CPU properties: Enable maintenance of the communication relation in the CPU properties of one CPU of the S7-1500 R/H system. STEP 7 automatically synchronizes this setting between the two CPUs.
- Transfer a data record: A PROFINET interface, e.g. X1, has different hardware identifiers for the two CPUs. Therefore, write the data record during runtime to the respective addressed PROFINET interface of both CPUs.

In the case of S7-1500 R/H systems, you can only maintain the communication relation at the PROFINET interface X1.

7.14.2 Enabling maintenance of the communication relation in the CPU properties

Requirements

If you want to enable maintenance of the communication relation in the CPU properties, the following requirements must be met:

- STEP 7 V19
- S7-1500 CPU FW version V3.1 or higher
- IO system, e.g. "PLC_1.PROFINET IO System (100)", has been configured at the relevant PROFINET interface

Procedure

The following procedure shows an example of how to enable maintenance of the communication relation at the integrated PROFINET interface X1. The procedure is identical for all integrated PROFINET interfaces of the S7-1500 CPU. To enable maintenance of the communication relation in the CPU properties, follow these steps:

1. Switch to the network view of STEP 7.
2. Configure an S7-1500 CPU, e.g. CPU 1516-3 PN/DP, with the required IO devices.
3. Select a PROFINET interface of the S7-1500 CPU, e.g. X1.
4. In the Inspector window, go to "General > Advanced options > Interface options".

5. In the "Interface options" area, select the "Maintain PROFINET IO communication on data record communication timeout" option.

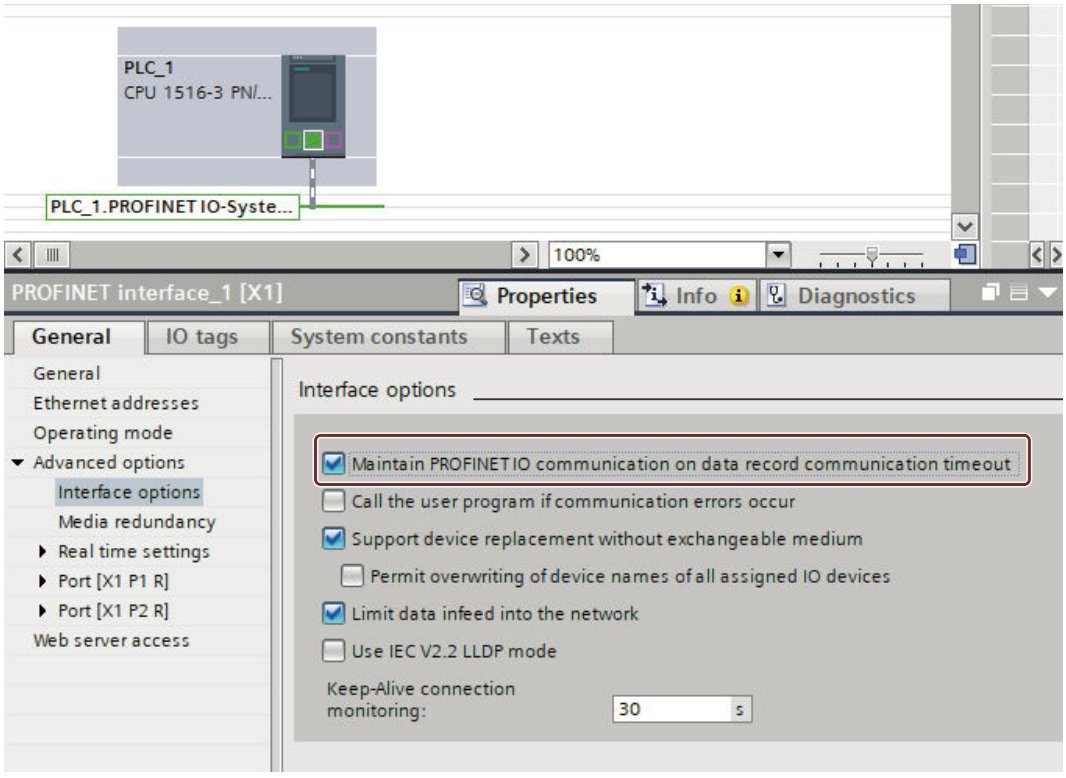


Figure 3-468 Selecting the "Maintain PROFINET IO communication on data record communication timeout" option

6. If required, repeat steps 3 to 5 for another integrated PROFINET interface of the S7-1500 CPU.
7. Load the changed settings into the S7-1500 CPU.

   Result: The communication relation is maintained at the respective configured PROFINET interface of the S7-1500 CPU.

The "Maintain PROFINET IO communication on data record communication timeout" option is only available if you have added an IO system to the relevant PROFINET interface of the S7-1500 CPU. If no IO system exists at this PROFINET interface, the option is displayed in gray. In this case, the option cannot be selected.

If you delete an existing IO system after selecting the "Maintain PROFINET IO communication on data record communication timeout" option, the check box remains selected. The option is displayed in gray in this case and cannot be changed.

Behavior of the option when replacing devices in STEP 7

The "Maintain PROFINET IO communication on data record communication timeout" option can only be selected in STEP 7 V19 for configured S7-1500 CPUs as of FW version V3.1. If you exchange or replace a S7-1500 CPU, the option behaves as follows, depending on the configured FW version:

- S7-1500 CPU with FW version V3.1 → S7-1500 CPU with FW version V3.1:
  STEP 7 applies the settings of the previous S7-1500 CPU to the new S7-1500 CPU.
- S7-1500 CPU with FW version V3.1 → S7-1500 CPU with FW version < V3.1:
  STEP 7 shows a warning message. The option is disabled and can no longer be selected.
- S7-1500 CPU with FW version V3.0 → S7-1500 CPU with FW version V3.1:
  STEP 7 shows an information message. The option can be selected and is deselected in the default settings.

The changes do not take effect on the new S7-1500 CPU until the configuration has been loaded. Therefore, load the changed configuration into the new S7-1500 CPU.

7.14.3 Enabling maintenance of the communication relation by data record transfer

Requirements

If you want to enable maintenance of the communication relation by transferring a data record, the following requirements must be met:

- STEP 7 version V18 or higher
- S7-1500 CPU FW version V3.0 or higher
- At least one IO device has been configured at the addressed PROFINET interface

Procedure

Transfer a data record 0xB072 to the PROFINET interface of the S7-1500 CPU. Coding in this data record indicates whether the communication relation is to be terminated or remain active following an error. The data record acts only on the addressed PROFINET interface.

Option for transferring the data record 0xB072: Definition of the data record structure in the static local data of a function block and call of this function block in the program cycle OB. To do this, follow these steps:

1. Create a function block in STEP 7.
2. For the static local data (Static) of the function block, create a structure of the data record 0xB072.
   – The following table shows the structure of the data record 0xB072:

Byte	Element	Coding	Explanation
0-1	BlockType	0xB072	Header The data record length is counted from byte 4 "BlockVersionHigh".
2-3	BlockLength	8	
4	BlockVersionHigh	0x01	
5	BlockVersionLow	0x00	

Byte	Element	Coding	Explanation
6-7	Reserved	-	-
8-9	ReadWriteBehaviorProperties	0, 1	0: Default behavior. The communication relation is terminated in the case of the scenarios described above. 1: The communication relation is maintained in the case of the scenarios described above.
10-11	Reserved	-	-

3. Call the created function block in the program cycle OB (OB 1) of your user program. A programming example for this function block can be found in the next section.

The newly set behavior is not permanently stored in the S7-1500 CPU. The default setting becomes active again after each POWER OFF/POWER-ON, memory reset, or loading of the hardware configuration. The changed behavior is not active until the write job in the program cycle OB has finished.

NOTE

Changing the communication behavior for each PROFINET interface

The call of the function block in the program cycle OB relates only to the addressed PROFINET interface of the S7-1500 CPU. If you want to maintain the communication relations for other PROFINET interfaces, you must call the function block separately in the program cycle OB for each additional integrated PROFINET interface of the S7-1500 CPU.

Maintaining the communication relation in S7-1500 R/H systems

You can also change the default behavior for S7-1500 R/H CPUs by transferring a data record 0xB072.

However, the S7-1500 R/H system does not automatically synchronize this change in behavior for the respective addressed PROFINET interface at both CPUs, since the PROFINET interfaces have different hardware identifiers. Therefore, write the data record during runtime to the respective addressed PROFINET interface of both CPUs. You can only maintain the communication relation at the PROFINET interface X1.

7.14.4 Example: Transfer data record for behavior change via FB

Task

You want to maintain the communication relation (AR) between the IO controller and IO device even in the event of a temporary data record transfer error, e.g. due to elevated network load.

Requirements

An S7-1500 CPU FW version V3.0 or higher with at least one configured IO device at the addressed PROFINET interface is required.

Solution

Transfer the data record 0xB072 to the PROFINET interface of the S7-1500 CPU. This instructs the S7-1500 CPU to maintain an existing communication relation with the IO device.

The following example shows you how to transfer the data record to the PROFINET interface using a function block (FB). Create a structure of the data record 0xB072 in the block interface under "Static". The following figure shows the structure of the data record in "Static" section.

FbBehaviorAR

	Name	Data type	Default value	Retain	Comment
1	Input				
2	Output				
3	InOut				
4	bStart	Bool	0	Set in IDB	Start writing Data record 16#B072
5	InterfaceID	HW_IO	64	Non-retain	Default for Interface X1
6	wBehaviorProperties	Word	16#1	Non-retain	0: AR will be dropped, 1: AR stays active
7	Static				
8	statArRecord	Struct		Non-retain	Data record 16#B072
9	statBlockType	Word	16#B072	Non-retain	Data record number
10	statBlockLength	Word	16#8	Non-retain	Length of block (default: 8)
11	statBlockVersionHigh	Byte	1	Non-retain	Byte 1 of blockversion
12	statBlockVersionLow	Byte	0	Non-retain	Byte 2 of blockversion
13	statReserved	Word	16#0	Non-retain	Reserved for future usage
14	statBehaviorProperties	Word	1	Non-retain	0: AR will be dropped, 1: AR stays active
15	statReserved1	Word	16#0	Non-retain	Reserved for future usage
16	instWrrec	WRREC			Instance of write record
17	Temp				
18	Constant				

Figure 3-469 Example: Interface of the function block for obtaining the communication relation

In addition to the data record 0xB072, the interface contains other tags that you use to transfer the data record. You need the tags in the "InOut" section to assign parameters for the "WRREC" instruction in the function block. The "WRREC" instruction is executed in an organization block (OB1) when the FB is called.

The program in the function block and the call in the program cycle OB are shown in the following sections.

Program in the function block

The data record is transferred at a positive signal at the "#bStart" tag. The parameters for the tags "#wBehaviorProperties", "#bStart" and "#InterfaceID" are passed to the function block when called in the program cycle OB.

```
//=============================================================
 // Called in OB1
 //=============================================================
 #statArRecord.statBehaviorProperties := #wBehaviorProperties;
 #instWrrec(REQ := #bStart,
 ID := #InterfaceID,
 INDEX := DWORD_TO_DINT(16#B072),
 LEN := 12, // 0 : any length,
 this record uses 12 Bytes,
 RECORD := #statArRecord);
 IF #instWrrec.ERROR THEN
 RETURN; // add error handling
```

```
END_IF;
IF #instWrrec.DONE = TRUE THEN
#bStart := FALSE;
END_IF;
```

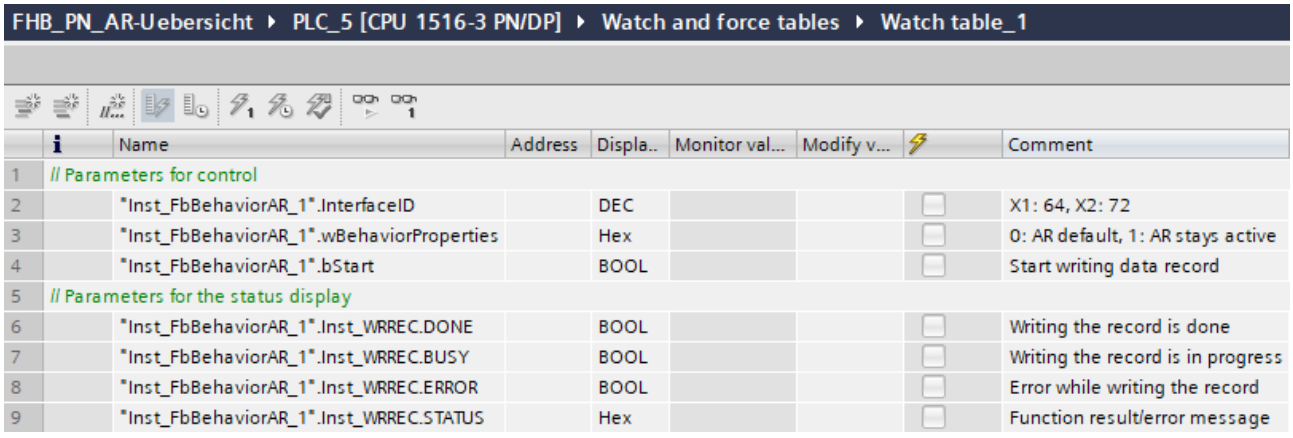
Calling in a program cycle OB

Drag-and-drop the created function block into the desired program cycle OB (e.g. OB1). The "InOut" parameters are not linked to tags in this example. Instead, they are controlled directly in the instance of the block call via a watch table.

```
//=========================================================
 // Call FbBehaviorAR
 //=========================================================
"Inst_FbBehaviorAR_1"(bStart:=_bool_inout_,
 InterfaceID:=_hw_io_inout_,
 wBehaviorProperties:=_word_inout_);
```

Control via the watch table

1. Create a new watch table.
2. Drag-and-drop the required tags from the instance of the function block into the watch table.



	i	Name	Address	Displa..	Monitor val...	Modify v...		Comment
1		// Parameters for control						
2		"Inst_FbBehaviorAR_1".InterfaceID		DEC			☐	X1: 64, X2: 72
3		"Inst_FbBehaviorAR_1".wBehaviorProperties		Hex			☐	0: AR default, 1: AR stays active
4		"Inst_FbBehaviorAR_1".bStart		BOOL			☐	Start writing data record
5		// Parameters for the status display						
6		"Inst_FbBehaviorAR_1".Inst_WRREC.DONE		BOOL			☐	Writing the record is done
7		"Inst_FbBehaviorAR_1".Inst_WRREC.BUSY		BOOL			☐	Writing the record is in progress
8		"Inst_FbBehaviorAR_1".Inst_WRREC.ERROR		BOOL			☐	Error while writing the record
9		"Inst_FbBehaviorAR_1".Inst_WRREC.STATUS		Hex			☐	Function result/error message

Figure 3-470 Watch table for transferring the data record

3. Load your project into the S7-1500 CPU.
4. Click "Go online".

You transfer the data record to the PROFINET interface as follows:

1. For the "Inst_FbBehaviorAR_1".InterfaceID" tag, enter the appropriate value for the interface for which you want to change the behavior.
2. To change the behavior, enter the value "1" for the "Inst_FbBehaviorAR_1".wBehaviorProperties" tag.
3. Control the "Inst_FbBehaviorAR_1".bStart" tag to transfer the "TRUE" data record.
4. Repeat steps 1 to 3 for an additional interface where you want to change the behavior.

You can see the status of the transmission to the PROFINET interface as follows:

- "Inst_FbBehaviorAR_1".Inst_WRREC.DONE: The data record was successfully transferred to the PROFINET interface.
- "Inst_FbBehaviorAR_1".Inst_WRREC.BUSY: The data record is currently being transferred to the PROFINET interface.
- "Inst_FbBehaviorAR_1".Inst_WRREC.ERROR: The transfer of the data record to the PROFINET interface was faulty.
- "Inst_FbBehaviorAR_1".Inst_WRREC.STATUS: Output of block status or error information. The corresponding interpretations can be found in the STEP 7 help system.

Note that the variables „Inst_FbBehaviorAR_1“.Inst_WRREC.DONE and „Inst_FbBehaviorAR_1“.Inst_WRREC.ERROR are only present for the duration of a program cycle.

Additional steps for S7-1500R/H systems

Each addressed PROFINET interface of the two R/H CPUs has different hardware identifiers. Therefore, transfer the data record to the respective addressed PROFINET interface of both CPUs for S7-1500 R/H systems.

The values for the "Inst_FbBehaviorAR_1".InterfaceID" tag for S7-1500 R/H systems are listed in the following table:

Table 3-51 Overview of CPUs and associated hardware identifiers of the PROFINET interfaces

CPU	PROFINET interface	Hardware identifier of the PROFINET interface
CPU with redundancy ID "1" (prefixed name: PLC_1)	X1	65164 (prefixed name: Local1~PROFINET-interface_1)
	X2	PROFINET IO is currently not supported.
CPU with redundancy ID "2" (prefixed name: PLC_2)	X1	65364 (prefixed name: Local2~PROFINET-interface_1)
	X2	PROFINET IO is currently not supported.

NOTE

Transfer of the data record to the backup CPU

Do not transfer the data record to the addressed PROFINET interface of the backup CPU until after the S7-1500 R/H system has reached the "Run REDUNDANT" system state. Otherwise, the data record cannot be transferred to the addressed PROFINET interface of the backup CPU.

The CPU redundancy error OB (OB72) starts when the S7-1500 R/H system has reached the "Run REDUNDANT" system state. The "Fault_ID" tag of the OB72 contains the error code "B#16#03" or "B#16#06".

7.15 PROFINET Security

7.15.1 Configuring the SNMP

Component interaction

PROFINET networks use the SNMP protocol for managing devices and the network infrastructure.

For information exchange, authentication must take place through the transfer of community strings. When SNMP is used, a community string must always have been assigned. Empty community strings are not allowed.

You can find configuration options for SNMP in the properties of the following devices:

- S7-1500 CPU as an IO controller/I-device
- IO devices that support the configuration of SNMP

To learn how to configure SNMP for the various components, see the following sections.

NOTE

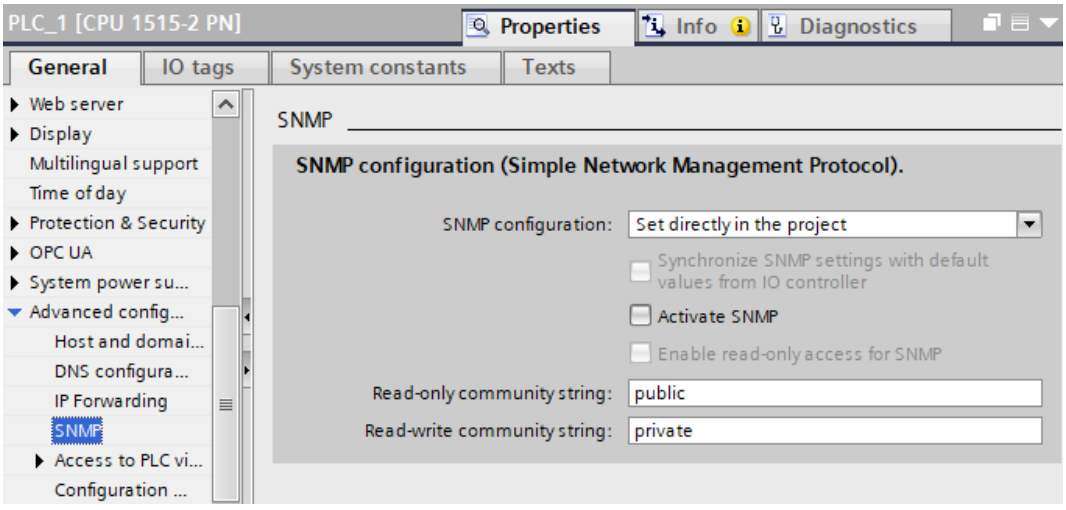
Avoidance of erroneous access attempts
Inform maintenance personnel about the SNMP-configuration in your plant.

Configuring SNMP for an IO controller

To configure SNMP for an IO controller, follow these steps:

1. Open the Properties of the IO controller in the network view or device view.
2. Navigate to the "Advanced configuration > SNMP" area in the Inspector window.
3. If you want to use SNMP, select the "Activate SNMP " option in the area "SNMP". Once you enable SNMP, a warning message appears informing you of the reduced protection against unauthorized access to functions and data of this device.
4. If you only need read access for SNMP, also select the "Enable read-only access for SNMP" option .

5. Change the Read-only and Read-write community strings.
   This increases the security of your system against cyber attacks. Empty community strings are not allowed.



Result: You have configured SNMP in the properties of your IO controller.

You can find information on the "Synchronize SNMP settings with default values from IO controller" option under "Configuring SNMP for an I-device".

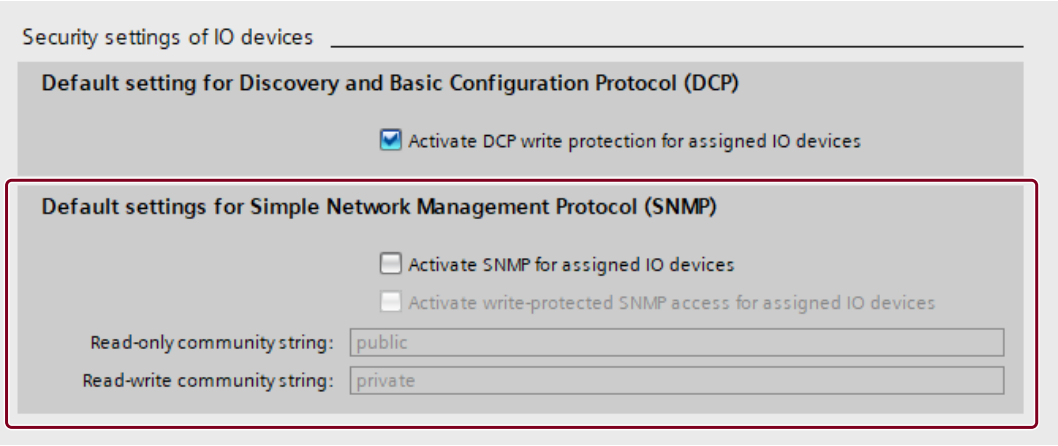
Configuring SNMP for the IO system of an IO controller

As of STEP 7 V20 and CPU FW version V4.0, you can configure SNMP parameters as default settings for an entire PROFINET IO system at the PROFINET interface of the IO controller. If IO devices support the configuring of SNMP, the SNMP settings in the device properties of the assigned IO devices are synchronized with these default settings at the PROFINET interface of the higher-level IO controller by default.

To configure the SNMP default settings for a PROFINET IO system, follow these steps:

1. Select the PROFINET interface of the IO controller to which the IO devices to be synchronized are connected in the network view or device view.
2. In the Inspector window, navigate to the "Advanced options > Security settings of the IO devices" area.
   STEP 7 as of V21 only displays this area if a PROFINET IO system has been added to the PROFINET interface of the IO controller.
3. If you want to use SNMP at assigned IO devices, enable the "Activate SNMP for assigned devices" option in the "Default settings for Simple Network Management Protocol (SNMP)" area.
4. If you need only read access for SNMP at the assigned IO devices, activate the "Enable read-only access for SNMP" option additionally.

5. Change the Read-only and Read-write community strings.
   This increases the security of your system against cyber attacks. Empty community strings are not allowed.



Result: You have configured the SNMP default settings for the entire PROFINET IO system at a PROFINET interface of the IO controller.

Configuring SNMP for an IO device

If an IO device supports the configuration of SNMP, you have the option of defining a separate SNMP configuration for this IO device as of STEP 7 V19. For IO devices that were imported as a GSD file, you can also modify the SNMP configuration in STEP 7 as of V19 or with other tools.

As of STEP 7 V20, IO devices are synchronized to the SNMP default settings of the PROFINET interface of their higher-level IO controller by default. Changes to the SNMP default settings are thus automatically synchronized at the IO devices.
Alternatively, you can define a separate SNMP configuration for each IO device.

To configure SNMP for an IO device in your PROFINET network, follow these steps:

1. Open the properties of the IO device in the network or device view.
2. Select "Advanced configuration" in the Inspector window.
   The option "Synchronize SNMP settings with default values from IO controller" is activated by default.
3. If you want to specify a different SNMP configuration for this IO device, deactivate the option "Synchronize SNMP settings with default values from IO controller".
   The following options can then be edited. The following settings are possible:
   - If you want to use SNMP, select the "Activate SNMP" option.
     Once you activate SNMP, a warning message appears informing you of the reduced protection against unauthorized access to functions and data of this device.
   - If you only need read access for SNMP, also select the "Enable read-only access for SNMP" option.
   - Change the Read-only and Read-write community strings.
     This increases the security of your system against cyber attacks. Empty community strings are not allowed.

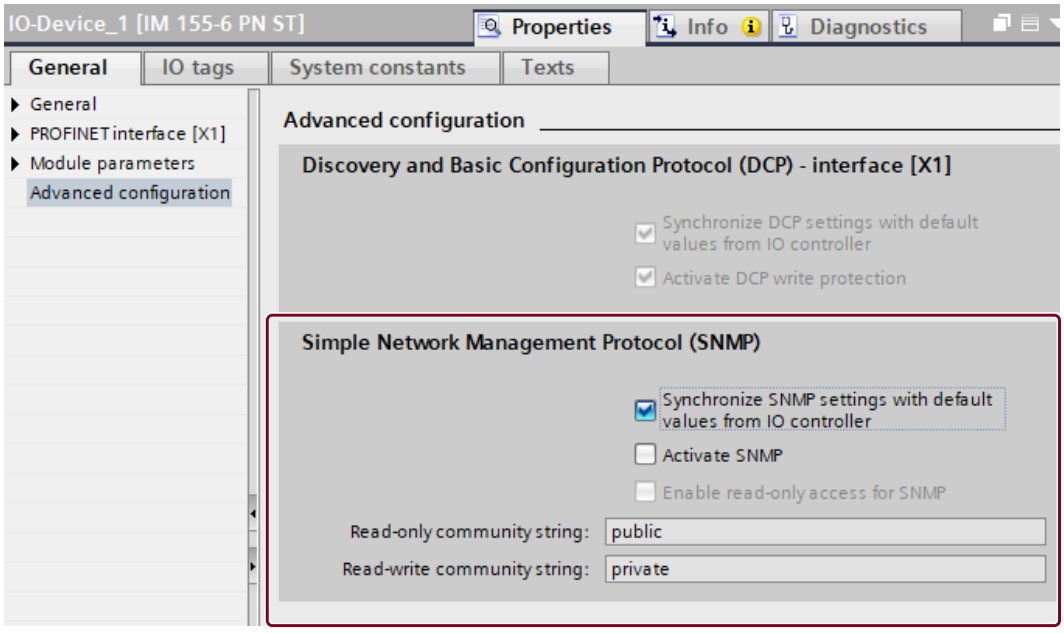


Figure 3-471 Configuring SNMP on an IO device

Result: You have configured SNMP in the properties of the IO device.

Configuring SNMP for an I-device (IO controller and I-device in the same project)

Since STEP 7 V18 you have the option of enabling SNMP in the CPU properties of an IO controller. When a CPU assumes the role of an I-device, you can also define the setting for SNMP in the CPU properties.

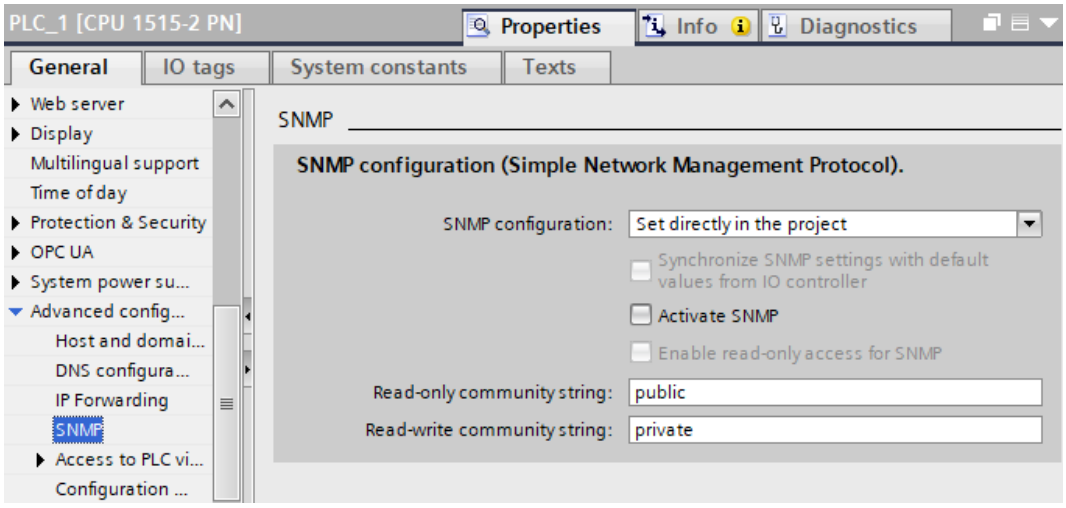
As of STEP 7 V20 and CPU FW version V4.0, you can configure SNMP parameters as default settings for an entire PROFINET IO system at the PROFINET interface of the higher-level IO controller. If I-devices support the configuring of SNMP by their higher-level IO controller, you can synchronize the SNMP configuration in the device properties of the I-device with the default settings at the PROFINET interface of the higher-level IO controller.

To access the SNMP configuration options for an I-device, follow these steps:

1. Open the Properties of the CPU that has been configured as an I-device in the network or device view.
2. Navigate to "Advanced configuration > SNMP" in the Inspector window.
3. Select one of the following options from the drop-down list next to "SNMP configuration":
   - Set directly in the project:
     The I-device receives its SNMP configuration from the configuration that is loaded onto the I-device. Changes to the SNMP configuration by a higher-level IO controller are prevented.
     The "Synchronize SNMP settings with default values from IO controller" option is grayed out in this case and cannot be changed. Configure the SNMP settings as described in steps 4 to 6. Load the configuration into the I-device.

– Via PROFINET interface ... (e.g. X1) from higher-level IO controller:
  Requirements:
  The "Parameter assignment of PN interface by higher-level IO controller" option is enabled at the I-device.
  An IO controller has been selected in the "Higher-level IO controller of the PN interface" drop-down list.
  The I-device receives its SNMP configuration from its higher-level IO controller. The "Synchronize SNMP settings with default values from IO controller" option is available for selection in this case. If you enable this option, the options underneath are disabled and indicate the synchronized SNMP default settings from the higher-level controller.
  Load the configuration into the lower-level IO controllers of the I-device. Because the SNMP parameters are transferred into the I-device by the higher-level IO controller, you do not have to reload the I-device configuration in this case.

4. If you want to use SNMP and the I-device is not being synchronized with the SNMP default settings, select the "Activate SNMP" option.
   After activation of SNMP, a warning message appears informing you of the reduced protection against unauthorized access to functions and data of this device.
5. If you only need read access for SNMP, also select the "Enable read-only access for SNMP" option .
6. Change the Read-only and Read-write community strings.
   This increases the security of your system against cyber attacks. Empty community strings are not allowed.



Result: You have configured SNMP in the properties of your project-integrated I-device.

Configuring SNMP for an I-device as a GSD file

To use an I-device in another project or Engineering System, export the configured I-device as a general station description file (GSD file) in STEP 7. When you import the GSD file in the desired project, STEP 7 shows the configured I-device as a GSD device (DP standard device) in the device or network view.

Before the GSD file export, define how you want to use SNMP on the DP standard device. As if STEP 7 V19, you have the following options in the settings of SNMP:

- Configuring of SNMP in the local settings of the I-device:
  Changes to the SNMP configuration in another project are prevented in the exported GSD file. The SNMP configuration options are not displayed on the inserted DP standard device.
- Configuring of SNMP by a higher-level IO controller in another project:
  The SNMP configuration must be created in the other project in the same way as for a standard IO device.
  Requirement:
  The option "Parameter assignment of PN interface by higher-level IO controller" is enabled at the I-device.

If you want to configure SNMP on the DP standard device in another project, make the following settings on the I-device CPU:

1. At the PROFINET interface of the CPU that is configured as an I-device:
   – Activate the "Parameter assignment of PN interface by higher-level IO controller" option in the Inspector window under "Properties > Operating mode".
2. In the SNMP settings of the I-device CPU:
   – Select the entry "via PROFINET interface ... (e.g. X1) from higher-level IO controller" from the drop-down list next to "SNMP configuration".
   In this case, the I-device takes over the SNMP configuration from the higher-level IO controller at its PROFINET interface X1.

Result: If using the I-device in another project as a DP standard device, you can configure SNMP the same as for a standard IO device.

If using the I-device as a shared I-device in multiple projects, the following applies: Configure SNMP only in the project with the controller to which the interface of the I-device was assigned.

7.15.2 Configuring DCP

Component interaction

DCP is a protocol for automatic detection and basic configuration of PROFINET devices. Consequently, DCP needs read and write access to the individual components in a PROFINET network.

To protect the components from malicious or inadvertent write access, the "Activate DCP write protection" function is available starting from STEP 7 V19.
When the "Activate DCP write protection" function is enabled on an IO device, the DCP write protection operates as follows on the individual components:

- The DCP write protection operates on the IO device and on the IO controller if an active communication relation exists between the IO device and the IO controller.
- The DCP write protection takes effect on the assigned IO controller of the IO device if the IO controller has established a communication relation with the IO device.

When configuring DCP, take into account the communication relations throughout the PROFINET network:

- An IO device has only one communication relation with its IO controller.
- A shared device/I-device has communication relations with all higher-level IO controllers.
- An IO controller has communication relations with all its assigned IO devices and shared devices/I-devices.

Consequently, DCP write access by the IO controller is only permitted again after all communication relations with DCP write protection with devices have been terminated and disabled (e.g. via one call each of D_ACT_DP).

To learn how to configure DCP, see the following sections.

NOTE

Avoidance of erroneous access attempts
Specific settings, such as changing of device names via DCP, only work for devices that are not currently participating in cyclic data exchange.

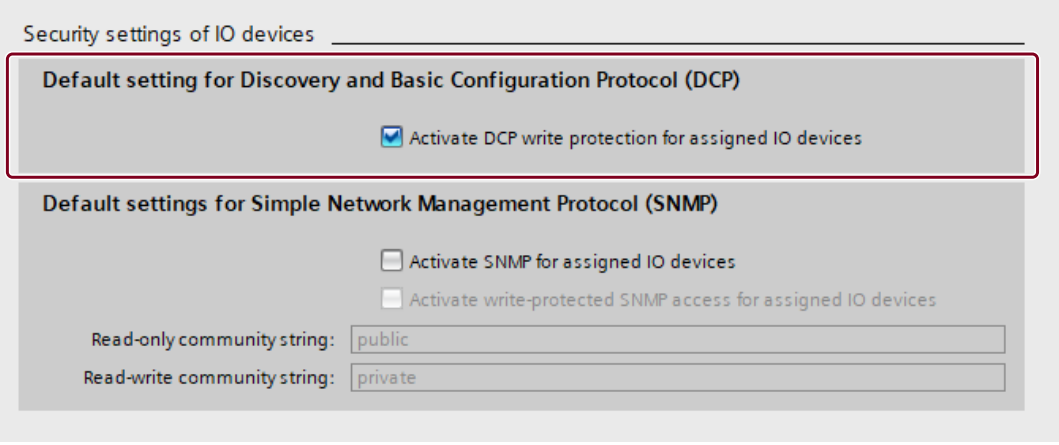
Configuring DCP for communication relations to all IO devices in the IO system

As of STEP 7 V20 and CPU FW version V4.0, you can configure DCP for an entire PROFINET IO system at the PROFINET interface of the IO controller. If IO devices support the configuring of DCP, the PROFINET interface of the higher-level IO controller synchronizes the DCP settings in the device properties of the IO devices by default. Changes to the DCP settings are also automatically synchronized.

Follow these steps to configure the DCP configuration for a PROFINET IO system:

1. Select the PROFINET interface of the IO controller in the network view or device view.
2. In the Inspector window, navigate to the "Advanced options > Security settings of the IO devices" area.
   STEP 7 as of V21 only displays this area if a PROFINET IO system has been added to the PROFINET interface of the IO controller.

3. If you want to use DCP write protection for communication with added IO devices, enable the "Activate DCP write protection for assigned IO devices" option in the "Default setting for Discovery and Basic Configuration Protocol (DCP)" area.

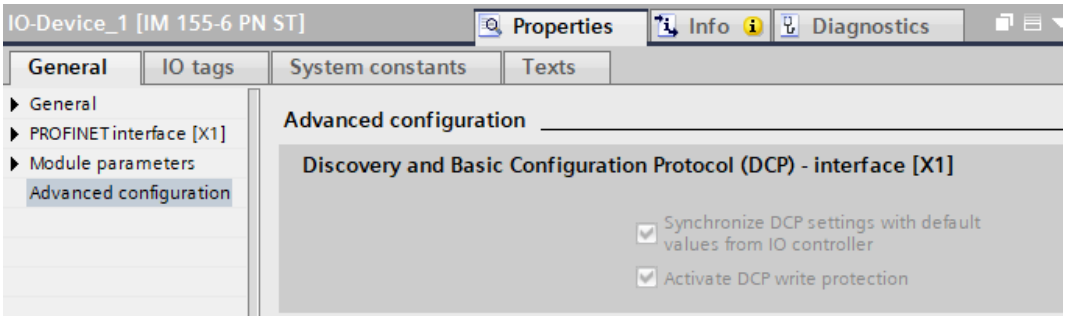


Result: You have configured DCP for the PROFINET IO system at a PROFINET interface of the IO controller.

Configuring DCP for a communication relation on an IO device

To configure DCP for a communication relation between IO controller and IO device, follow these steps:

1. Open the properties of the IO device in the network or device view.
2. Select the entry "Advanced configuration" under "General" in the Inspector window.



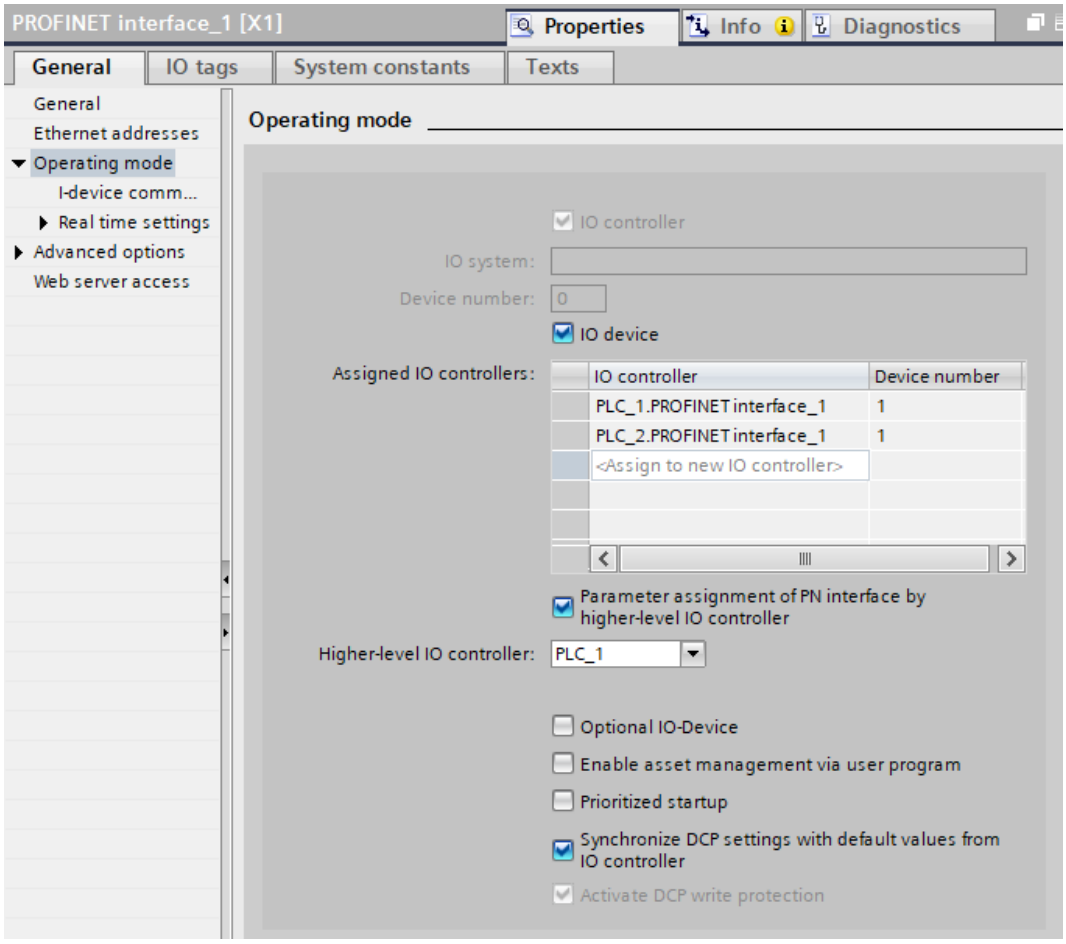
The "Synchronize DCP settings with default values from IO controller" and "Activate DCP write protection" options are enabled by default on all IO devices that support these functions. The options cannot be changed in the following cases:

- The IO device is not assigned to any IO controller.
- The IO controller to which the IO device is assigned does not support the "Activate DCP write protection" function.

Configuring DCP for a communication relation on an I-device

To configure DCP for a communication relation between an IO controller and I-device in a common project with the assigned IO controllers, follow these steps:

1. Open the properties of the required PROFINET interface, e.g. X1, in the network or device view.
2. Select the entry "Operating mode" under "General" in the Inspector window.



The "Activate DCP write protection" option is enabled by default on all I-devices that support this function. If an I-device can additionally synchronize the default values from the IO controller, the "Synchronize DCP settings with default values from IO controller" option is shown and enabled by default. The options cannot be changed in the following cases:

- The I-device is not assigned to any IO controller.
- The IO controller to which the I-device is assigned does not support the "Activate DCP write protection" function.

If you use an I-device as a shared I-device for IO controllers in different projects, the I-device will be inserted into other projects as a DP standard device. In this case, you therefore configure the DCP the same as for a standard IO device. The DCP write protection takes effect on each IO controller that has a communication relation with the shared I-device and supports the DCP write protection function.

PROFINET with the redundant S7-1500R/H system

8

Introduction

The same basic rules apply to PROFINET IO communication with the redundant S7-1500R/H as with the S7-1500 automation system. The redundant S7-1500R/H system exchanges IO data cyclically with the IO devices.

The redundant S7-1500R/H system supports a limited scope of PROFINET functions.

The redundant S7-1500R/H system supports media redundancy (MRP) in the PROFINET ring.

You can use the following IO devices on the redundant S7-1500R/H system:

- IO devices with system redundancy S2
- IO devices with system redundancy R1 (S7-1500H as of firmware version V3.0)
- Standard IO devices over the "Switched S1 device" function of the CPU

When configuring PROFINET with the redundant S7-1500R/H system, you must observe a few specifics, e.g. special configuration requirements.

Restrictions

- Real-time communication:
  - RT with a fixed send clock of 1 ms
  - No IRT
  - No MRPD redundancy procedure
  - No PROFINET with performance upgrade
- No isochronous mode
- No direct data exchange
- No operation as I-device
- No access to shared devices
- No support of docking systems
- No support of series machine projects
- Port options (only for PROFINET interface X1):
  - No port disabling possible
  - No configuring of boundaries possible
- Functionality as IO controller:
  - No prioritized startup
  - No enabling/disabling of IO devices
  - No support of series machine projects, e.g. IO systems that can be used multiple times
- PROFINET interface X2 does not support IO functionality (CPU 1515R/CPU 1517H/CPU 1518HF)
- No diagnostics using the web server
- No IP address assignment by the DHCP server

8.1 Media redundancy in the redundant S7-1500R/H system

You can use the redundant S7-1500R/H system in media redundancy networks (MRP). In this case, some or all PROFINET devices are connected to the S7-1500R/H with media redundancy via one or more PROFINET rings. If a PROFINET ring is interrupted, then a reconfiguration may occur. After a short reconfiguration time, the PROFINET devices can be accessed again via an alternative path. The PROFINET ring is mandatory for the redundant S7-1500R system.

S7-1500H CPUs as of FW version V4.0 have two ports at PROFINET interface X2, but do not support media redundancy (ring topology) at this PROFINET interface.

8.2 H-Sync Forwarding

Introduction

H-Sync Forwarding enables a PROFINET device with MRP to forward synchronization data (synchronization frames) of a S7-1500R redundant system only within the PROFINET ring.

In addition, H-Sync Forwarding forwards the synchronization data even during reconfiguration of the PROFINET ring. H-Sync Forwarding avoids a cycle time increase if the PROFINET ring is interrupted.

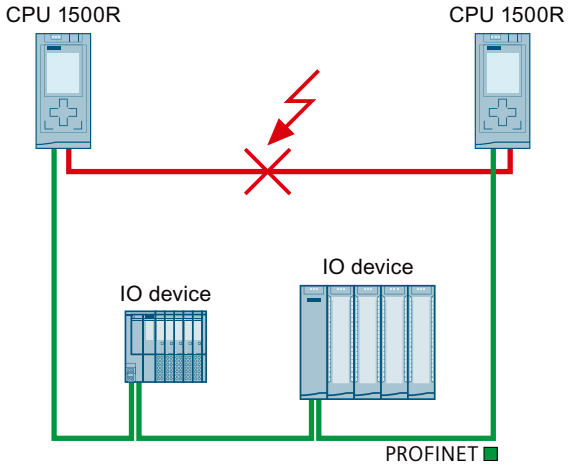
NOTE

Support of H-Sync Forwarding
The technical specifications typically state whether a PROFINET device supports H-Sync forwarding.
The GSD file will also indicate whether the device supports H-Sync Forwarding. The device supports H-Sync Forwarding when the "AdditionalForwardingRulesSupported" attribute in the "MediaRedundancy" element is set to "true".

Conditions

- H-Sync Forwarding is not relevant for redundant S7-1500H systems. With the redundant S7-1500H system, the H-Sync frames are transmitted exclusively via the fiber-optic cables.
- **When you use PROFINET devices with more than two ports (e.g. switch) in the PROFINET ring of an R-system, these devices must support H-Sync Forwarding.**
  H-Sync frames leave the PROFINET ring with a switch without H-Sync Forwarding. This results in an additional load on the network. Another serious result is that the redundancy of other R-systems in the network can fail or startup can be prevented.

- **H-Sync Forwarding is recommended if you are using PROFINET devices with only 2 ports in the PROFINET ring of an R-system**.
  When you operate PROFINET devices without H-Sync Forwarding in the PROFINET ring of the redundant S7-1500R/H system, the following scenario will result in an additional cycle time increase:



1. The redundant S7-1500R system is in the RUN-Redundant system state.
2. The PROFINET cable which directly connects the two CPUs fails.
3. The PROFINET ring is interrupted.
4. The PROFINET ring is being reconfigured.
5. PROFINET devices without H-Sync Forwarding do not forward any H-Sync frames during the reconfiguration time of the PROFINET ring.
6. The cycle time increases by the reconfiguration time of the PROFINET ring.

Figure 3-472 Failure of the PROFINET cable between the CPUs

If the cyclic program exceeds the cycle monitoring time, the time error OB (OB 80) may be started. Redundancy is lost if the time error OB (OB 80) is not present or the cycle time was exceeded twice with OB 80.

NOTE

If failure of the PROFINET cable that directly connects the two CPUs of the redundant S7-1500R system is unlikely, you can use PROFINET devices without H-Sync Forwarding in the PROFINET ring of the redundant S7-1500R system.
Example: Both CPUs of the redundant S7-1500R system are located directly next to each other in the control cabinet. In this case, it is unlikely that the PROFINET cable will fail.

8.3 System redundancy S2

Introduction

System redundancy S2 is the connection of an IO device via an interface module that supports two ARs to the IO controllers in the redundant system.

IO devices with system redundancy S2 enable uninterrupted process data exchange with the S7-1500R/H redundant system in the event of:

- a CPU fails
- Interruption of the PROFINET ring
- Interruption of the line topology (for S7-1500H as of FW version V3.0)

An IO device with system redundancy S2 supports system redundancy ARs.

In a redundant system, an IO device with system redundancy S2 has a system redundancy AR with each of the two CPUs (IO controllers). An IO device thus supports ARs of two IO controllers simultaneously (for the same modules).

A system redundancy AR can be either a primary AR or a backup AR. An IO device activates the data of the primary AR at the outputs. The data of the backup AR are not initially evaluated.

In STEP 7, you configure system redundancy S2 for an IO device by assigning the IO device to both CPUs of the S7-1500R/H redundant system.

Behavior in system state RUN-Redundant

Both CPUs are IO controllers. The PROFINET communication runs simultaneously on both system redundancy ARs, in each case between one of the CPUs (IO controllers) and the IO device. If the primary CPU fails or is switched to STOP, then the backup CPU becomes the primary CPU and also switches the backup AR to primary AR. The data of this AR becomes active at the outputs.

Abbreviations used for AR in the figure below:

- P-AR: Primary AR
- B-AR: Backup AR

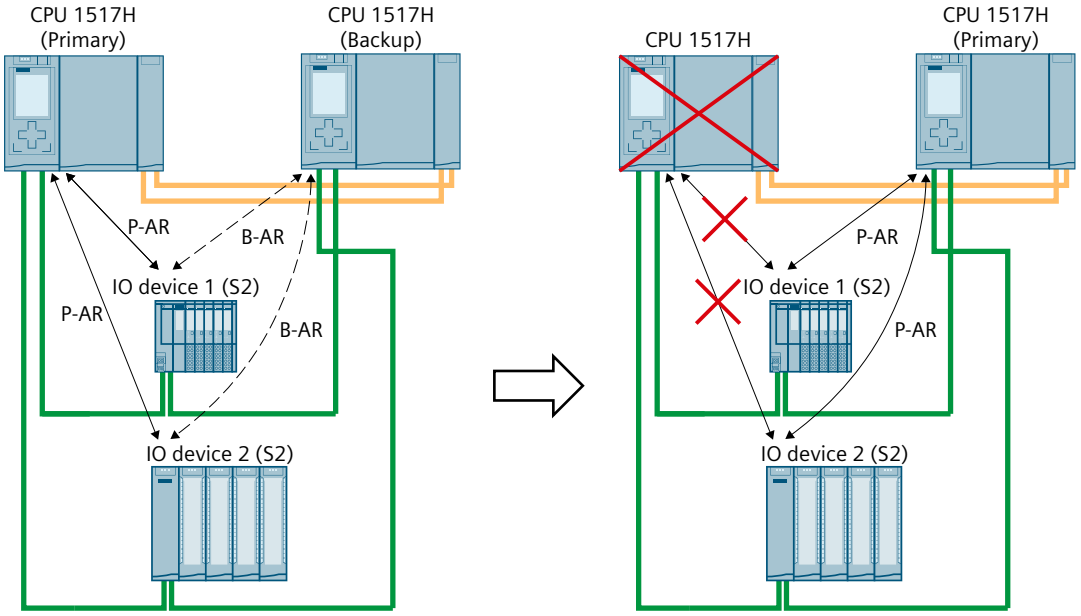


Figure 3-473 Primary backup AR

NOTE

S7-1500H with line topology

With line topology, only the primary AR can fail. In this case, the system switches to the backup AR, but the operating states and the roles of the CPUs remain unchanged.

Behavior in system state RUN-Solo

Only the primary CPU is an IO controller. The PROFINET communication runs on the primary AR between the primary CPU (IO controller) and the IO device. There is no AR between the backup CPU and the IO device.

8.4 System redundancy R1

Introduction

System redundancy R1 is the connection of an IO device via two interface modules, each of which supports an AR to the IO controllers in the redundant system.

IO devices with system redundancy R1 enable uninterrupted process data exchange with the S7-1500H redundant system when:

- a CPU fails
- an interface module fails
- a subnet fails.

Unlike system redundancy S2, system redundancy R1 has a separate interface module for each of the two ARs. Due to these redundant interface modules, the availability is higher than with an S2 device.

In STEP 7 you configure an IO device with system redundancy R1 by:

- Connecting the left interface module of the R1 device to the left H-CPU in the network view.
- Connecting the right interface module of the R1 device to the right H-CPU in the network view.

Reference

You can find information about the setup variants with the redundant system S7-1500R/H in the System Manual Redundant System S7-1500R/H (https://support.industry.siemens.com/cs/us/en/view/109754833).

Behavior in system state RUN-Redundant

The PROFINET communication runs on both system redundancy ARs simultaneously, each between one of the CPUs (IO controller) and an interface module of the R1 device.

In the event of a failure of an interface module of an R1 device or a line break in the line topology, only the ARs switch over. The roles of the H-CPUs do not change.

Abbreviations used for AR in the figures below:

- P-AR: Primary AR
- B-AR: Backup AR

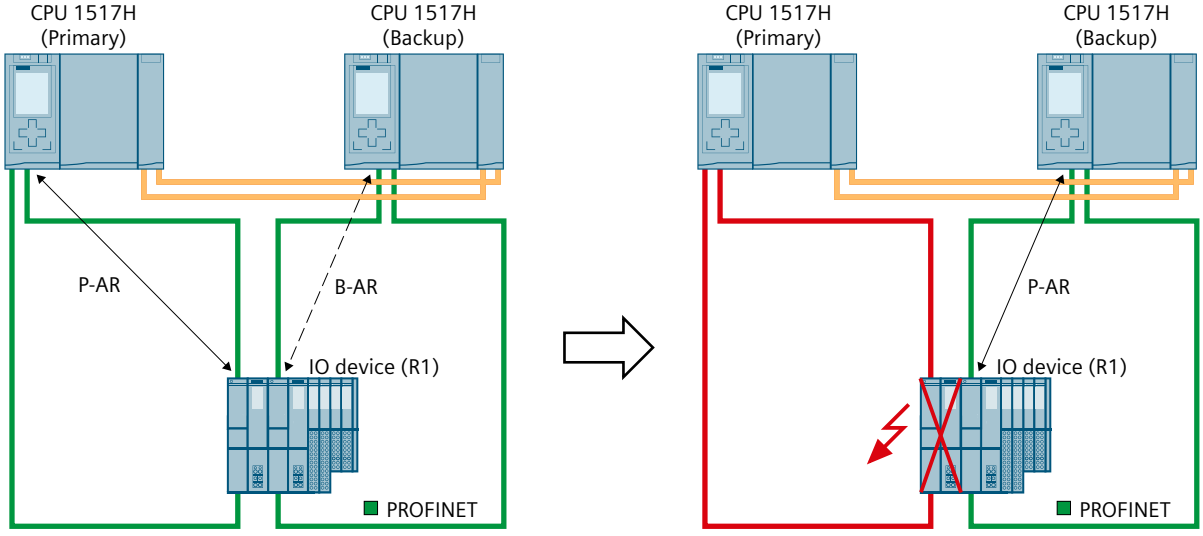


Figure 3-474 Failure of an interface module of an R1 device in the redundant S7-1500H system

If, however, the primary CPU fails or is switched to STOP, the S7-1500H redundant system then behaves as follows:

- The previous backup CPU becomes the new primary CPU.
- The new primary CPU uses the AR to the other, functioning interface module of the IO device and still has access to the inputs and control over the outputs of the IO device.
- The AR between the previous primary CPU and the assigned interface module is disconnected.

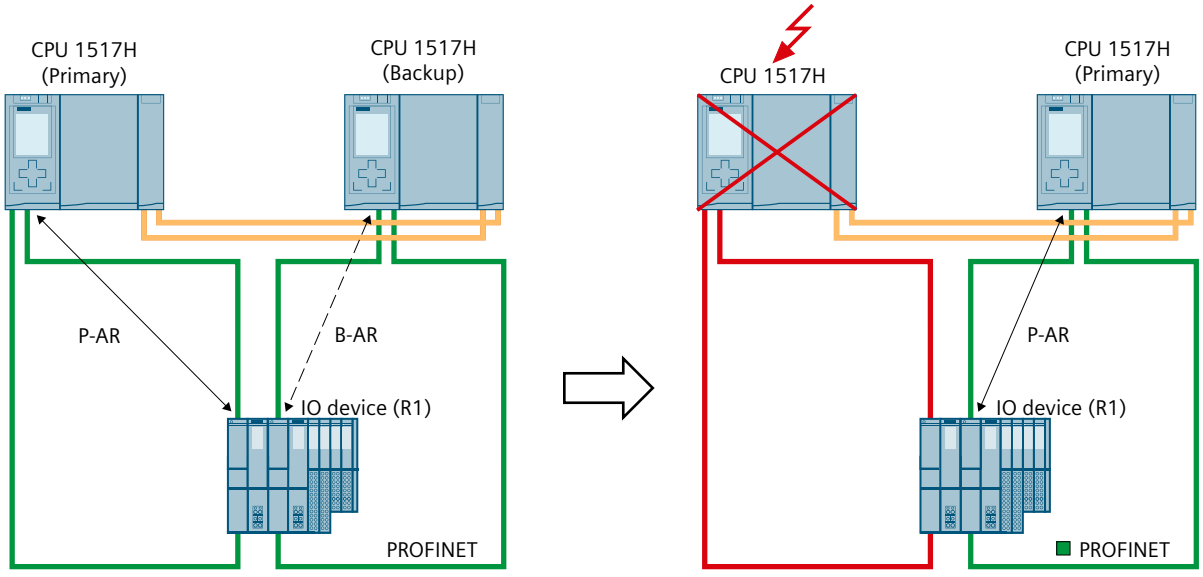


Figure 3-475 Failure of a CPU in the redundant S7-1500H system

NOTE

S7-1500H with line topology

With line topology, only the primary AR can fail. In this case, the system switches to the backup AR, but the operating states and the roles of the CPUs remain unchanged.

Behavior in system state RUN-Solo

Only the primary CPU is an IO controller. PROFINET communication runs on the AR between the primary CPU (IO controller) and the interface module of the IO device assigned to the primary CPU. The backup CPU separates all its ARs.

8.5 Switched S1 device

Introduction

As of FW version V2.8, the S7-1500R/H redundant system supports the "Switched S1 device" function.

The "Switched S1 device" function of the CPU enables operation of standard IO devices on the S7-1500R/H redundant system.

Standard IO devices, too, are always assigned to both CPUs of the S7-1500R/H redundant system. In contrast to an IO device with system redundancy S2, a standard IO device supports only one AR. The AR is available to the primary CPU of the redundant S7-1500R/H system.

In STEP 7 you configure an IO device connected via the "Switched S1 device" function by assigning a standard IO device to both CPUs of the redundant S7-1500R/H system.

As of FW version V3.0, the backup CPU of S7-1500H can establish an AR to an S1 device in a line topology. The primary CPU then receives data via the backup CPU.

NOTE

Standard IO devices in the redundant system S7-1500R

Standard IO devices usually do not support H-Sync Forwarding (Page 320).

To avoid a cycle time increase when the PROFINET ring is interrupted, integrate the standard IO devices downstream of a switch and not in the PROFINET ring.

Behavior in system state RUN-Redundant

The PROFINET communication runs on the AR between one of the CPUs (IO controller, in this example the primary CPU) and the standard IO device. There is no AR between the backup CPU and the standard IO device.

If the primary CPU fails or is switched to STOP, the S7-1500R/H redundant system responds as follows:

- The AR between the primary CPU and the standard IO device is disconnected.
- The previous backup CPU becomes the new primary CPU.
- The S7-1500R/H redundant system temporarily has no access to the inputs and no control over the outputs of the standard IO device. During this time, the configured substitute value behavior applies to the standard IO device.
- The new primary CPU builds an AR to the standard IO device.
- As soon as the new primary CPU has set up the AR, the S7-1500R/H redundant system has access to the inputs again and control over the outputs of the standard IO device.

Abbreviation used for AR in the figures below:

- AR: "normal" AR between a standard IO device and a CPU of the redundant system S7-1500R/H.

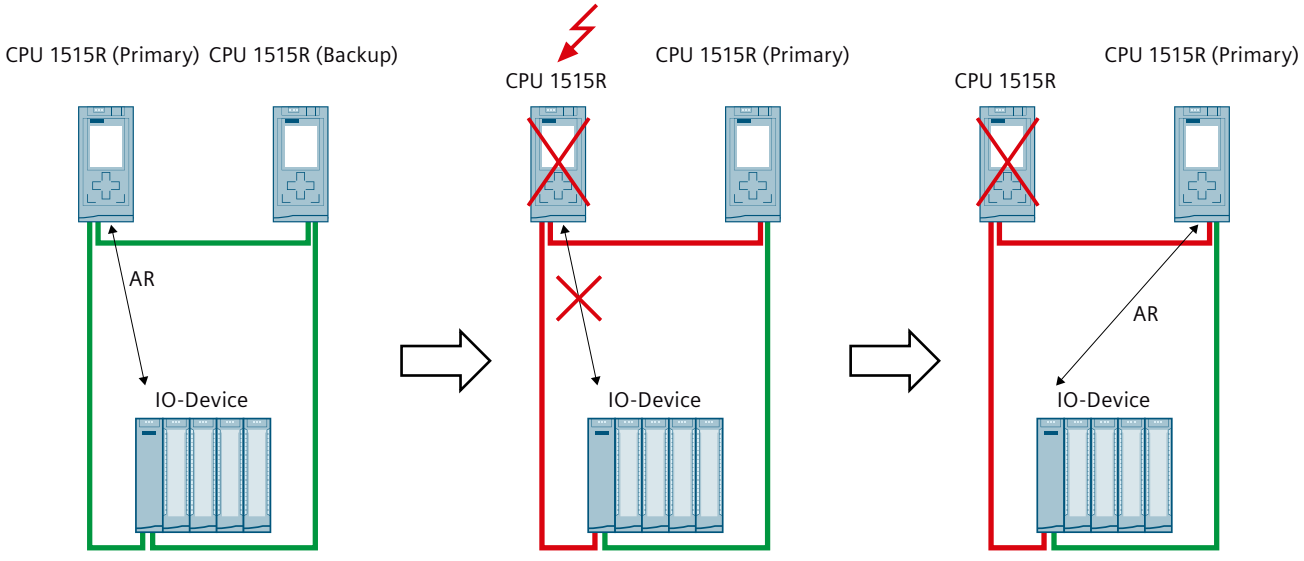


Figure 3-476 Behavior of standard IO devices in case of failure of the primary CPU

If a line in a line topology fails, the redundant S7-1500H system behaves as follows:

- If the line between the primary CPU and a standard IO device is interrupted, then the redundant S7-1500H system temporarily has no access to the inputs and no control over the outputs of the standard IO device. The status of the outputs depends on the substitute value behavior of the respective channels.
- The respective other CPU establishes an AR to the standard IO device.
- Once the new AR has been set up, the redundant S7-1500H system again has access to the inputs and control over the outputs of the standard IO device.

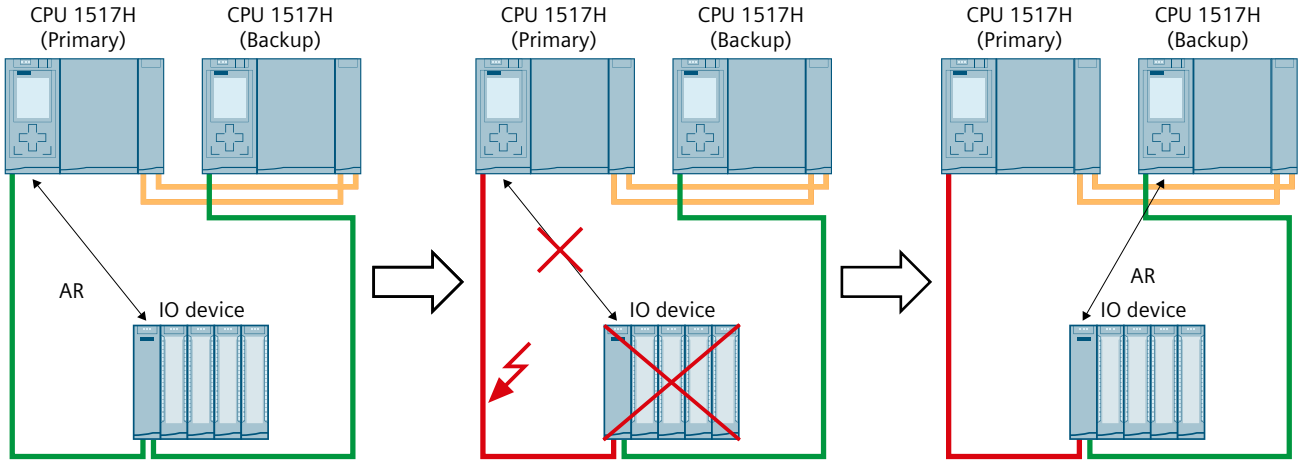


Figure 3-477 Behavior of standard IO devices in case of line failure

Behavior in system state RUN-Solo

Only the primary CPU is an IO controller. PROFINET communication runs on the AR between the primary CPU and the standard IO device. There is no AR between the backup CPU and the IO device.

OB behavior for standard IO devices with primary-backup switchover

If the primary CPU fails or goes to STOP, the standard IO devices temporarily fail. OB 72 "Redundancy error" is called, additional OB 86 "Module rack failure" for the failed IO devices are not called. To detect the failed IO devices, call the DeviceStates instruction in OB 72.

With the "Switched S1 device" function, the new primary CPU establishes the ARs to the standard IO devices again. OB 86 is called for each return of an IO device.

Influence changeover time of switched S1 devices

As of FW version V2.9, you can influence the changeover time between disconnection and return of switched S1 devices after a failure/STOP of the primary CPU.

Advantages:

- Optimization of the changeover time between disconnection and return of switched S1 devices
- Prioritization of the return of S1 devices in the PROFINET ring by setting a lower changeover time for S1 devices with important process functions.

The changeover time depends on the watchdog timer of the switched S1 device. The watchdog timer is the product of the update time multiplied by the accepted update cycles without IO data. With the parameters, you influence the time as of which the new primary CPU starts returning the S1 device. The return also depends on the amount of time that is required for the parameter assignment of the S1 device.
You set the parameters in STEP 7 in the properties of the interface of each S1 device:

- Update time: Advanced options > Real time settings > IO cycle > Update time
- Watchdog timer: Advanced options > Real time settings > IO cycle > Watchdog timer > Accepted update cycles without IO data

Setting a shorter changeover time of an S1 device: Reduce the values of the parameters/of a parameter.

Setting a longer changeover time of an S1 device: Increase the values of the parameters/of a parameter.

8.6 Main differences between IO device with system redundancy S2, R1 and standard IO device

Table 3-52 Main differences between IO device with system redundancy S2, R1 and standard IO device

Property	IO device with system redundancy S2	IO device with system redundancy R1	Standard IO device
Requirement for IO device	Device supports system redundancy S2	Device supports system redundancy R1	-
Maximum simultaneously supported ARs with regard to the same modules	2	2	1
Behavior when replacing the primary CPU	Continuous connection with S7-1500R/H redundant system Process data is transferred further.	Continuous connection with redundant S7-1500H system Process data is transferred further.	Temporary disconnection from S7-1500R/H redundant system. No process data is transferred until the standard IO device is available again. The status of the outputs depends on the substitute value behavior of the respective channels.
Behavior in case of failure of an interface module	Failure of the S2 device	R1 device continues to transmit process data via the redundant interface module	Failure of the standard IO device
Number of interface modules per device	1	2	1
Number of ARs per interface module	2	1	1

8.7 Installation guidelines

Configuration requirements for the topology with the redundant S7-1500R system

Topology properties	PROFINET ring
MRP role of the CPU	Manager (auto)
MRP role of the IO devices	Client
Other S7-1500R/H systems	No

Port interconnection:

- The two CPUs are directly interconnected via one of the two ports of PROFINET interface X1. No other devices of the ring are located in between.
- The two CPUs can be indirectly interconnected via the other two ports. The other devices of the ring are located in between. See the examples below.

Table 3-53 Number of PROFINET devices, IO devices in the redundant system

Maximum number of devices	Maximum number of S7-1500R
Maximum number of PROFINET devices in the PROFINET ring of the R system The maximum number includes switches, S7-1500R/H CPUs, S7-1500 CPUs (as of V2.5) and HMI devices. It does not include media converters.	50 (recommendation 16)[1]
Maximum number of IO devices that can be connected to the R-CPUs	64

1) Recommendation: The number of devices in the PROFINET ring affects the availability of the S7-1500R system. The number of PROFINET devices including R-CPUs in the PROFINET ring should not exceed 16. If you operate significantly more devices in the PROFINET ring, the availability is reduced.
The technical specifications in the documentation are based on the recommended maximum of 16 PROFINET devices in the ring in S7-1500R.

Configuration requirements for the topologies with the redundant S7-1500H system

Topology properties	PROFINET ring	Line topology	Combined topology	H-CPUs without additional devices
MRP role of the CPU	Manager (auto)	Not device in the ring		Not device in the ring
MRP role of the IO devices	Client	Not device in the ring	Depending on the installation location: Not device in the ring **or** client	-
Other S7-1500R/H systems	No	Yes		Yes

Table 3-54 Number of PROFINET devices, IO devices in the redundant system

Maximum number of devices	**Maximum number of S7-1500H**
Maximum number of PROFINET devices in the PROFINET ring of the R/H system The maximum number includes switches, S7-1500R/H CPUs, S7-1500 CPUs (as of V2.5) and HMI devices. It does not include media converters.	50
Maximum number of IO devices that can be connected to the H-CPUs	256

8.8 Configuring PROFINET IO on a redundant S7-1500R/H system

PROFINET IO configurations with the redundant S7-1500R/H system

The following figures show you examples of PROFINET IO configurations with the redundant S7-1500R/H system.

Abbreviations of AR used in the following figures:

- SR-AR: System redundancy AR between an IO device (S2/R1) and a CPU of the redundant S7-1500R/H system
- AR: "normal" AR between a standard IO device and the associated IO controller

S2 IO devices in the PROFINET ring

The redundant S7-1500R system consists of the two CPUs 1515R and two S2 devices in the PROFINET ring. The IO devices support MRP and H-Sync forwarding.

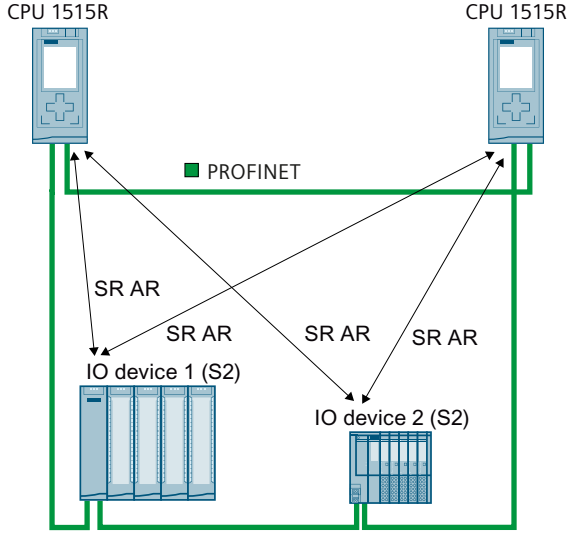


Figure 3-478 Example of a S7-1500R redundant system with two IO devices in the PROFINET ring

IO devices R1 in PROFINET rings

The redundant system S7-1500H consists of the two CPUs 1517H and two R1 devices in two PROFINET rings. The IO devices support MRP.

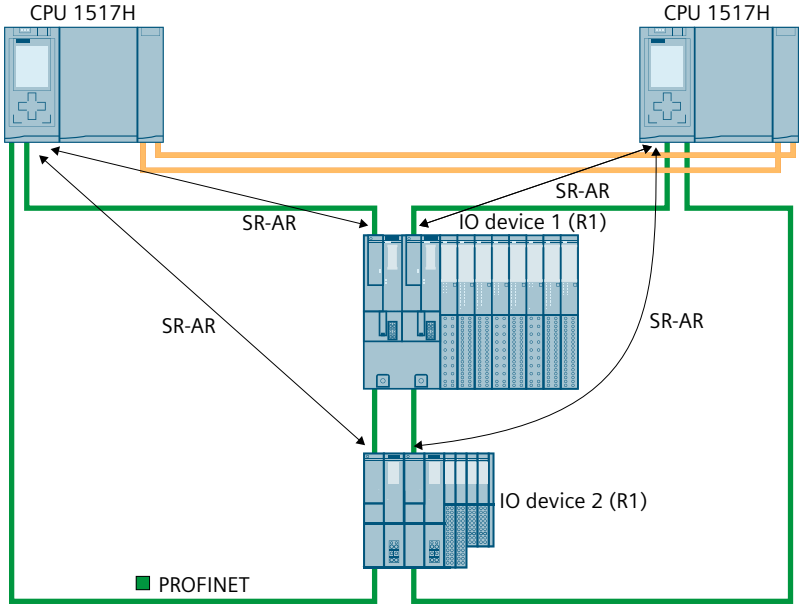


Figure 3-479 Example of a redundant S7-1500H system with two IO devices in two PROFINET rings

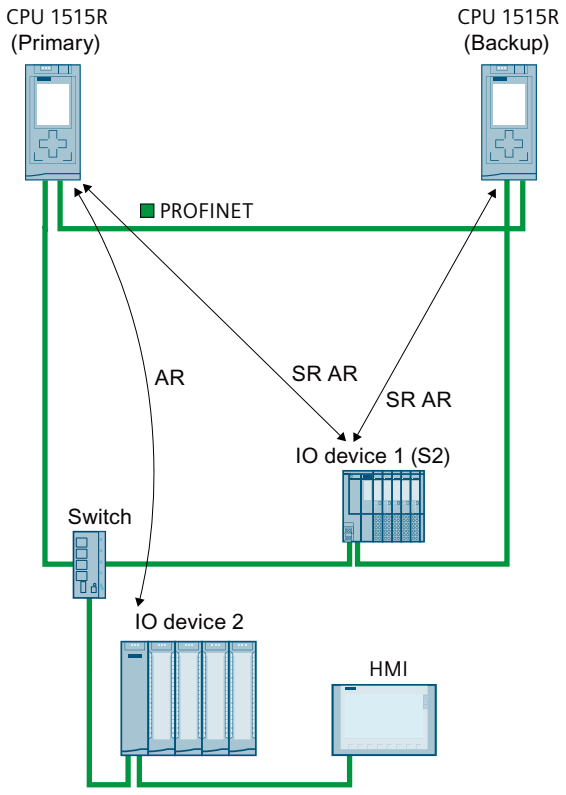
PROFINET devices downstream of a switch

To connect additional PROFINET devices to the PROFINET ring, use a switch. For the redundant S7-1500R system, ensure that a switch in the PROFINET ring supports H-SYNC Forwarding in addition to MRP.

You connect the following devices to the PROFINET ring with a switch.

- PROFINET devices with one port
- Non MRP-capable PROFINET devices
- PROFINET devices that do not support H-Sync Forwarding, such as standard IO devices.

The following figure shows a redundant S7-1500R system with connected PROFINET devices downstream of a switch.



IO device 1 (S2)	IO device 1 is located in the PROFINET ring. The IO device 1 supports system redundancy S2, MRP and H-Sync Forwarding.
Switch	The switch is located in the PROFINET ring. The switch supports MRP and H-SYNC Forwarding.
IO device 2	The IO device 2 is connected to the PROFINET ring via the switch. IO device 2 is a standard IO device that is connected to the redundant S7-1500R system via the "Switched S1 device" function.
HMI device	The HMI device is connected to the PROFINET ring via the switch.

Figure 3-480 PROFINET devices downstream of a switch

Additional PROFINET IO system in the configuration

The configuration can also contain additional IO controllers with their own IO devices. To have enough bandwidth in the PROFINET ring for the redundant S7-1500R/H system, place additional IO controllers with their I/O devices downstream of a switch.

When determining the maximum number of IO devices inside and outside the PROFINET ring, the redundant system in STEP 7 does not recognize the S7-1500 CPUs. If you use S7-1500 CPUs, you must check the maximum number yourself.

The CPU supports H-Sync forwarding and thus may be a node of the PROFINET ring.

The following figure shows a redundant S7-1515R system. An additional PROFINET IO system with a CPU 1516 as IO controller is located downstream of the switch. A separate standard IO device has been assigned to the IO controller.

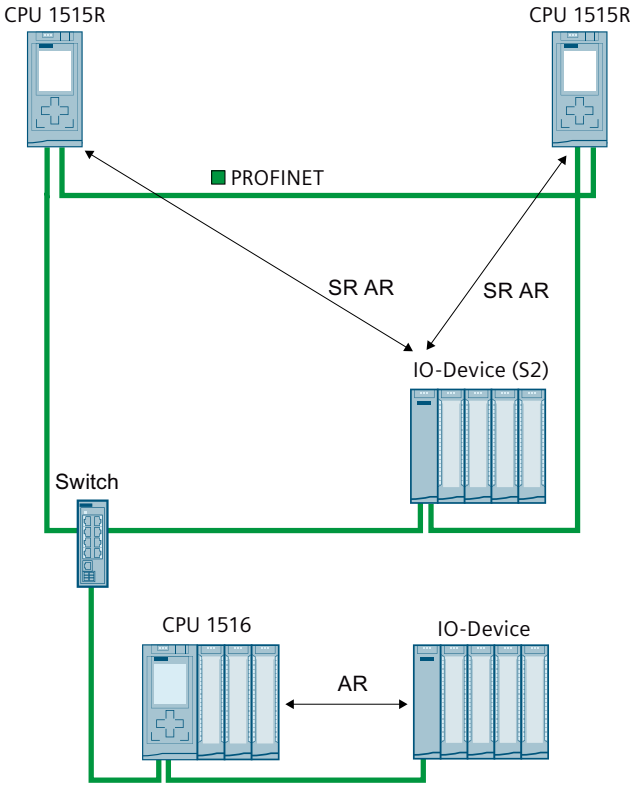


Figure 3-481 Example of a redundant S7-1500R system with an additional PROFINET IO system

Additional IO controllers can also be connected as I-device to the redundant S7-1500R/H system. An I-device is connected like a standard IO device to the redundant S7-1500R/H system.
The redundant S7-1500R/H system supports the use of I-devices only via GSD file and as standard IO device.

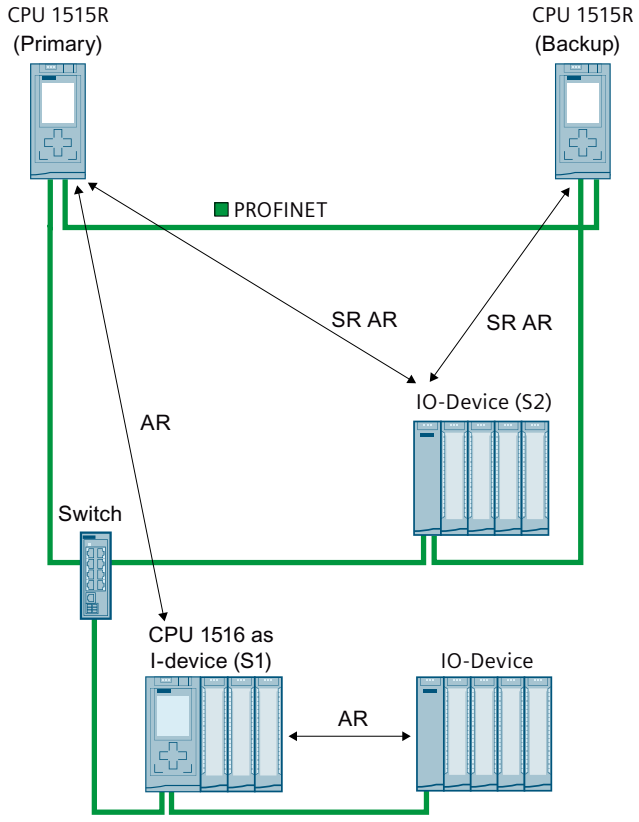


Figure 3-482 I-device downstream of a switch

Connection to another PROFINET IO system via the PN/PN coupler

The redundant S7-1500R/H system cyclically exchanges IO data with another PROFINET IO system via a PN/PN coupler.

In the following figure, the PN/PN coupler connects a redundant S7-1515R system to another PROFINET IO system. The left side of the PN/PN coupler is assigned to the redundant S7-1515R system. The assignment is system-redundant and media-redundant. The right side of the PN/PN coupler is assigned to the CPU 1516 (IO controller). The PROFINET IO system of the CPU 1516 has no redundancy in this example.

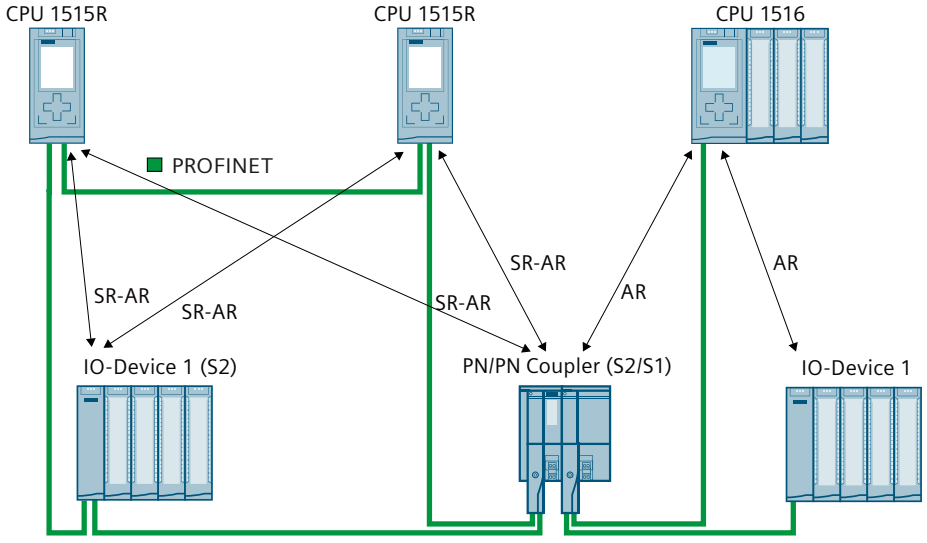


Figure 3-483 Configuration with the PN/PN coupler with one-sided system redundancy (S2/S1)

Connection to an additional redundant S7-1500R/H system via the PN/PN coupler

Two redundant S7-1500R/H systems cyclically exchange IO data via the PN/PN coupler.

In the following figure, the PN/PN coupler connects two redundant S7-1515R systems to each other. Each of the two PN/PN coupler sides are assigned to a redundant S7-1515R system. Each of the two sides of the PN/PN coupler are connected to the respective redundant S7-1515R system in a system-redundant and media-redundant manner.

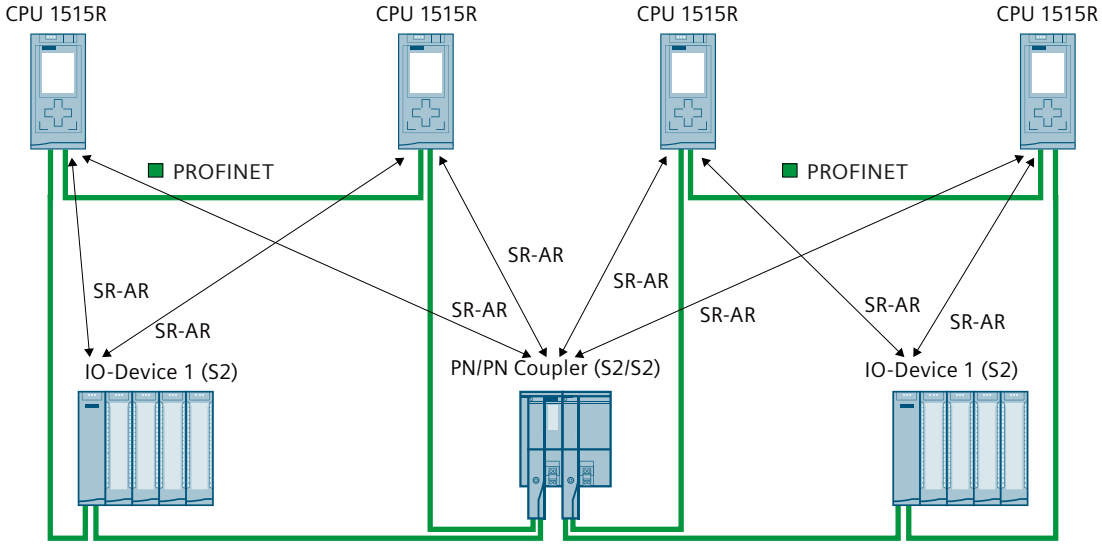


Figure 3-484 Configuration with the PN/PN coupler with two-sided system redundancy (S2/S2)

Reference

You can find more information on the PN/PN coupler in the PN/PN Coupler (https://support.industry.siemens.com/cs/ww/en/view/44319532) manual.

Gateway from a PROFINET IO system to PROFIBUS DP nodes

You can extend the redundant S7-1500R/H system by a gateway from PROFINET IO to PROFIBUS DP with an IE/PB LINK HA. Related information and configuration options can be found in the S7-1500R/H System Manual (https://support.industry.siemens.com/cs/ww/en/view/109754833).

8.9 Assigning IO device to the redundant S7-1500R/H system

Using two examples, this section describes how to assign IO devices to the redundant S7-1500R/H system.

- Procedure for S7-1500R with S2 or S1 devices.
- Procedure for S7-1500H with R1 devices.

Requirements

- Redundant S7-1500R/H system
- IO device:

Redundant system	Switched S1 device (Standard IO device)	IO device with System redundancy S2	IO device with System redundancy R1
S7-1500H as of firmware version V3.0	X	X	X
S7-1500R/H as of firmware version V2.8	X	X	-
S7-1500R/H with firmware version less than V2.8	-	X	-

Procedure for S7-1500R/H with S2/S1 devices

To assign S2 or S1 devices to the redundant S7-1500H system, connect the interface module of the IO device to each S7-1500H CPU.

1. In the network view of STEP 7, select the PROFINET interface of the IO device.
2. Drag-and-drop a line between the PROFINET interface of the IO device and the PROFINET interface X1 of the left CPU.

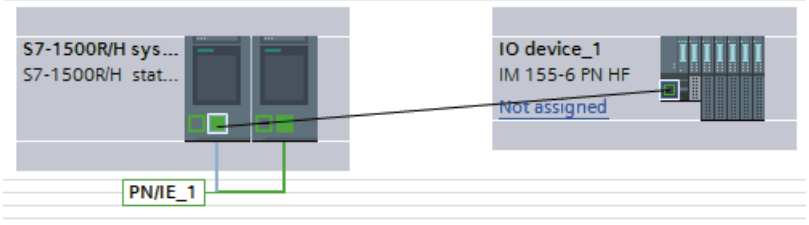


Figure 3-485 Assign IO device to the left CPU

3. Drag-and-drop a line between the PROFINET interface of the IO device and the PROFINET interface X1 of the right CPU.

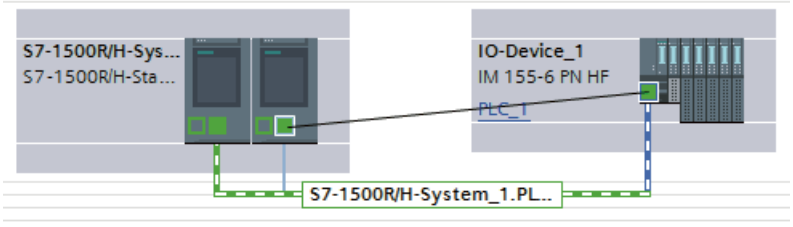


Figure 3-486 Assign IO device to the right CPU

Result: The IO device is connected to the redundant S7-1500R system.

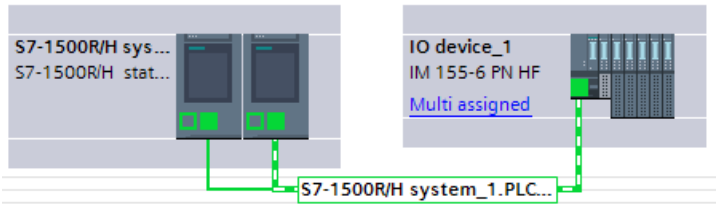


Figure 3-487 S2 device assigned

Procedure for S7-1500H with R1 devices

To assign R1 devices to the redundant S7-1500H system, connect each interface module of the R1 device to an H-CPU.

The left interface module of each R1 device must be connected to the left H-CPU in the network view. The right interface module of each R1 device must be connected to the right H-CPU in the network view.

To do so, proceed as follows:

1. Switch to the network view.
2. Drag-and-drop a line between the PROFINET interface of the left interface module of the ET200SP-R1_1 station and the PROFINET interface X1 of the left H-CPU.
3. Drag-and-drop a line between the PROFINET interface of the right interface module of the ET200SP-R1_1 station and the PROFINET interface X1 of the right H-CPU.
4. Switch to the device view of the ET200SP-R1_1 station and set the watchdog timer for both interface modules. To do this, navigate in the Inspector window to "Properties > PROFINET interface [X1] > Advanced options > Real-time settings > IO cycle".
5. Repeat steps 1 to 4 for the ET200SP-R1_2 station.

   Result: The R1 devices are connected to the S7-1500H redundant system.

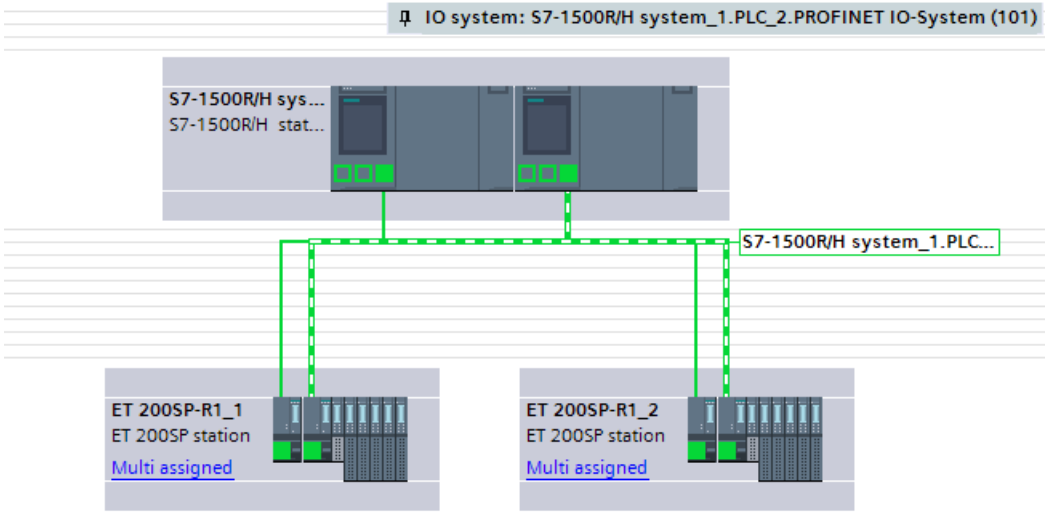


Figure 3-488 R1 devices assigned in the network view with system redundancy

NOTE

Alternative method for assigning IO devices.

For larger projects, we recommend assigning the IO devices as follows:

1. Switch to the network view.
2. Move the cursor over the station you want to assign.
3. Press the right mouse button and select "Assign to new DP master/IO Controller" in the shortcut menu.
4. Select both IO Controllers in the following dialog and then click on "Ok". This assigns the left interface module to the left IO Controller and the right interface module to the right IO Controller.
5. Repeat steps 2 through 4 for additional IO devices or mark several stations simultaneously.

I-device as standard IO device

If you want to assign an I-device to the redundant S7-1500R/H system, you have to include the configured I-device via its exported GSD file.

To operate an I-device as standard IO device on the redundant S7-1500R/H system, always use the GSD file of the I-device in the H-system configuration.

- SIMATIC CPU as I-device
  - First, configure the SIMATIC CPU in STEP 7 as an I-device with all transfer areas.
  - Export the I-device as a GSD file. The GSD export can be found in the properties of the PROFINET interface under "Operating mode > I-device communication > Export Generic System Description file (GSD)".
  - Install the GSD file in STEP 7.
- HMI device as I-device ("Direct key" function)
  - The GSD files for SIMATIC Comfort Panel and SIMATIC Mobile Panel can be found under the link at the end of this section.

Assign the I-device integrated via GSD file to the redundant system S7-1500R/H.

See also

GSD file HMIs (https://support.industry.siemens.com/cs/ww/en/view/73502293)

8.10 Configuring media redundancy (MRP) for a configuration with the redundant S7-1500R/H system

This section describes by means of two examples how to configure media redundancy (MRP) for a configuration with the redundant S7-1500R/H system.

- Configuring MRP for a configuration with S2 devices (ET 200SP) with the redundant S7-1500R system.
- Configuring MRP for a configuration with R1 devices (ET 200SP) with the redundant S7-1500H system.

Requirements

- Redundant S7-1500R/H system.
- All devices in the ring support the media redundancy protocol MRP.
- IO devices are assigned to the redundant S7-1500R/H system.
- The MRP domain "mrpdomain-2" was created in the domain settings (S7-1500H).

Configuring MRP for a configuration with S2 devices (ET 200SP) with the redundant S7-1500R system

Specifying MRP role and MRP domain of the CPUs of the redundant S7-1500R system
As soon as you create a redundant S7-1500R system in STEP 7, STEP 7 automatically assigns the MRP role "Manager (auto)" for the PROFINET interfaces X1 of the two CPUs.

Specifying MRP role and MRP domain for the S2 devices of the redundant S7-1500R system in STEP 7
To specify the media redundancy for additional devices in the ring, follow these steps:

1. In the network view of STEP 7, select the PROFINET interface X1 of one of the two CPUs of the redundant S7-1500R system.
2. In the Inspector window, navigate to "Properties > General > Advanced options > Media redundancy".
3. Click the "Domain settings" button.

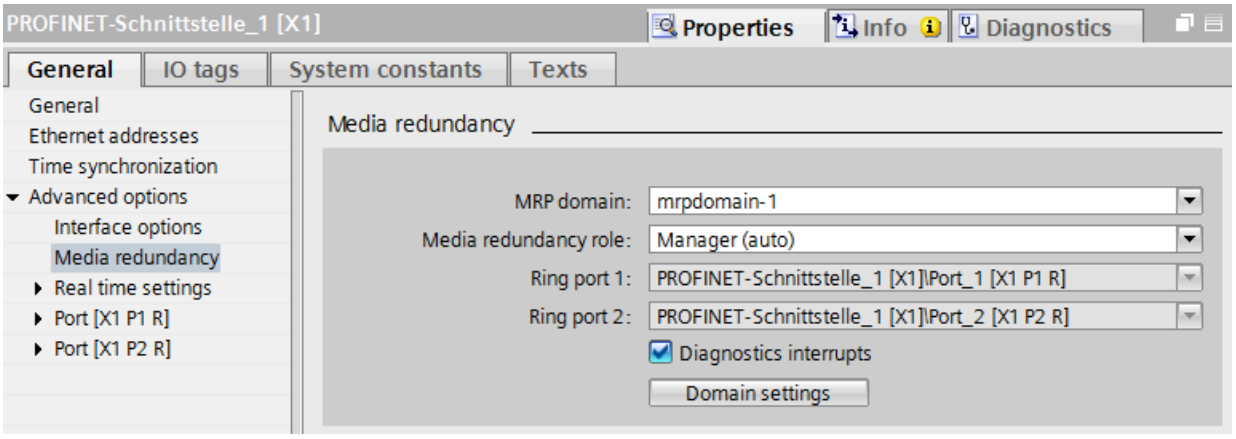


Figure 3-489 S7-1500R: MRP role "Manager (auto)"

In the Inspector window, STEP 7 displays the properties of the MRP domain in which the PROFINET interface X1 of the CPU is located.

4. In the "MRP role" column of the "Devices" table, assign the MRP role "Client" to all the other devices of the ring.

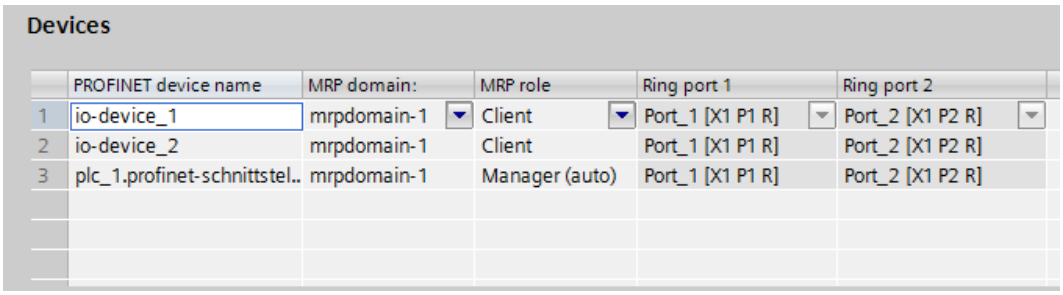


Figure 3-490 S7-1500R: Assigning MRP roles for ring devices

Configuring MRP for a configuration with R1 devices (ET 200SP) with the redundant S7-1500H system

Set MRP role and MRP domain of the CPUs of the redundant S7-1500H system

As soon as you create a S7-1500H redundant system in STEP 7, STEP 7 automatically assigns the MRP role "Not device in the ring" for the PROFINET interfaces X1 of the two CPUs. For the project engineering as PROFINET ring you have to change the MRP role to "Manager (auto)".

To change the MRP role of the redundant system, follow these steps:

1. Switch to the device view of the S7-1500H redundant system.
2. Select the PROFINET interface X1 of the upper H-CPU (mounting rail_0) of the S7-1500H redundant system.
3. In the Inspector window, navigate to "Properties > General > Advanced options > Media redundancy".
4. Change the MRP domain to "mrpdomain-1" (if required) and the media redundancy role for the H-CPU to "Manager (auto)".
5. Select the PROFINET interface X1 of the lower H-CPU of the S7-1500H redundant system.
6. Change the MRP domain to "mrpdomain-2" (if required) and the media redundancy role for the H-CPU to "Manager (auto)".
7. Enable the "Diagnostic interrupts" option.

NOTE

If the "Diagnostic interrupts" option is enabled, diagnostic interrupts are generated at the ring ports in the event of the following errors:
Wiring or port error:

- A neighbor of the ring port does not support media redundancy MRP.
- A ring port is connected to a non-ring port.
- A ring port is connected to the ring port of a different MRP domain.

You can find additional information in the STEP 7 online help.

Specifying MRP role and MRP domain for the R1 devices of the redundant S7-1500H system in STEP 7.

To define the media redundancy for the other devices (IO devices) of the rings, proceed as follows:

1. Switch to the device view of the left ET 200SP (ET200SP-R1_1).
2. Click on the PROFINET interface X1 of the left IM 155-6 PN R1.
3. Change the MRP domain to "mrpdomain-1" (if required) and the media redundancy role to "Client".
4. Click on the PROFINET interface X1 of the right IM 155-6 PN R1.
5. Change the MRP domain to "mrpdomain-2" and the media redundancy role to "Client".
6. Switch to the device view of the right ET 200SP (ET200SP-R1_2) and repeat steps 2 to 5.

NOTE

Alternative method for assigning MRP role and MRP domain.

1. Switch to the network view.
2. Click the connection PN/IE_1.
3. In the Inspector window, navigate to "Properties > General > MRP domains".
4. Scroll down to the "Devices" section.

- Under "PROFINET IO system", select the controller interface.
- Under "Devices" you configure the respective MRP domain and the MRP role.

8.11 MRP interconnection with the redundant system S7-1500R/H

- The S7-1500H CPUs support system redundancy R1 as of firmware version V3.0.
- The S7-1500R/H CPUs support MRP interconnection as of firmware version V2.9.

MRP interconnection enables the redundant data exchange via S7-1500R/H across two or more MRP rings.

Requirements for S7-1500R/H

In addition to the requirements for S7-1500, the following requirements are in effect for S7-1500R/H:

- For S7-1500R/H: The two CPUs of the redundant system are located in the same ring (as of firmware version V2.9).
- For S7-1500H: The two CPUs of the redundant system are located in one or two rings (as of firmware version V3.0).
- You have configured the media redundancy role of the two CPUs as "Manager (auto)" in the ring with the two R/H CPUs.

  You have configured the following in the other rings:

  – For one or more PROFINET devices the media redundancy role "Manager (auto)" or
  – For exactly one PROFINET device the media redundancy role "Manager"

  You have assigned the MRP client role to the other devices in all rings.

Topology with S2 devices

Topology with two rings, using the example of S7-1500R
The following figure shows the redundant coupling based on the example of S7-1500R in 2 rings.

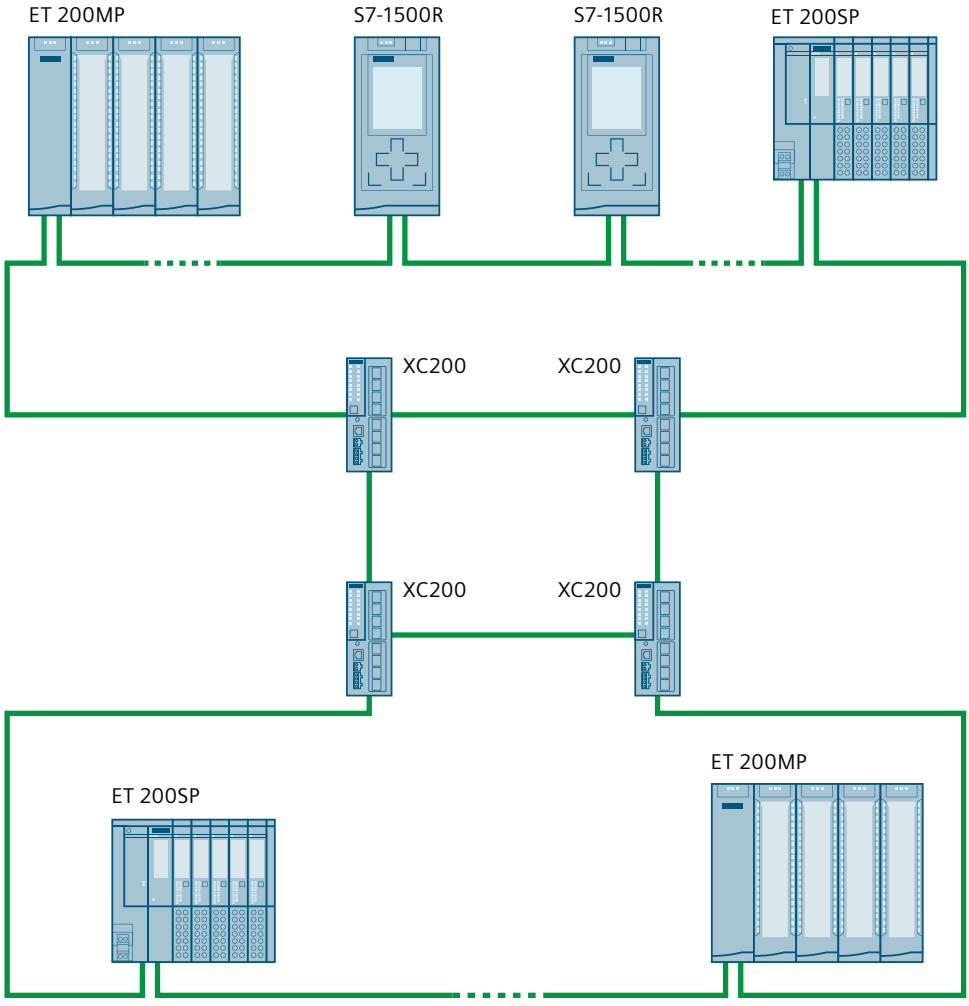


Figure 3-491 Example: Redundant connection of S7-1500R in 2 rings with MRP interconnection

Topology with two rings, using the example of S7-1500H
The figure below shows the redundant coupling, using the example of S7-1500H in two rings.

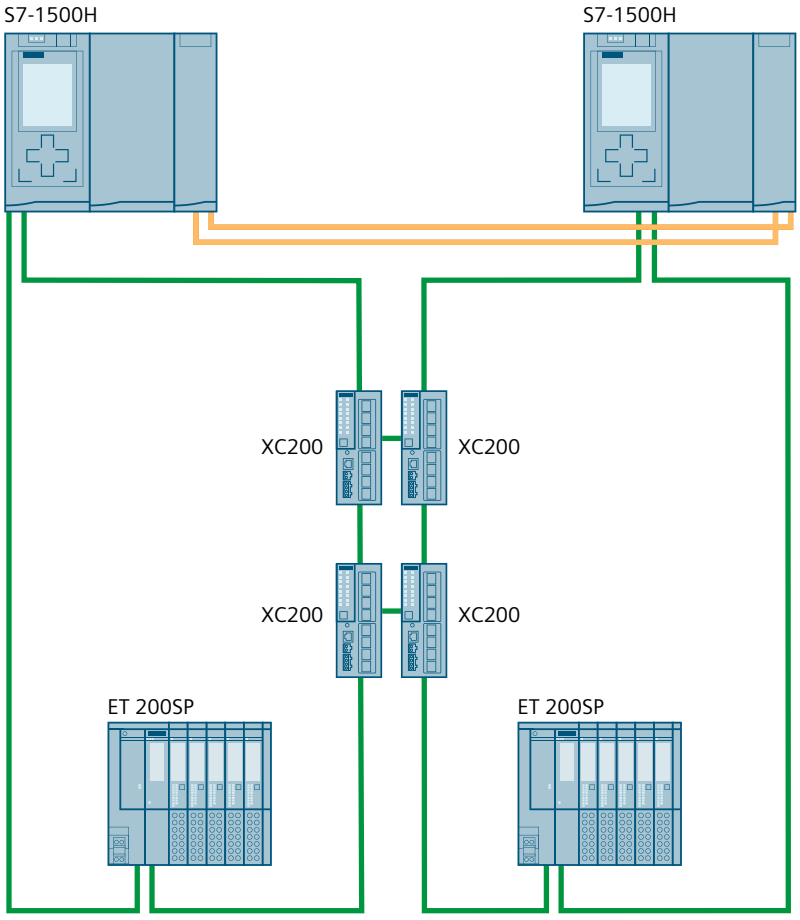


Figure 3-492 Example: Redundant connection of S7-1500H in two rings with MRP interconnection

Topology with multiple rings, using the example of S7-1500H
The figure below shows the redundant coupling, using the example of S7-1500H in four rings.

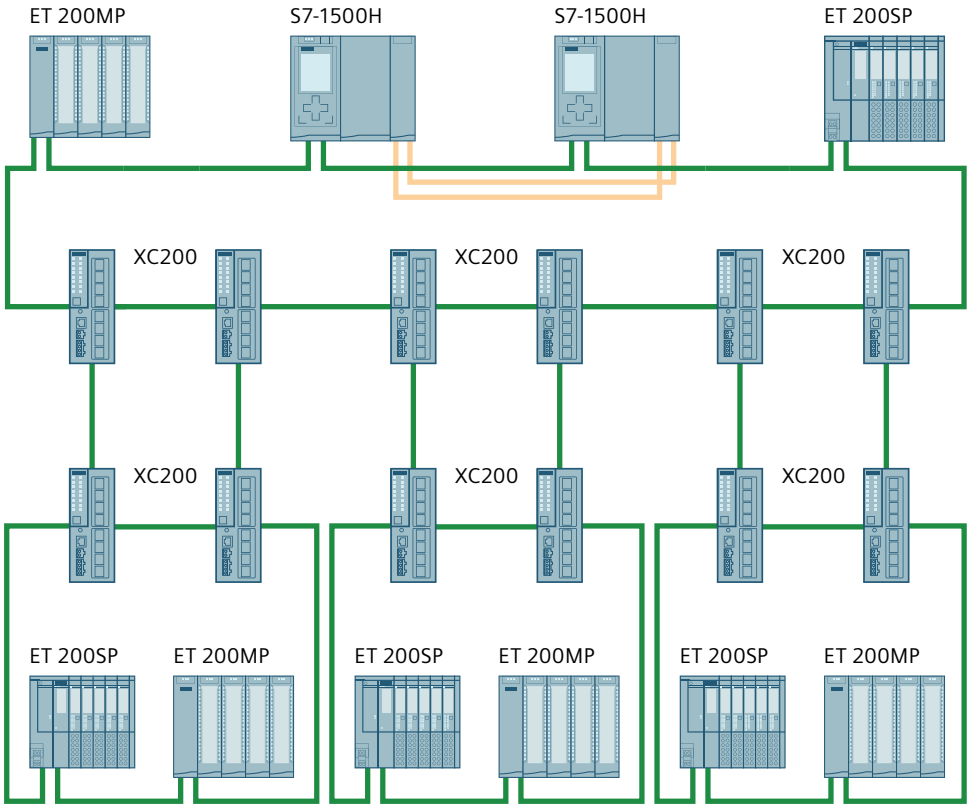


Figure 3-493 Example: Redundant coupling, using the example of S7-1500H in four rings

Topology with R1 devices

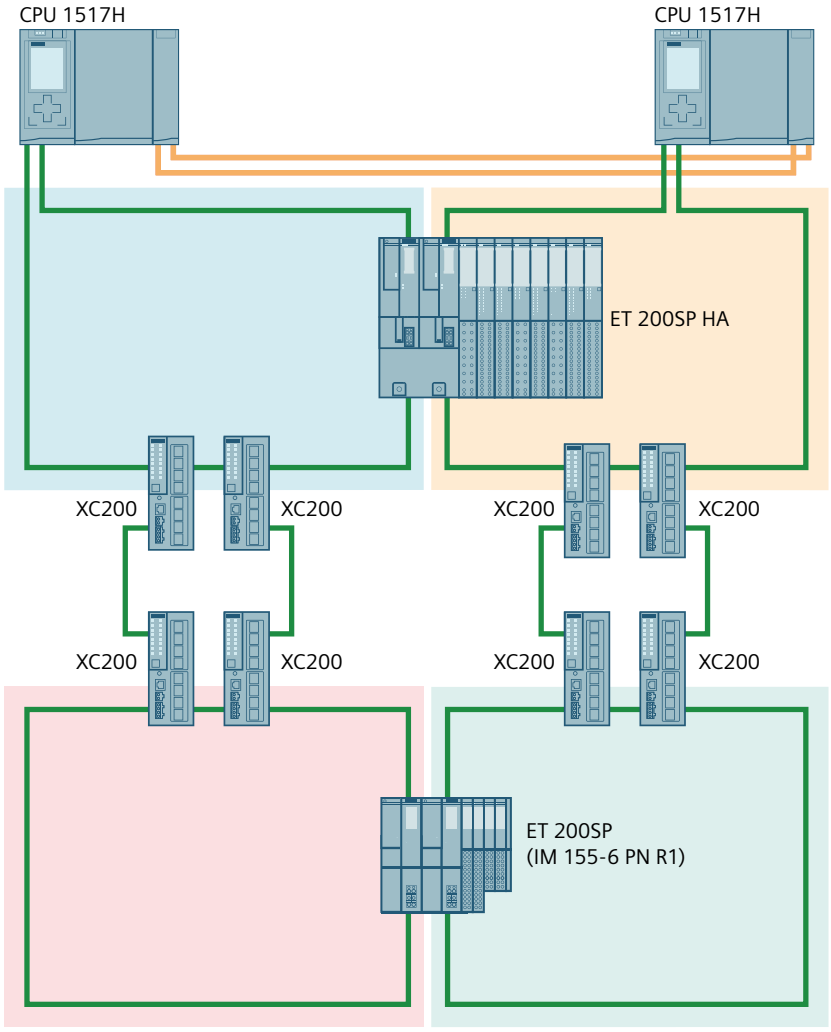


Figure 3-494 Example: S7-1500H configuration with R1 devices and switches with MRP interconnection in the PROFINET ring

Additional information

You can find all information that generally applies to MRP interconnection and thus also to redundant S7-1500R/H systems with MRP interconnection, in the section MRP interconnection (Page 194), for example, constraints, principle of operation, configuration and times.

Tool for setting the watchdog timer

For the correct setting of the watchdog timer, you can use the "S7-1500R/H AddIn (https://support.industry.siemens.com/cs/de/en/view/109769093)" which is available on the Internet and can also be used for MRP interconnections.

SIEMENS

SIMATIC

PROFIBUS
PROFIBUS with STEP 7 V13

Function Manual

Documentation guide 1

Description 2

Parameter assignment/addressing 3

Diagnostics 4

Functions 5

Service & Support A

12/2014
A5E03775446-AC

Preface

Purpose of the manual

This function manual provides an overview of the PROFIBUS communication system with SIMATIC STEP 7 V13.

STEP 7 V13 is integrated into the powerful graphic Totally Integrated Automation Portal (TIA Portal), the new integration platform for all automation software tools.

This function manual supports you in planning a PROFIBUS system. The manual is structured into the following subject areas:

- PROFIBUS basics
- PROFIBUS diagnostics
- PROFIBUS functions

Basic knowledge required

The following knowledge is required in order to understand the manual:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge about the use of Windows-based computers
- Proficiency with STEP 7

Scope

This function manual is the basic documentation for all SIMATIC products from the PROFIBUS environment. The product documentation is based on this documentation.

The examples are based on the functionality of the S7-1500 automation system.

Changes compared to previous version

As compared to the previous version (version 07/2014), this manual contains the following amendments/changes:

- Extension of the documentation to STEP 7 (TIA Portal) V13 SP1
- Addition of the function Intelligent DP slaves (I-slaves)
- New guide

Conventions

STEP 7: We refer to "STEP 7" in this documentation as a synonym for the configuration and programming software "STEP 7 as of V12 (TIA Portal)" and subsequent versions.

This documentation contains figures of the devices described. The figures may differ slightly from the device supplied.

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Additional support

You will find information about available technical support in the appendix Service & Support (Page 79).

The technical documentation for the individual SIMATIC products and systems is available on the Internet (http://www.siemens.com/simatic-tech-doku-portal).

The online catalog and the ordering system are available on the Internet (http://mall.industry.siemens.com).

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security on the Internet (http://www.siemens.com/industrialsecurity).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find more information on the Internet (http://support.automation.siemens.com).

Table of contents

1 Documentation guide 6

2 Description 9

2.1 Introduction to PROFIBUS 9
2.1.1 Applications of PROFIBUS DP 9
2.1.2 PROFIBUS terminology 11
2.1.3 PROFIBUS DP interface 13

2.2 Structure of PROFIBUS networks 14
2.2.1 Passive network components for RS 485 networks 15
2.2.1.1 RS 485 cables 15
2.2.1.2 PROFIBUS FastConnect system 16
2.2.1.3 PROFIBUS bus connector 18
2.2.1.4 M12 bus connector 20
2.2.1.5 Bus terminals for RS 485 networks 20
2.2.1.6 M12 bus terminating resistor 20
2.2.2 Passive components for optical networks 21
2.2.2.1 Fiber-optic cables 21
2.2.2.2 Plastic and PCF fiber-optic cables 22
2.2.2.3 Glass fiber-optic cables 23
2.2.3 Active network components 24
2.2.3.1 Network components in electrical networks 24
2.2.3.2 Network components in optical networks 28
2.2.4 Examples for topology 29
2.2.4.1 Topology with RS485 repeater 29
2.2.4.2 Topology with diagnostic repeater 32
2.2.4.3 OLM topology 35
2.2.4.4 WLAN topology 35
2.2.4.5 Connecting PROFIBUS to PROFINET 36

3 Parameter assignment/addressing 37

3.1 Assigning the DP slave to a DP master 38
3.2 PROFIBUS address 40
3.3 Network settings 41
3.4 Cable configuration 43
3.5 Additional network stations 44
3.6 Bus parameters 46
3.7 Constant bus cycle time 49

4 Diagnostics 51

4.1 Overview 51

4.2 Diagnostics using the display of the S7-1500 52

4.3 Diagnostics with the diagnostic repeater 53

4.4 I&M data (Identification and Maintenance) 54

5 Functions 55

5.1 Isochronous mode 55

5.1.1 What is isochronous mode? 55

5.1.2 Use of isochronous mode 56

5.1.3 Isochronous applications 56

5.1.4 Sequence of synchronization 57

5.1.5 Requirements for configuration 58

5.1.6 Configuring isochronous mode 59

5.1.7 Diagnostics and interrupt functions 62

5.1.8 Parameter settings for isochronous mode 63

5.1.8.1 Viewing isochronous mode parameters 63

5.1.8.2 Change parameters 64

5.2 Acyclical data exchange 66

5.3 SYNC/FREEZE groups 66

5.4 Interrupts 69

5.5 Intelligent DP slaves (I-slaves) 70

5.5.1 I-slave functionality 70

5.5.2 Data exchange with higher-level DP master 72

5.5.3 Configuring an I-slave 73

5.5.4 Configuring transfer areas 74

5.5.5 Sample program 75

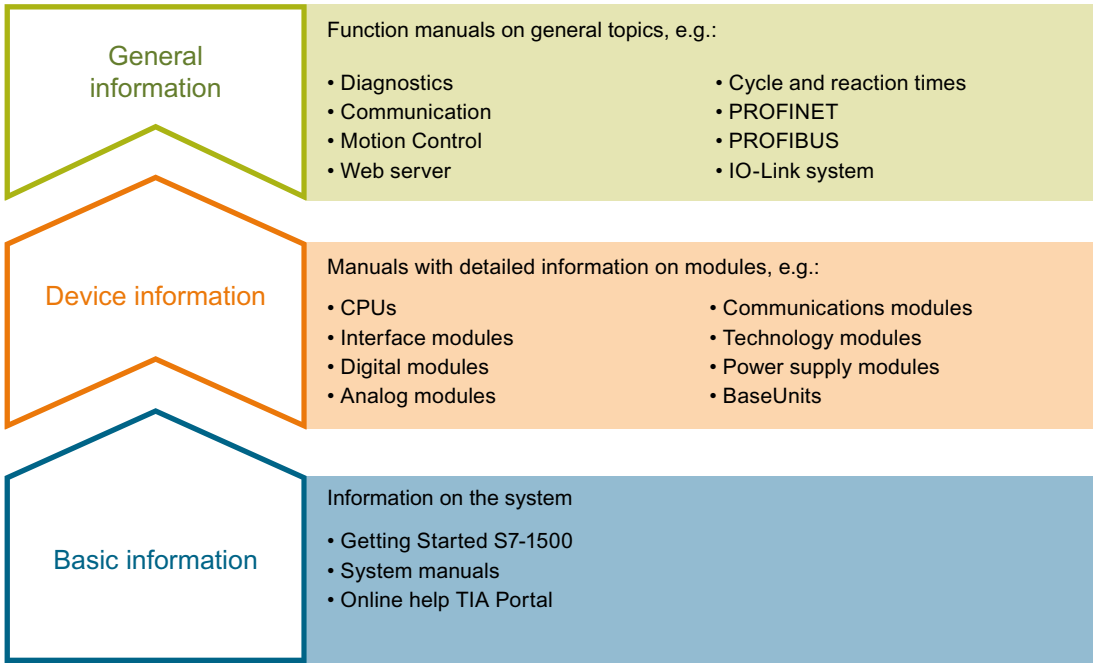
5.5.6 Diagnostics and interrupt behavior 78

A Service & Support 79

Documentation guide

1

The documentation for the SIMATIC S7-1500 automation system and the SIMATIC ET 200MP, ET 200SP and ET 200AL distributed I/O systems is divided into three areas.
This division allows you easier access to the specific information you require.



Basic information
System manuals and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500, ET 200MP, ET 200SP and ET 200AL systems. The STEP 7 online help supports you in the configuration and programming.

Device information
Product manuals contain a compact description of the module-specific information, such as properties, terminal diagrams, characteristics and technical specifications.

General information
The function manuals contain detailed descriptions on general topics such as diagnostics, communication, Motion Control, Web server.

You can download the documentation free of charge from the Internet (http://w3.siemens.com/mcms/industrial-automation-systems-simatic/en/manual-overview/Pages/Default.aspx).

Changes and additions to the manuals are documented in product information sheets.

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- S7-1500/ET 200MP (http://support.automation.siemens.com/WW/view/en/86140384)
- ET 200SP (http://support.automation.siemens.com/WW/view/en/84133942)
- ET 200AL (http://support.automation.siemens.com/WW/view/en/95242965)

My Documentation Manager

The My Documentation Manager is used to combine entire manuals or only parts of these to your own manual.
You can export the manual as PDF file or in a format that can be edited later.

You can find the My Documentation Manager on the Internet (http://support.automation.siemens.com/WW/view/en/38715968).

Applications & Tools

Applications & Tools supports you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus in individual products.

You can find Applications & Tools on the Internet (http://support.automation.siemens.com/WW/view/en/20208582).

CAx Download Manager

The CAx Download Manager is used to access the current product data for your CAx or CAe systems.

You configure your own download package with a few clicks.

In doing so you can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find the CAx Download Manager on the Internet (http://support.automation.siemens.com/WW/view/en/42455541).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (http://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool).

Description 2

2.1 Introduction to PROFIBUS

What is PROFIBUS?

PROFIBUS is a bus system that networks automation systems and field devices that are compatible with PROFIBUS. As communication medium for the field level, PROFIBUS is an important part of Totally Integrated Automation (TIA).

The different communication networks can be used independent of one another or they can be combined with each other.

PROFIBUS protocols

PROFIBUS DP (distributed I/O) is a communication network for the field level according to IEC 61158-2 / EN 61158-2 with the hybrid access protocols token bus and master-slave. The networking takes place by means of two-wire lines or fiber-optic cables. Data transmission rates of 9.6 kbps to 12 Mbps are possible.

PROFIBUS PA is the PROFIBUS for process automation (PA). It connects the PROFIBUS DP communication protocol with the MBP (Manchester Bus Powered) transmission technology to IEC 61158-2.

PROFIBUS PA networks can be designed based on shielded, twisted two-wire lines intrinsically safe and are therefore suitable for hazardous areas (Ex zones 0 and 1). The data transmission rate is 31.25 kbps.

2.1.1 Applications of PROFIBUS DP

Introduction

The efficiency of control systems is not determined by automation devices alone, but depends to a large extent on the overall configuration of an automation solution. This includes a powerful communication system in addition to plant visualization and operator control and monitoring.

The STEP 7 engineering tool supports you during the engineering and configuration of an automation solution.

Applications of PROFIBUS DP

The PROFIBUS network offers wireless connection of several controllers, components and subnets as electrical network, optical network or by using links. Sensors and actuators are controlled centrally by means of PROFIBUS DP.

The following figure shows connection options to PROFIBUS DP:

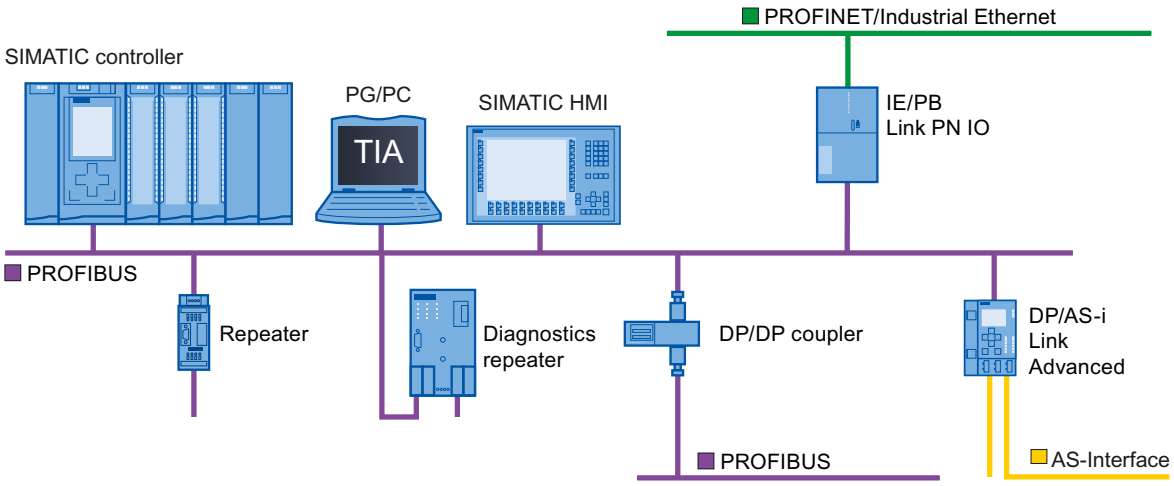


Figure 3-495 Connection options to PROFIBUS DP

Objectives of PROFIBUS DP

Distributed automation systems are increasingly used in production and process automation. This means a complex control task is divided up into smaller, more transparent subtasks with distributed control systems. This creates a high demand for communication between the distributed systems.

Distributed systems offer the following benefits:

- Independent and simultaneous commissioning of individual devices is possible
- Small, manageable programs
- Parallel processing due to distributed automation systems
- Reduced response times
- Higher-level structures can take on additional diagnostics and logging functions.
- Increased plant availability because the rest of the overall system can continue to work when a subordinate station fails.

2.1.2 PROFIBUS terminology

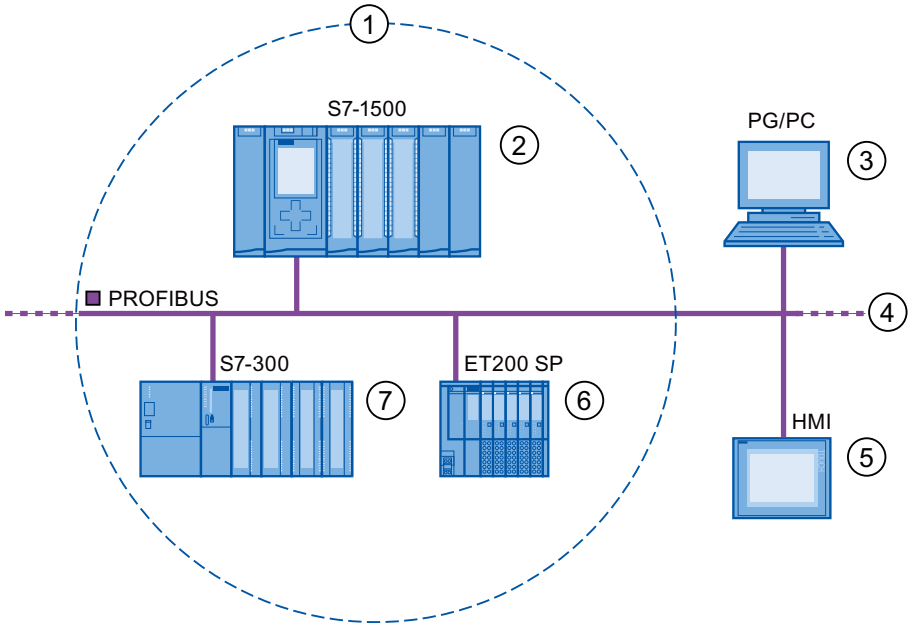
Definition: Devices in the PROFIBUS environment

In the PROFIBUS environment, "device" is the generic term for:

- Automation systems (for example, PLC, PC)
- Distributed I/O systems
- Field devices (for example, hydraulic devices, pneumatic devices)
- Active network components (e.g., diagnostic repeater, optical link module)
- Gateways to AS interface or other fieldbus systems

Devices with PROFIBUS DP

The figure below shows the most important components with PROFIBUS DP. The table below lists the designations of the individual components.



Number	PROFIBUS	Note
①	DP master system	
②	DP master	Device used to address the connected DP slaves. The DP master exchanges input and output signals with field devices. The DP master is often the controller on which the automation program runs.
③	PG/PC	PG/PC/HMI device for commissioning and diagnostics DP master of class 2
④	PROFIBUS	Network infrastructure
⑤	HMI	Device for operating and monitoring functions
⑥	DP slave	Distributed field device assigned to the DP master, e.g., valve terminals, frequency converters.
⑦	I-slave	Intelligent DP slave

Figure 3-496 Devices with PROFIBUS

Overview of I/O communication

I/O communication is the reading or writing of inputs/outputs of the distributed I/O. The figure below gives you an overview of I/O communication using PROFIBUS DP:

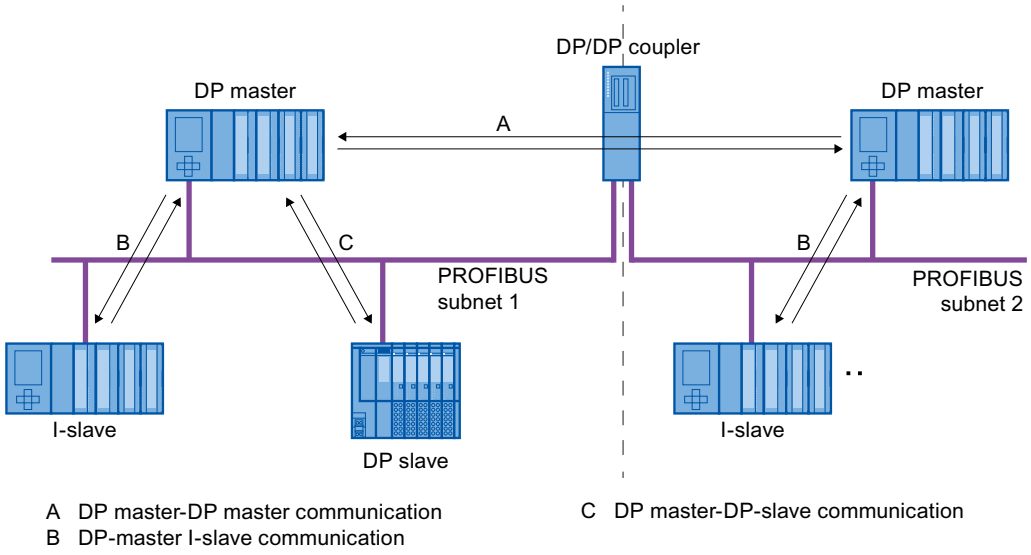


Figure 3-497 I/O communication using PROFIBUS DP

I/O communication is also available with the communication module (CM) or the interface module (IM) with integrated DP interface. These DP interfaces behave like integrated DP interfaces of the CPU.

I/O communication using PROFIBUS DP

Table 3-55 I/O communication using PROFIBUS DP

Communication between ...	Explanation
DP master and DP slave	The data exchange between a DP master and DP slaves with I/O modules takes place as follows: The DP master queries the DP slaves of its master system one after the other, receives input values from the DP slaves, and transmits output data to the DP slaves (master-slave principle).
DP master and I-slave	A fixed amount of data is transmitted cyclically between the user programs in CPUs of DP masters and I-slaves. The DP master does not access the I/O modules of the I-slave, but instead accesses configured address areas, called transfer areas, that can be inside or outside the process image of the I-slave CPU. If parts of the process image are used as transfer areas, these may not be used for actual I/O modules. Data transmission takes place with load and transfer operations using the process image or by direct access.
DP master and DP master	A fixed amount of data is transmitted cyclically between the user programs in CPUs of DP masters. A DP/DP coupler is required as additional hardware. The DP masters mutually access configured address areas, called transfer areas, inside or outside the process image of the CPUs. If parts of the process image are used as transfer areas, these may not be used for actual I/O modules. Data transmission takes place with load and transfer operations using the process image or by direct access.

Additional information

You can find additional information on the hardware configuration in the STEP 7 online help.

2.1.3 PROFIBUS DP interface

Properties

A PROFIBUS device has at least one PROFIBUS interface with an electrical (RS 485) interface or optical (Polymer Optical Fiber, POF) interface.

Table 3-56 Properties of the PROFIBUS DP interface

Standard	PROFIBUS: IEC 61158/61784
Physical bus/media	PROFIBUS cables (twisted two-wire lines RS 485 or fiber-optic cables)
Transmission rate	9.6 kbps to 12 Mbps

Representation of the PROFIBUS DP interface in STEP 7

In the device view of STEP 7, the PROFIBUS DP interfaces for a DP master and a DP slave are highlighted by a purple rectangle:

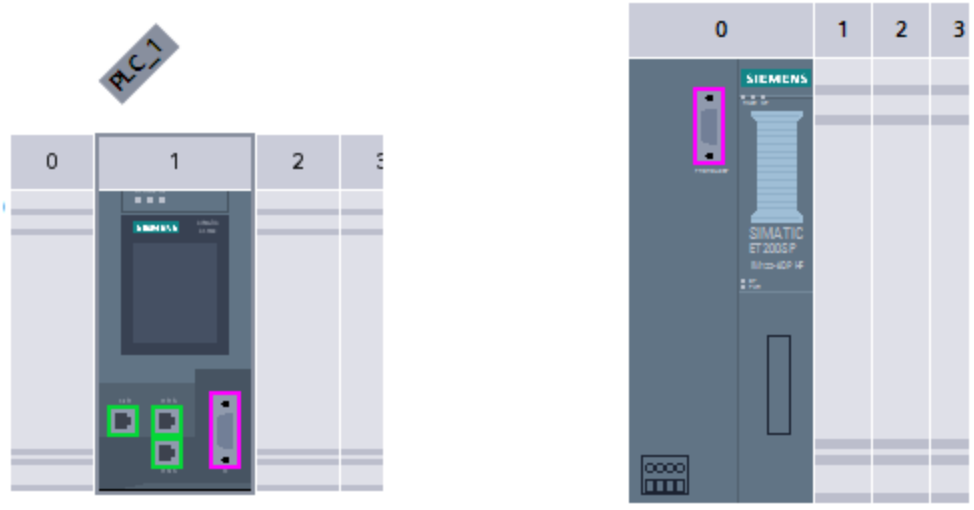


Figure 3-498 PROFIBUS DP interfaces

2.2 Structure of PROFIBUS networks

Contents of this chapter

The following chapter provides background information on building your communication network.

- Overview of the most important passive network components: These are network components that forward a signal without the possibility of actively influencing it, for example, cables, connectors.
- Overview of the most important active network components: These are network components that actively affect a signal, for example, repeaters, diagnostic repeaters.
- Overview of the most common network structures (topologies)

Physical connections of industrial networks

PROFIBUS devices can be networked in industrial plants in two different physical ways:

- By means of electrical signals via copper cables
- By means of optical signals via fiber-optic cables

Selection criteria for networking

The table below includes selection criteria for electrical and optical networking of PROFIBUS devices:

Table 3-57 Selection criteria for electrical and optical networking

Criteria		Electrical PROFIBUS	Optical network with OLM	Optical network with OBT
Transmission medium	Shielded two-wire line	●	–	–
	POF	–	●	●
	PCF	–	●	●
	Glass	–	●	–
Distances	Max. network span	PROFIBUS DP: 9.6 km PROFIBUS PA: 1.9 km	90 km	9.6 km
	Between two devices	up to 1 km 1)	up to 15 km 2)	up to 300 m 2)
Topology	Bus	●	–	–
	Linear	–	●	●
	Tree	●	●	●
	Ring	–	●	●
Transmission protocols		DP, PA	DP, PA	DP
Connection of	OLM	–	●	–

● Suitable

– Not relevant for this application

1) Depending on data rate and type of service used

2) Depending on cable type used

Criteria		Electrical PROFIBUS	Optical network with OLM	Optical network with OBT
devices by means of	Integrated interfaces	●	–	●
	Bus terminal	●	–	●
	Bus connector	●	–	–
Electrical network segments can be connected		●	●	–

● Suitable

– Not relevant for this application

1) Depending on data rate and type of service used

2) Depending on cable type used

Installation guideline for PROFIBUS networks

A PROFIBUS segment must be terminated at the start and end; passively with a connector or actively with a bus terminating resistor.

The same principles apply to the installation of a PROFIBUS network as described in the SIMATIC NET PROFIBUS networks (http://support.automation.siemens.com/WW/view/en/35222591) manual.

2.2.1 Passive network components for RS 485 networks

2.2.1.1 RS 485 cables

Introduction

The following applies to all RS 485 cables for PROFIBUS from Siemens:

- Their double shielding makes them especially suited for laying in industrial environments with electromagnetic interference.
- A continuous grounding concept can be implemented by means of the outer shield of the bus cable and the ground terminals of the bus terminals.
- The imprinted meter marking makes it easier to determine the length (accuracy ±5%).

RS 485 cables for PROFIBUS

SIMATIC NET PROFIBUS cables are available in different versions which allow optimum adaptation to different areas of application:

- FC Standard Cable GP (bus cable for fixed laying inside buildings)
- FC Standard Cable IS GP (bus cable for hazardous area)
- FC-FRNC Cable GP (bus cable with halogen-free protective jacket for use inside buildings)
- FC Food Cable (bus cable with PE jacket for use in the food and beverage industry)
- FC Robust Cable (bus cable with PUR jacket for environments subject to chemical and mechanical stress)
- FC Ground Cable (ground cable with PE jacket)

- PROFIBUS FC Trailing Cable (trailing cable for tow chains)
- PROFIBUS Festoon Cable (bus cable for festoon mounting)
- PROFIBUS Torsion Cable (torsion-free bus cable for networking movable plant parts, for example, robots)
- PROFIBUS FC Flexible Cable (bus cable for machine parts that are moved infrequently or cabinet doors)
- SIENOPYR-FR ship cable (for permanent laying on ships and off-shore units in all rooms and on open deck)
- PROFIBUS Hybrid Standard Cable (hybrid cable with 2 power wires (1.5 mm^2) for data and power supply of the ET 200pro)
- PROFIBUS Hybrid Robust Cable (trailable hybrid cable with 2 power wires (1.5 mm^2) for data and power supply of the ET 200pro)

Maximum cable lengths

When using copper cables, the maximum size of a PROFIBUS segment depends on the transmission rate.

If these lengths are not sufficient for your application, you can expand the network by using repeaters. You can achieve a maximum size by cascading up to nine repeaters.

Table 3-58 Maximum cable lengths

Transmission rate	Maximum cable length of a bus segment	Maximum distance between two stations
9.6 to 187.5 kbps	1000 m	10000 m
500 kbps	400 m	4000 m
1.5 Mbps	200 m	2000 m
3 to 12 Mbps	100 m	1000 m

2.2.1.2 PROFIBUS FastConnect system

PROFIBUS FastConnect (FC)

PROFIBUS FastConnect is a system for fast and easy fabrication of PROFIBUS copper cables.

The system consists of three components:

- FastConnect bus cables for quick mounting
- FastConnect stripping tool
- FastConnect bus connector for PROFIBUS with insulation displacement method

FastConnect bus cables and stripping tool

The special design of the FastConnect bus cables allows for the use of the FastConnect stripping tool to accurately strip away the protective jacket and the braided shield in one step. The connection of the prepared cables takes place in the FastConnect bus connectors using the insulation displacement method.

All PROFIBUS FastConnect bus cables can also be connected to the conventional bus connectors with screw-type terminals.

Area of application

You need FastConnect bus connectors for PROFIBUS for the following applications:

- Connect devices with an electrical 9-pin D-Sub interface to IEC 61158-2 directly with SIMATIC NET PROFIBUS cables.
- Connect electrical segments or individual devices to the Optical Link Module (OLM) and Optical Bus Terminal (OBT).
- Connect devices or programming devices to the repeater.

Versions

The FastConnect bus connector in degree of protection IP20 is available in the following versions:

- with integrated terminating resistor and isolating function
- with or without PG socket
- with a cable outlet of 35°, 90° or 180°

- with device category 3G suitable for zone 2 hazardous area

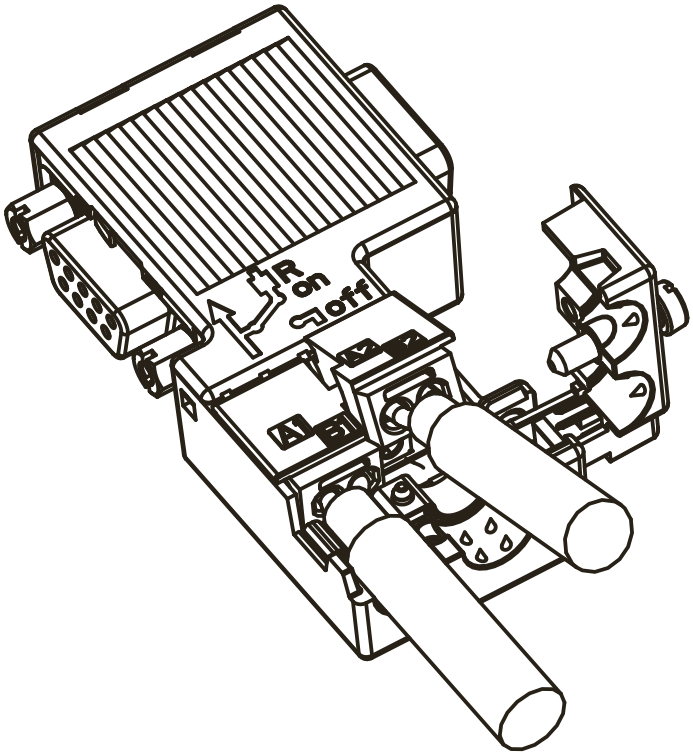


Figure 3-499 Example for PROFIBUS FastConnect bus connector with PG socket, cable outlet 90°

Additional information

For additional information on the available components visit the Siemens Mall (http://mall.industry.siemens.com).

2.2.1.3 PROFIBUS bus connector

Area of application

You need PROFIBUS bus connectors for the following applications:

- Connect devices with a 9-pin D-Sub interface to IEC 61158-2 directly with the SIMATIC NET PROFIBUS cables.
- Connect electrical segments or individual devices to the Optical Link Module (OLM) and Optical Bus Terminal (OBT).
- Connect devices or programming devices to the repeater.

Versions

The PROFIBUS bus connector in degree of protection IP20 is available in the following versions:

- with integrated terminating resistor and isolating function
- with or without PG socket
- with a cable outlet of 35°, 90° or 180°
- with device category 3G suitable for zone 2 hazardous area

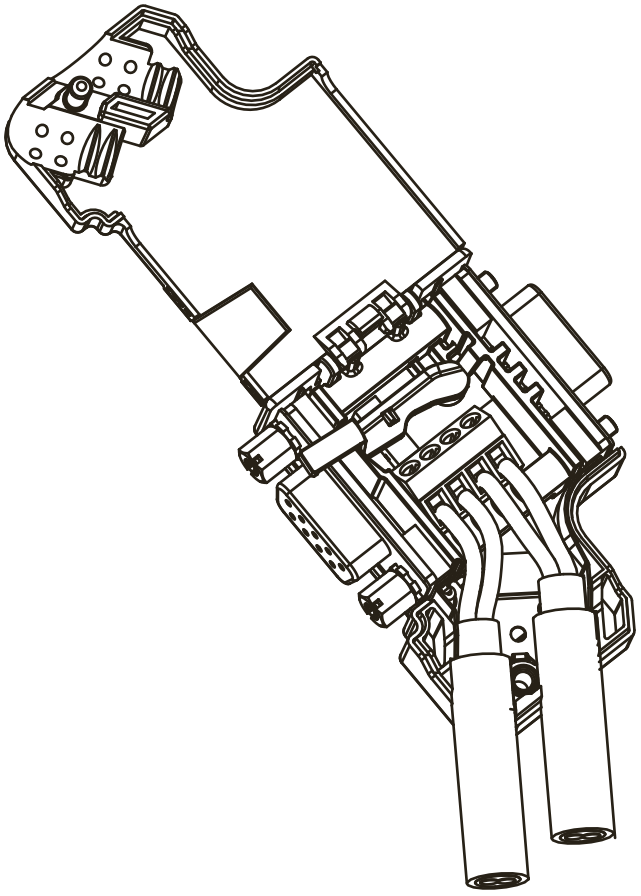


Figure 3-500 Example for PROFIBUS bus connector with PG socket, cable outlet 35°

Additional information

For additional information on the available components visit the Siemens Mall (http://mall.industry.siemens.com).

2.2.1.4 M12 bus connector

Area of application

Devices with an electrical M12 interface can use the M12 bus connector for SIMATIC NET PROFIBUS for direct connection with the SIMATIC NET PROFIBUS cables.

The M12 bus connector in degree of protection IP65 is available in the following versions:

- with screw-type terminals
- with insulation displacement termination
- with a cable outlet of 180°

2.2.1.5 Bus terminals for RS 485 networks

Bus terminal RS 485 and bus terminal M12

A bus terminal is used for the connection of an individual PROFIBUS station with RS485 interface to the PROFIBUS bus cable.

Bus terminals in degree of protection IP20 are available in the following versions:

- Bus terminal RS 485 with or without PG interface, transmission rate 9.6 kbps to 1.5 Mbps, integrated terminating resistor combination (connectible), with 1.5 m and 3 m connecting cable
- Bus terminal M12, transmission rate 9.6 kbps to 12 Mbps, integrated terminating resistor combination with isolating function, with 1.5 m connecting cable

2.2.1.6 M12 bus terminating resistor

Terminating segment with terminating resistor

If there is a station with M12 connection system at the beginning or end of a PROFIBUS segment, you need an M12 bus terminating resistor.

The M12 PROFIBUS connection of a device consists of an M12 socket for the infeed and an M12 male connector to loop-through the bus signal.

This means you need one bus terminating resistor with male contacts (6GK1905-0EC00) and with female contacts (6GK1905-0ED00) for each M12 bus cable.

2.2.2 Passive components for optical networks

2.2.2.1 Fiber-optic cables

Types of fiber-optic cables

Data transmission with fiber-optic cables takes place through modulation of electromagnetic waves in the range of visible and invisible light. These cables are made of high-quality plastic fibers and glass fibers:

- Plastic and PCF fiber-optic cables (Page 22)
- Glass fiber-optic cables (Page 23)

The different types of fiber-optic cables provide solutions matched to the operating and environmental conditions for the connection of components with each other.

Benefits

Fiber-optic cables offer the following benefits when compared with electrical cables:

- Galvanic isolation of the devices and segments
- No potential equalization currents
- No impact on transmission path through external electromagnetic interference
- No lightning protection elements required
- No noise radiation along the transmission route
- Low weight
- Depending on the type of fiber you can implement cable lengths up to few kilometers at even higher transmission rates.
- No dependency of the maximum permitted distances on the transmission rate

Additional information

Additional information of the properties and technical specifications of the passive components and connectors for fiber-optic cables is available in the PROFIBUS network manual (http://support.automation.siemens.com/WW/view/en/35222591).

2.2.2.2 Plastic and PCF fiber-optic cables

Plastic and PCF fiber-optic cables

Plastic (POF) and PCF fiber-optic cables are used for the connection of Optical Link modules with connections for plastic fiber-optic cables (OLM/P), Optical Bus Terminal (OBT) and devices with integrated optical interfaces. Under certain conditions, they are an inexpensive alternative to conventional glass fiber-optic cables.

Plastic Fiber Optic duplex core

The plastic fiber-optic duplex core is a flat dual core with PVC inner jacket without protective jacket. The cable can be easily assembled on-site.

The cable is intended for indoor applications with low mechanical loads or inside cabinets. For OLM connections and with integrated optical interfaces you cover a length of up to 50 m between two devices with this cable.

Plastic Fiber Optic standard cable

The plastic fiber optic standard cable consists of two plastic fibers with robust polyamide inner jacket surrounded by Kevlar tensile elements and a purple PVC protective jacket. The cable can be easily assembled on-site.

The robust round cable is suited for indoor applications. The maximum distance that can be covered is 80 m for OLM/P connections and 50 m with integrated optical interfaces and OBT.

PCF Standard Cable

The pre-assembled PCF Standard Cable consists of two PCF fibers surrounded by Kevlar tensile elements and a purple PVC protective jacket. It is always supplied with a pulling aid installed on one end to pull in the cable channels.

The robust round cable is suited for indoor applications with cable lengths up to 400 m (OLM) or 300 m (integrated optical interfaces, OBT) between two devices.

PCF Standard Cable GP

The PCF Standard Cable GP consists of two PCF fibers surrounded by Aramid tensile elements and a green PVC protective jacket. The cable is pre-assembled and can be ordered by the meter. It is supplied with a pulling aid installed on one end to pull in the cable channels.

The robust round cable is suited for indoor and outdoor applications with cable lengths up to 400 m (OLM) or 300 m (integrated optical interfaces, OBT) between two devices.

PCF Trailing Cable

The PCF Trailing Cable consists of two PCF fibers surrounded by Aramid tensile elements and a green PUR protective jacket. The cable is pre-assembled and can be ordered by the meter. It is supplied with a pulling aid installed on one end to pull in the cable channels.

The robust round cable is suited for moving indoor and outdoor applications with cable lengths up to 400 m (OLM) or 300 m (integrated optical interfaces, OBT) between two devices.

PCF Trailing Cable GP

The PCF Trailing Cable GP consists of two PCF fibers surrounded by Aramid tensile elements and a green PVC protective jacket. The cable is pre-assembled and can be ordered by the meter. It is supplied with a pulling aid installed on one end to pull in the cable channels.

The robust round cable is suited for moving indoor and outdoor applications with cable lengths up to 400 m (OLM) or 300 m (integrated optical interfaces, OBT) between two devices.

2.2.2.3 Glass fiber-optic cables

Glass fiber-optic cables

Glass fiber-optic cables are suitable for connection of optical interfaces that work in the wavelength range around 850 nm and around 1300 nm. They include two graded-index multimode fibers of the type 62.5/125 µm.

The glass fiber-optic cables are available in different versions which makes for an optimum adaptation to different areas of application:

- Fiber Optic standard cable
- INDOOR Fiber Optic indoor cable
- Flexible Fiber Optic trailing cable

Fiber Optic standard cable

The standard cable is the universal cable for indoor and outdoor use.

INDOOR Fiber Optic indoor cable

The indoor cable is intended for weather-proof indoor use. It is halogen-free, non-crush and flame-retardant.

Flexible Fiber Optic trailing cable

The trailing cable was designed for the special application of forced movement, for example, for constantly moved machine parts such as trailing chains. It is mechanically designed for 100,000 bending cycles by ±90° (with the specified minimum radius). Integrated dummy elements ensure a round cross-section of the cable. The trailing cable can be used indoors and outdoors.

Maximum distances between two optical link modules

The following distances may not be exceeded between two OLMs regardless of the optical power budget:

- OLM/P11, OLM/P12: 400 m
- OLM/G11, OLM/G12, OLM/G12-EEC: 3 km
- OLM/G11-1300, OLM/G12-1300: 15 km

Additional information

All operating instructions (http://support.automation.siemens.com/WW/view/en/10805951/133300) of the SIMATIC NET bus components include information on distances that can be covered with the SIMATIC NET glass fiber-optic cables. You can configure your optical network without any calculations using simple limits.

2.2.3 Active network components

2.2.3.1 Network components in electrical networks

Active network components

The following active network components are available for PROFIBUS in electrical networks:

- Repeater RS485
- Diagnostics repeater
- PROFIBUS Terminator
- DP/DP coupler
- IE/PB Link PN IO
- IWLAN/PB Link PN IO
- Active components for the connection of CAN
- Active components for the gateway between PROFIBUS and AS-Interface
  - DP/AS-i LINK Advanced
  - DP/AS-Interface Link 20E
  - DP/AS-i F-Link

RS485 repeater

The RS485 IP20 repeater connects two PROFIBUS bus segments in RS485 technology with up to 32 devices. It provides transmission rates from 9.6 kbps to 12 Mbps.

The RS485 repeater refreshes a signal regarding amplitude, signal width and edge steepness between two segments. It is used when more than 32 stations are connected to the bus or the maximum cable length of a segment is exceeded.

Bus segments can be operated ungrounded (galvanic isolation of segments) with an RS485 repeater.

Diagnostics repeater

The diagnostic repeater connects three PROFIBUS segments in RS485 technology, two of which are diagnostics-capable segments with 31 devices each. It is designed as DP slave to send diagnostics alarms to the DP master.

The diagnostic function provides the location and the cause of cable faults, such as wire break or missing terminating resistors. The fault location is indicated relative to the existing devices.

The diagnostics repeater refreshes a signal regarding amplitude, signal width and edge steepness between the segments. The cascading depth between any two PROFIBUS devices is limited to nine diagnostics repeaters.

PROFIBUS Terminator

The PROFIBUS Terminator forms an active bus termination. Bus devices can be switched off, removed or replaced without affecting data transmission. This is particularly true for bus devices on both ends of the bus cable at which terminating resistors must be connected or supplied. The PROFIBUS Terminator can be mounted on a standard mounting rail.

IE/PB Link PN for the connection of a PROFIBUS segment to an Industrial Ethernet network

The IE/PB Link PN IO as independent component provides the seamless transition between Industrial Ethernet and PROFIBUS. Through the use of IE/PB Link PN IO as substitute on the Ethernet, the existing PROFIBUS devices can continue to be used and can be integrated into a PROFINET application.

A PROFINET IO controller is required for this configuration. The IE/PB Link PN acts as master on the PROFIBUS end.

IWLAN/PB Link PN IO as gateway between LAN and PROFIBUS

PROFIBUS devices can be coupled to PROFINET IO by means of IWLAN/PB Link PN IO. This means you can integrate existing PROFIBUS configurations into PROFINET.

The IWLAN/PB Link PN IO supports the use of IWLAN and WLAN antennas for wireless data transmission, for example, in suspended monorail systems or conveyor systems. Because of the PROFINET support, the numerous PROFIBUS system services, for example, diagnostics by bus, can continue to be used.

A PROFINET IO controller is required for this configuration. The IWLAN/PB Link PN IO acts as master on the PROFIBUS end.

CANopen module for connection to CAN

You can use the CANopen module to easily connect CANopen applications to PROFIBUS.

Typical areas of application:

- Control of hydraulic valves/hydraulic axes in vehicles
- Control of motors in packaging machines and on conveyor belts
- Use in wind turbines for detection of angular encoders
- Detection of HMI devices on machines, e.g., joysticks
- Detection of measured data from displacement transducers, inclination sensors or angle encoders on tower cranes or gantry cranes

DP/DP coupler for connection of two PROFIBUS networks

The PROFIBUS DP/DP coupler is used to connect two PROFIBUS DP networks. Data (0 to 244 bytes) is transmitted from the DP master of the first network to the DP master of another network and vice versa.

The DP/DP coupler comes equipped with two independent DP interfaces that establish the connection to the two DP networks. There is one slave at each DP network. The data exchange between the two DP networks takes place by internal copying in the coupler.

DP/PA bus link for connection of PROFIBUS PA

The DP/PA bus link is the connection between PROFIBUS DP and PROFIBUS PA. This means it connects the process control systems with the field devices of the process automation.

The following components are available for a DP/PA bus link:

- DP/PA coupler Ex [ia]
- DP/PA coupler FDC 157-0
- Interface module IM 153-2 for establishing a DP/PA link.
- Active field distributor AFDiS for hazardous areas

Active components for the gateway between PROFIBUS and AS-Interface

- **DP/AS-i LINK Advanced**:

  The **DP/AS-i LINK Advanced** is PROFIBUS DPV1 slave (according to IEC 61158-2/EN 61158-2) and AS-Interface master (according to AS-Interface specification V3.0 according to EN 50295) and provides transparent data access to AS-Interface from PROFIBUS DP.

  PROFIBUS DP masters can cyclically exchange I/O data with the AS-Interface; DP masters with acyclic services can also make AS-Interface master calls. The **DP/AS-i LINK Advanced** is particularly suited for distributed configurations and for the connection of a subordinate AS-Interface network.

  The DP/AS-i LINK Advanced in the version as AS-Interface single master is completely sufficient for applications with typical configuration limits.

  For applications with high configuration limits, the DP/AS-i LINK Advanced is used as AS-Interface double master. In this case, the duplicate configuration limits can be used on two independently running AS-Interface strands.

- **DP/AS-Interface Link 20E:**

  The DP/AS-Interface Link 20E is PROFIBUS DP slave (in accordance with EN 61158) and AS-Interface master (in accordance with AS-Interface specification V3.0 according to EN 50295) and supports operation of the AS-Interface on PROFIBUS DP.

  Single PROFIBUS masters can cyclically exchange I/O data with the AS-Interface; masters with acyclic services can exchange I/O data and make master calls.

- **DP/AS-i F-Link:**

  The DP/AS-i F-Link is PROFIBUS DP-V1 slave (according to EN 61158) and AS-i master (according to AS-Interface specification V3.0 to EN 50295) and provides transparent data access to AS-Interface from PROFIBUS DP. The DP/AS-i F-Link is also the only AS-i master that can forward safety-oriented input data of ASIsafe slaves to a fail-safe CPU with PROFIBUS DP master by means of the PROFIsafe protocol. Additional safety cabling or monitoring is not required (in particular, no AS-Interface safety monitor). Depending on the slave type, you can transmit binary values or analog values. All slaves according to AS-Interface specification V2.0, V2.1 or V3.0 can be operated as AS-i slaves.

  As fully-featured AS-i master according to specification V3.0, you can use higher configuration limits on the AS-i network (496 inputs and outputs each, up to 62 digital or analog slaves).

Additional information

Information on the components is available in the Siemens Mall (http://mall.industry.siemens.com).

Additional information is available in these manuals:

- PROFIBUS Network Manual (http://support.automation.siemens.com/WW/view/en/35222591)
- Diagnostic repeater (http://support.automation.siemens.com/WW/view/en/7915183)
- DP/DP Coupler (http://support.automation.siemens.com/WW/view/en/1179382)
- SIMATIC NET Twisted-Pair and Fiber-Optic Networks (http://support.automation.siemens.com/WW/view/en/8763736)
- Basics on Setting up an Industrial Wireless LAN (http://support.automation.siemens.com/WW/view/en/9975764)
- SIMATIC bus links, DP/PA coupler, active field distributors, DP/PA Link and Y Link (http://support.automation.siemens.com/WW/view/en/1142696)
- Information on the CANopen module is available on the Internet (http://www.hms-networks.com/can-for-et200s).
- DP/AS-interface LINK Advanced (http://support.automation.siemens.com/WW/view/en/22502958/133300) manual
- DP/AS-i F-Link (http://support.automation.siemens.com/WW/view/en/24196041) manual

See also

Topology with RS485 repeater (Page 29)
OLM topology (Page 35)
WLAN topology (Page 35)
Connecting PROFIBUS to PROFINET (Page 36)

2.2.3.2 Network components in optical networks

Active network components

The following active network components are available for PROFIBUS in optical networks:

- Optical Link Module OLM
- Optical Bus Terminal OBT

Optical Link Module OLM

You can use the PROFIBUS Optical Link Modul OLM to install PROFIBUS networks in line, star structure and redundant ring structure.

The transmission rate of a fiber-optic cable line does not depend on the distance and can be 9.6 kbps to 12 Mbps.

Applications for OLM include, for example, plant buses on PROFIBUS base, networking across buildings using glass fiber-optic cables, mixed networks with electrical and optical segments, large networks (road tunnels, traffic guidance systems) and networks with high demands on availability (redundant ring networks).

Optical Link modules can be combined by means of an RS485 interface and individual devices or entire electrical segments can be integrated into the optical PROFIBUS network.

The following distances may not be exceeded between two OLMs regardless of the optical power budget:

- OLM/P11, OLM/P12: 400 m
- OLM/G11, OLM/G12, OLM/G12-EEC: 3 km
- OLM/G11-1300, OLM/G12-1300: 15 km

Optical Bus Terminal OBT (optical bus terminal)

The Optical Bus Terminal connects an individual PROFIBUS device without integrated optical interface or a PROFIBUS RS 485 segment with up to 31 devices to an optical PROFIBUS.

An individual PROFIBUS DP device is connected with its RS 485 interface by means of a PROFIBUS cable with integrated terminating resistor, for example, connecting cable 830-1T, to the RS 485 interface of the OBT. The OBT is integrated into the optical line by means of two optical interfaces.

The following optical transmission media can be connected to the OBT:

- Plastic fiber-optic cable up to 50 m single distance length. They can be assembled on-site with two 2x2 Simplex connectors.
- PCF fiber-optic cable up to 300 m single distance length. The cables are delivered pre-assembled.

Additional information

Information on the components is available in the Siemens Mall (http://mall.industry.siemens.com).

Additional information is available in these manuals:

- PROFIBUS network manual (http://support.automation.siemens.com/WW/view/en/35222591)
- SIMATIC NET PROFIBUS, Optical Link Module (http://support.automation.siemens.com/WW/view/de/56606534/0/en)
- SIMATC NET Twisted-Pair and Fiber-Optic Networks (http://support.automation.siemens.com/WW/view/en/8763736)

2.2.4 Examples for topology

2.2.4.1 Topology with RS485 repeater

Configuration options with the RS485 repeater

You can operate the RS485 repeater in the following configurations:

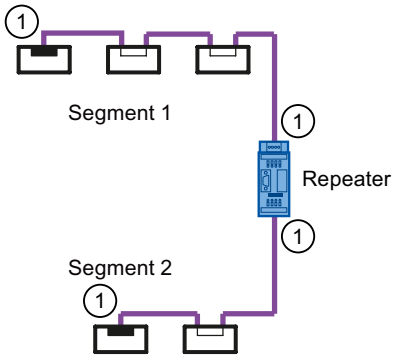


Figure 3-501 Segment 1 and segment 2 connected to RS485 repeater

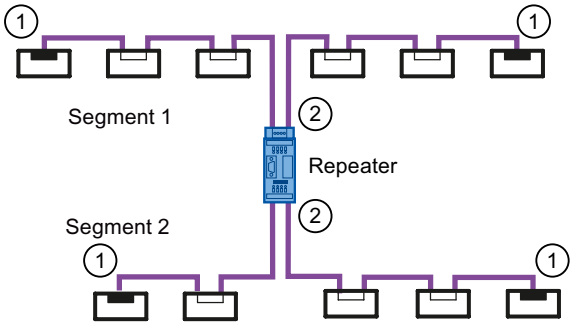


Figure 3-502 Segment 1 and segment 2 looped-through to RS485 repeater

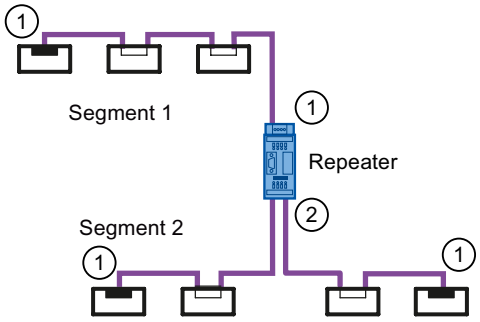


Figure 3-503 Segment 1 connected to RS485 repeater and segment 2 looped-through to RS485 repeater

① Connect terminating resistor

② Do not connect terminating resistor

Configuration example

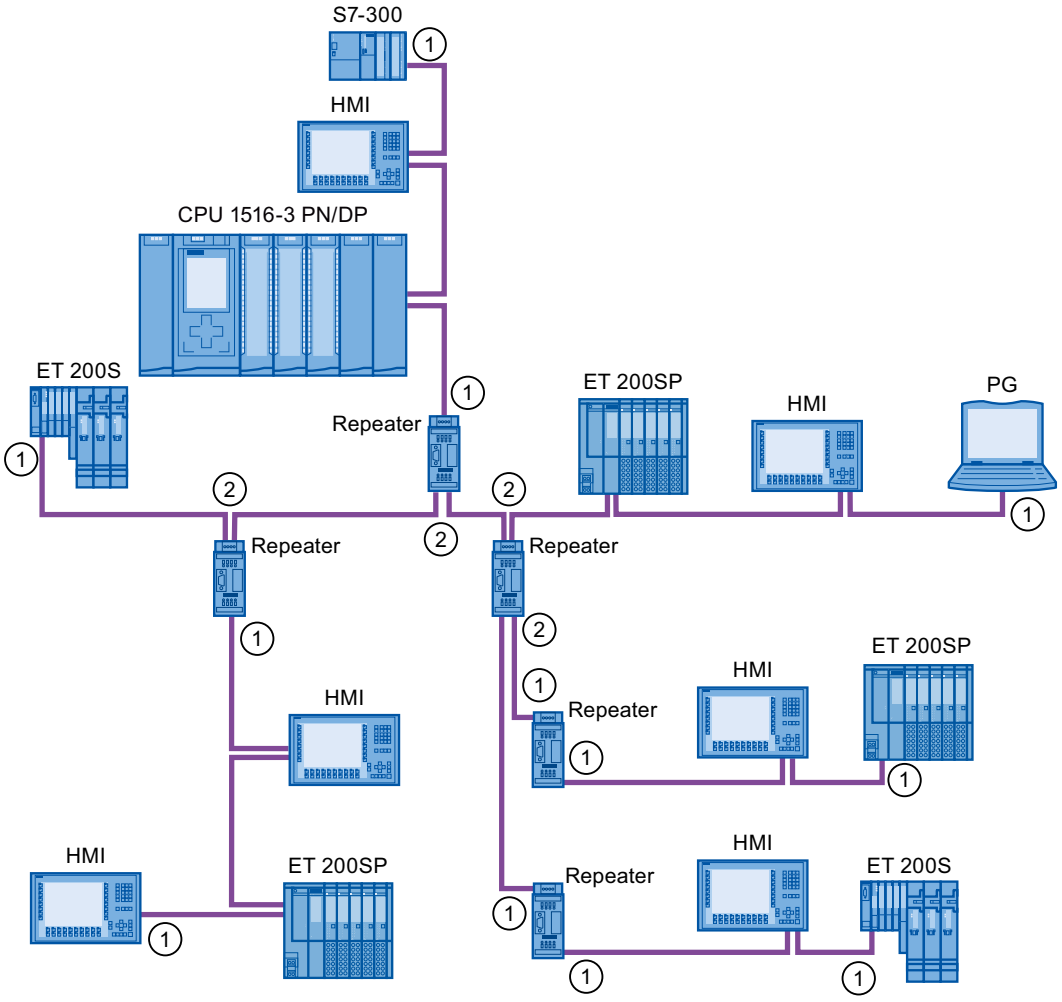


Figure 3-504 Configuration example with five RS485 repeaters

① Connect terminating resistor

② Do not connect terminating resistor

Maximum configuration

If you install a PROFIBUS network with RS485 repeaters, you may not connect more than nine RS485 repeaters in series.

2.2.4.2 Topology with diagnostic repeater

Diagnostic repeater with three segments

You may not exceed the maximum permitted cable length of 100 m per segment that can be monitored for the diagnostic repeater. The segments connected to DP2 and DP3 are diagnostics-capable. The cable length that can be monitored is limited for some cable types.

Maximum cascade depth

You can connect up to nine diagnostic repeaters in series between any two PROFIBUS stations.

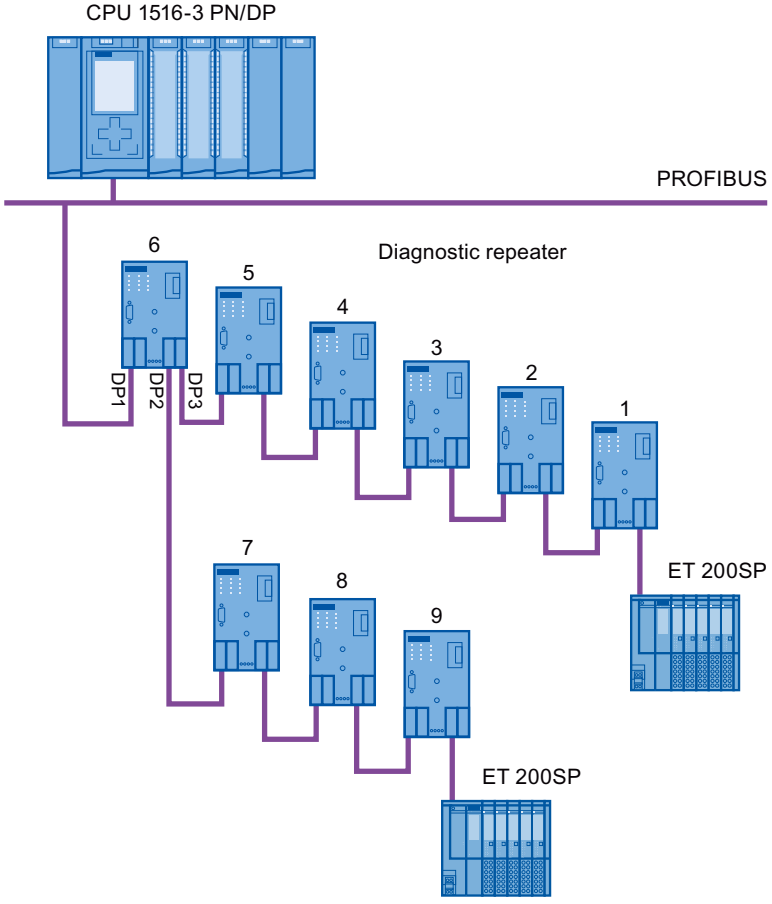


Figure 3-505 Schematic layout of a PROFIBUS network with maximum possible cascade depth at diagnostic repeaters

Example: Maximum cascade depth exceeded

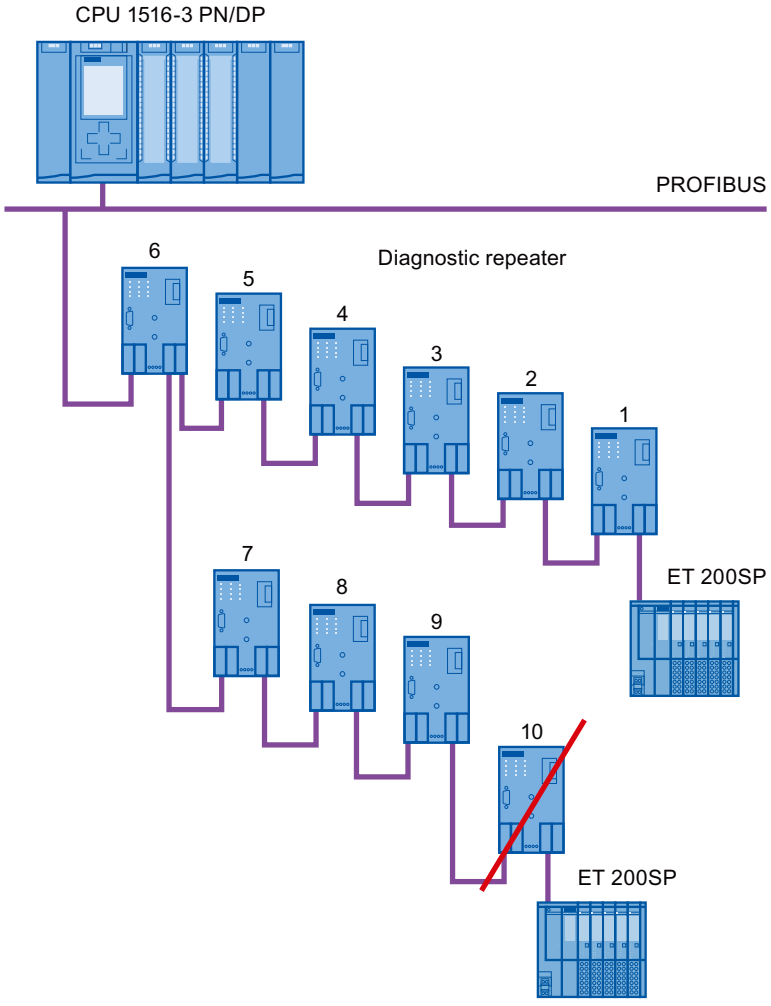


Figure 3-506 Maximum cascade depth exceeded

Layout with several segments

You can increase the number of used diagnostic repeaters by using several segments. The example shows a layout in which the maximum cascade depth is exceeded at two segments.

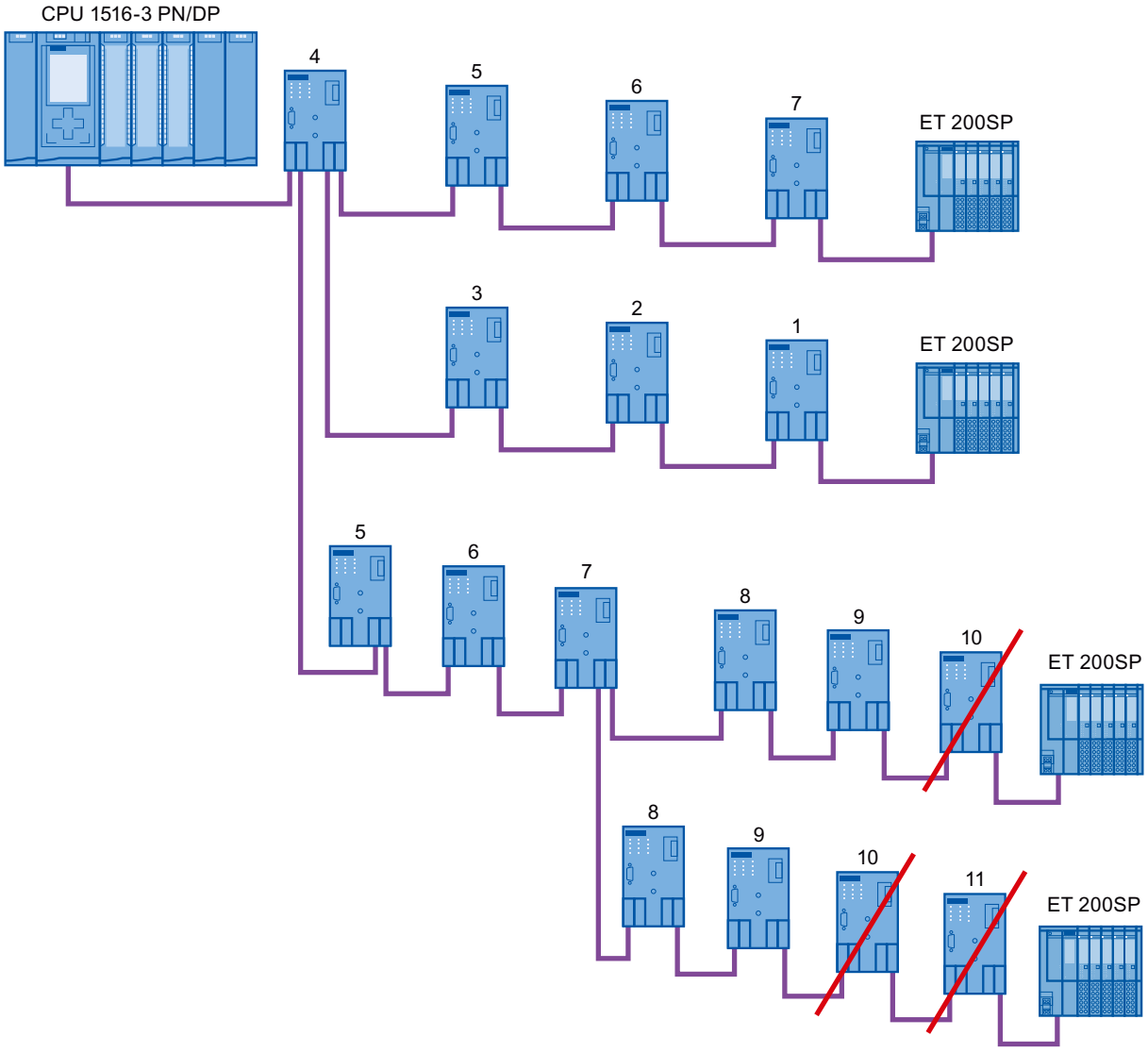


Figure 3-507 Layout with several segments, maximum cascade depth exceeded

Additional information

Additional information is available in the Diagnostic Repeater (http://support.automation.siemens.com/WW/view/en/7915183) manual.

2.2.4.3 OLM topology

Combination of electrical and optical networks with OLM

Additional distances can be covered by means of the Optical Link Module.

Because bus cables across several buildings are particularly vulnerable to damage caused by overvoltage (effect of lightning), the devices in the connected bus segment must be protected against overvoltage.

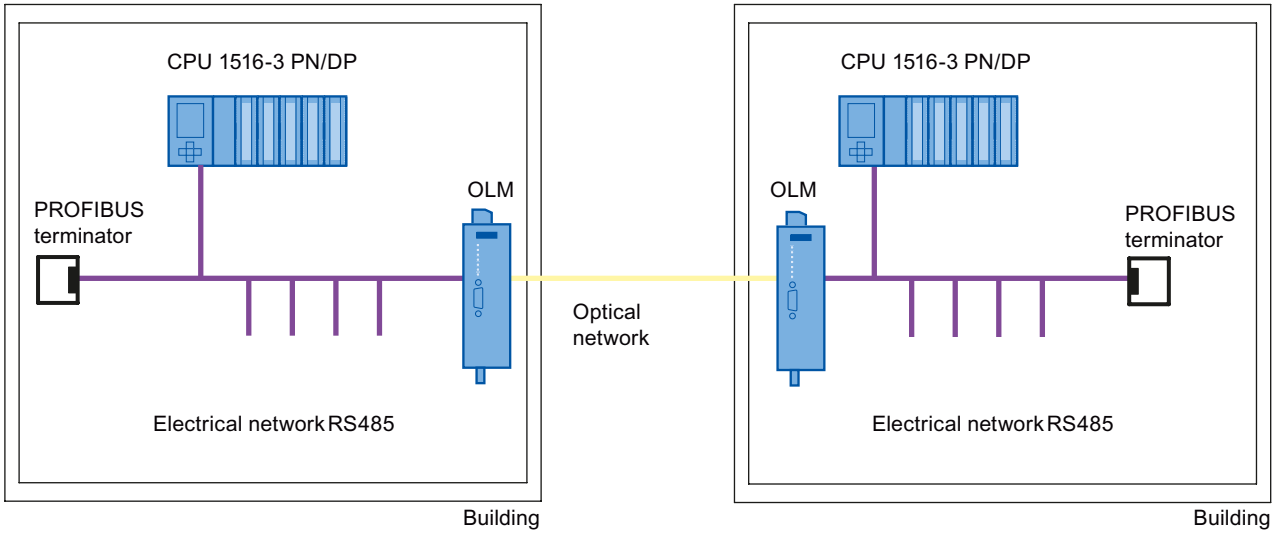


Figure 3-508 Combination of electrical and optical networks

2.2.4.4 WLAN topology

IWLAN/PB Link PN IO as gateway between Industrial Wireless LAN and PROFIBUS

The IWLAN/PB Link PN IO supports the use of IWLAN and WLAN antennas for wireless data transmission. This means the numerous PROFIBUS system services, for example, diagnostic by bus, can be used throughout.

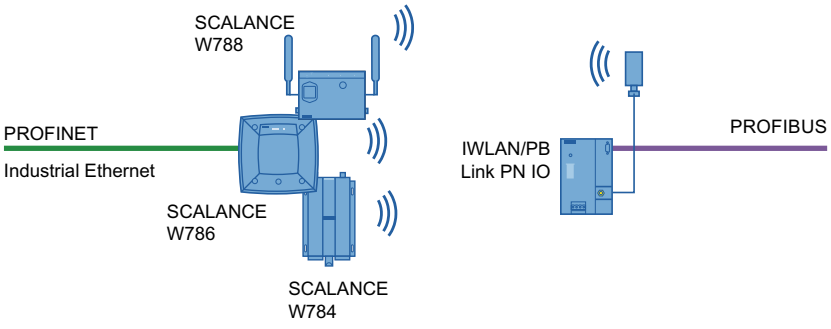


Figure 3-509 PROFIBUS and WLAN

2.2.4.5 Connecting PROFIBUS to PROFINET

PROFIBUS can be integrated in PROFINET. In this way, you can set up any hybrid systems consisting of fieldbus and Ethernet-based subsystems. This provides a continuous data exchange.

Coupling of PROFIBUS and PROFINET

With a proxy-capable PROFINET device that is equipped with a PROFIBUS interface in addition to a PROFINET interface, you can integrate existing PROFIBUS configurations into the PROFINET configuration.

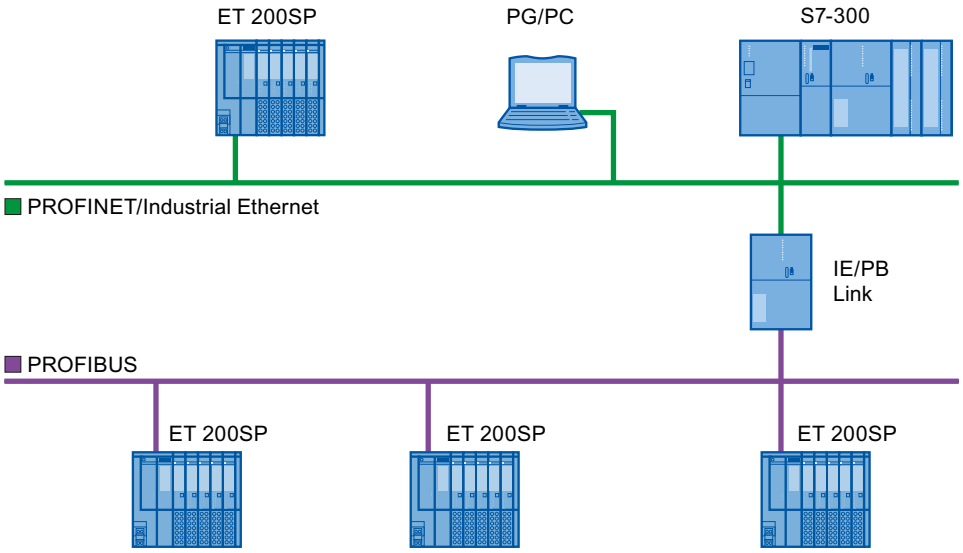


Figure 3-510 Connection of PROFIBUS and PROFINET with IE/PB link

PROFINET device with proxy functionality

The PROFINET device with proxy functionality is the substitute for a PROFIBUS device on Ethernet. The proxy functionality allows a PROFIBUS device to communicate not only with its master but also with all devices on PROFINET.

With PROFINET, existing PROFIBUS systems can be integrated into the PROFINET communication with the aid of an IE/PB link. The IE/PB link PN IO then handles communication via PROFINET on behalf of the PROFIBUS components.

Parameter assignment/addressing 3

To set up an automation system, you will need to configure, assign parameters and link the individual hardware components. The work needed for this is undertaken in the STEP 7 device, topology and network view.

Configuration

"Configuring" is understood to mean arranging, setting and networking devices and modules within the device or network view.

A PROFIBUS address is automatically assigned to each module. The addresses can be subsequently modified.

The CPU compares the preset configuration created in STEP 7 with the actual configuration of the plant. Errors can be detected and signaled immediately this way.

The exact procedure for configuring devices is described in detail in the STEP 7 online help.

Parameter assignment

"Parameter assignment" is understood to mean setting the properties of the components used. The settings for the hardware components and for data exchange are assigned, for example, activating diagnostics, input delay with DI.

The parameters are downloaded into the CPU and transferred to the corresponding modules when the CPU starts up. Modules can be replaced with ease because with SIMATIC CPUs the set parameters are automatically downloaded into the new module during each startup.

Adjusting the hardware to the project requirements

You need to adapt the hardware if you want to set up, expand or change an automation project. To do this, add hardware components to your layout, link them with existing components, and adapt the hardware properties to the tasks.

The properties of the automation systems and modules are preset so that in many cases you do not have to assign parameters again.

But parameter assignment is required in the following cases:

- You want to change the preset parameters of a module.
- You want to use special functions.
- You want to configure communication connections.

Basic procedure for creating a PROFIBUS DP system

- Configuration
  - Creating PROFIBUS devices and modules in STEP 7
  - Assigning the DP slave to a DP master (Page 38)
- Optional: Parameter assignment
  - Assigning the PROFIBUS address (Page 40)
  - Making network settings (Page 41)
  - Considering cable configuration (Page 43)
  - Considering additional network devices (Page 44)
  - Bus parameters – creating a user-defined profile (Page 46)
  - Configuring constant bus cycle time (Page 49)

3.1 Assigning the DP slave to a DP master

PROFIBUS DP system

A PROFIBUS DP system consists of a PROFIBUS DP master and its assigned PROFIBUS DP slaves. Once the devices have been placed in the network view or device view, STEP 7 assigns default parameter values to them. Initially, you only have to assign the DP slaves to one DP master.

Requirement

- The network view of STEP 7 is open.
- A CPU has been placed (e.g., CPU 1516-3 PN/DP).
- A DP slave has been placed (e.g., IM151-1 HF).

Procedure

To assign DP slaves to a DP master, follow these steps:

1. On the DP slave, use the left mouse button to click on the "Not assigned" link. The "Select DP master" menu opens.
2. Select the DP master in the menu to which you want to assign the DP slave.

   Result: A subnet with a DP system is created on the CPU. The CPU is now the PROFIBUS DP master. The DP slave is assigned to the DP master.
3. Repeat steps 1 and 2 for all other DP slaves that you want to assign to the DP master.

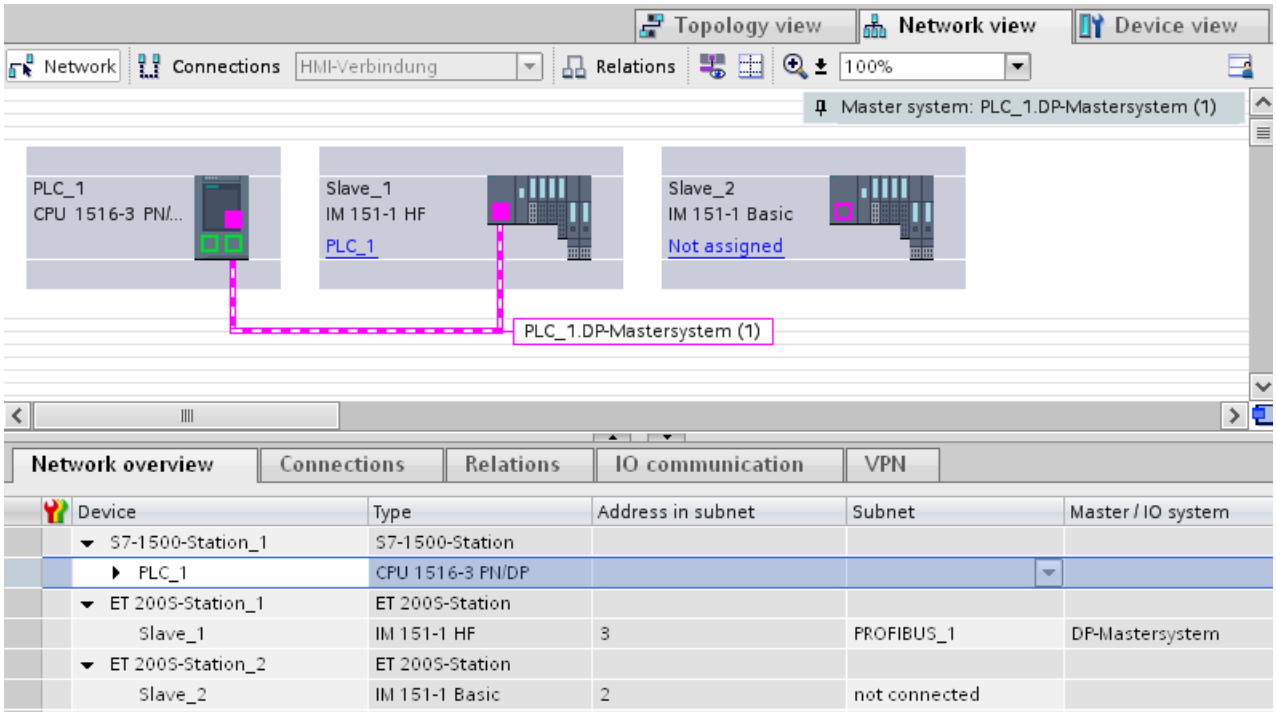


Figure 3-511 Assigning the DP slave to a DP master

Network overview

You can check the communication relationships of the activated interface in the network overview. The network overview is context-sensitive for selection in the network view:

- The selection of the CPU shows the DP communication of the CPU.
- The selection of the station shows the communication of the entire station.
- The selection of the interface shows the DP communication of the interface.

3.2 PROFIBUS address

Devices can be connected to the PROFIBUS subnet that communicate by means of configured connections or that are part of a PROFIBUS DP master system.

If the DP slave has already been assigned to a DP master, the PROFIBUS subnet to which the device is connected is automatically displayed under "Interface linked with".

In the Inspector window under "PROFIBUS", select the subnet to which the interface is linked or add a new subnet.

All devices of a subnet must have different PROFIBUS addresses.

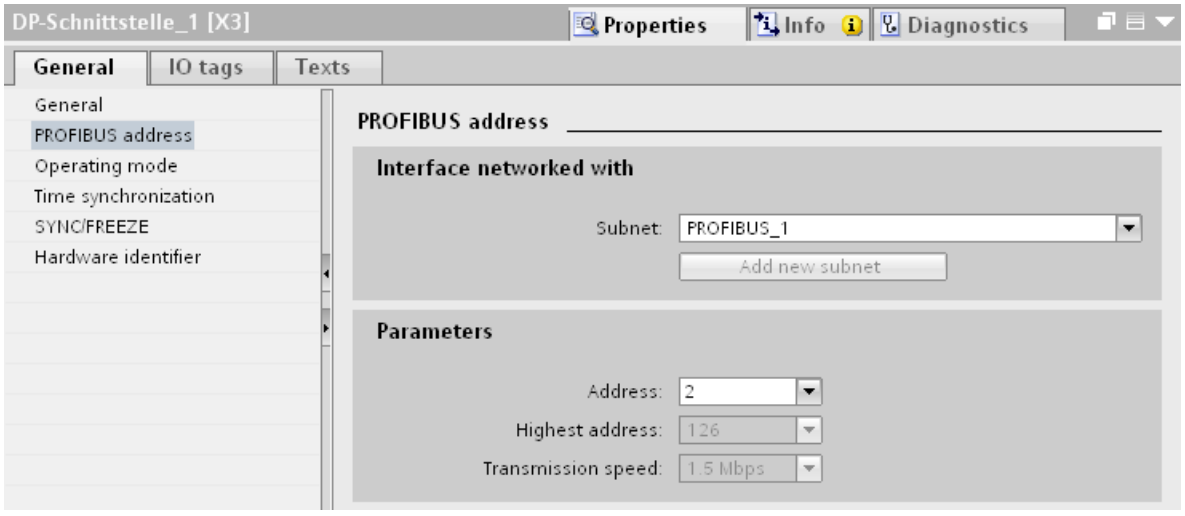


Figure 3-512 PROFIBUS address

Rules for address assignment

STEP 7 automatically assigns device addresses.

You can change the addresses if you observe the following points:

- Assign a unique PROFIBUS address to each device in the PROFIBUS network, each DP master and each DP slave in the PROFIBUS network.
- Depending on the DP slave, not all permitted PROFIBUS addresses are supported. For devices with BCD switches, it is often the case that only the PROFIBUS addresses 1 to 99 are supported.

Changing the PROFIBUS address

You change the PROFIBUS address under "Parameter".

3.3 Network settings

Highest PROFIBUS address (HSA)

Outputs the highest PROFIBUS address of an active device. PROFIBUS addresses greater than HSA are permitted for passive devices, but only up to 126.

Profile

Depending on the connected device types and the protocols used, different profiles are available on the PROFIBUS. The profiles differ with respect to their setting options and calculation of the bus parameters.

The PROFIBUS subnet will only work properly if the bus parameters of all devices have the same values.

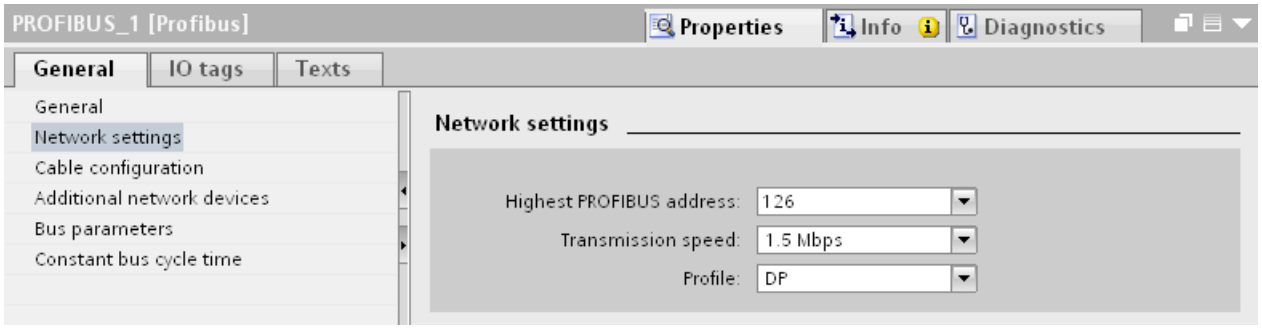


Figure 3-513 Network settings

Profiles and transmission rates

Table 3-59 Profiles and transmission rates

Profiles	Supported transmission rates
DP	9.6 kbps to 12 Mbps
Standard	9.6 kbps to 12 Mbps
Universal (DP/FMS) (FMS is not supported)	9.6 kbps to 1.5 Mbps
User-defined	9.6 kbps to 12 Mbps

DP (recommended profile)

Select the "DP" profile if only devices meeting the requirements of the standard EN 61158-6-3 are connected to the PROFIBUS subnet. The setting of the bus parameters has been optimized for these devices. These include devices with DP master and DP slave interfaces of SIMATIC S7 as well as distributed I/O devices from third parties.

NOTE

Profile for constant bus cycle time and isochronous mode

DP is the recommended profile for the configuration of constant bus cycle time and isochronous mode.

Standard

Compared with the "DP" profile, the "Standard" profile gives you the option to take into consideration devices of another project or devices that have not been configured here for calculation of the bus parameters. The bus parameters are then calculated with a simple algorithm that was not optimized.

Universal (DP/FMS) (FMS is not supported)

Select the "Universal (DP/FMS)" profile if individual devices in the PROFIBUS subnet use the FMS service (e.g., CP 343-5, PROFIBUS FMS devices).

As with the "Standard" profile, here, too, you have the option to take additional devices into consideration for calculation of the bus parameters.

User-defined

The PROFIBUS subnet will only work properly if the parameters for the profile have been synchronized. Select the "User-defined" profile if none of the other profiles "match" for operation of a PROFIBUS device and if you have to adapt the bus parameters for your special layout.

You cannot configure all theoretically possible combinations with the user-defined profile either. The PROFIBUS standard prescribes some parameter limits depending on other parameters. It is, for example, not permitted that a responder responds (Min Tsdr) before the initiator is able to receive the frame (Trdy). These standard specifications are also checked in the "User-defined" profile.

NOTE

User-defined settings

Use user-defined settings only if you are familiar with the PROFIBUS parameters. It is usually better to work with the "DP" profile.

Contact Customer Support (Page 79) if you have any questions.

The bus parameters that were last valid on the PROFIBUS subnet are automatically set as user-defined. If the "DP" bus profile was valid for the subnet, for example, the bus parameters for "DP" are set in the "User-defined" bus profile. You can modify the parameters based on these settings.

The monitoring times are not automatically recalculated in the "User-defined settings" setting so that the uniformity of the set values is not changed without your knowledge, for example, to configure other configuration tools.

You can calculate the monitoring times Ttr and watchdog based on the parameters you have set. To do so, click on the "Recalculate" button.

See also

Additional network stations (Page 44)

3.4 Cable configuration

Considering cable configuration

Information on the cable configuration can be taken into consideration for calculation of the bus parameters. To do so, select the check box "Take into account the following cable configuration" in the properties of the PROFIBUS subnet.

The other information depends on the type of cable used.

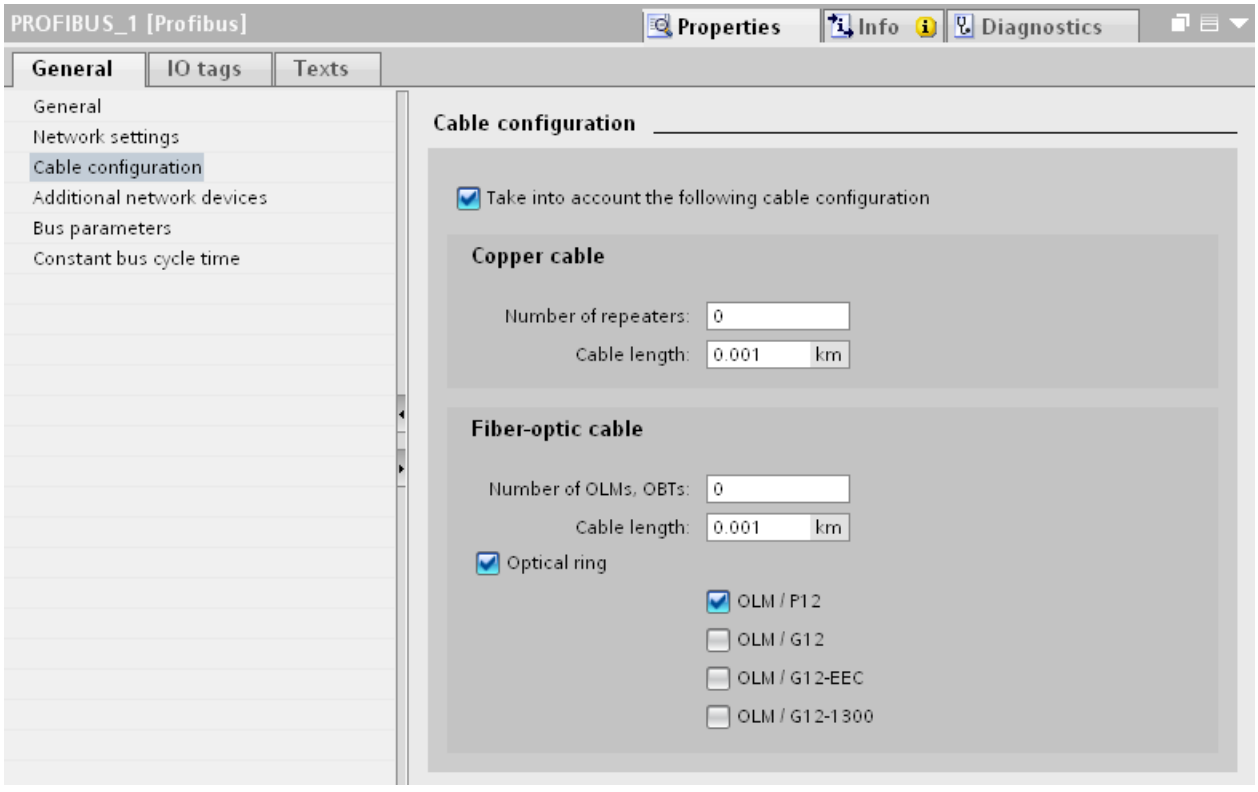


Figure 3-514 Cable configuration

Cable configuration: Fiber-optic cables/optical ring

The calculation depends on the used OLM types. Select the corresponding check box. Multiple selections are possible.

Adapting bus parameters in the optical ring

With the layout as ring, there is a kind of redundancy because you have the option to address all devices using the ring structure even if the connection between two devices is interrupted.

The following configuration conditions must be met in the optical ring:

- A free address below HSA (Highest Station Address)
- Increase of the retry value to at least 3
  (Network settings: user-defined profile)
- Checking and adapting of the slot time
  (Network settings: user-defined profile; bus parameters: Tslot parameter:
  You need short slot time values for OLM / P12, medium slot time values for OLM / G12 and OLM / G12-EEC and high slot time values for OLM / G12-1300. This results in a high performance for small networks and a medium to low performance with medium to large networks.

Additional information

Additional information on adaptation of the retry value and the slot time is available in the PROFIBUS Network Manual (http://support.automation.siemens.com/WW/view/en/35222591).

3.5 Additional network stations

Communication load - considering additional network stations

The bus parameters depend on the communication volume of the active network stations. There are differences between cyclical communication (DP) and connection-oriented, acyclical communication (S7 communication, Send/Receive (FDL)). Contrary to DP, the number and size of the communication jobs (communication load) depends on the user program. This means the communication load cannot always be determined automatically.

If you select the check box "Consider the following network stations", you can consider network stations in the calculation of the bus times that were not configured in the project.

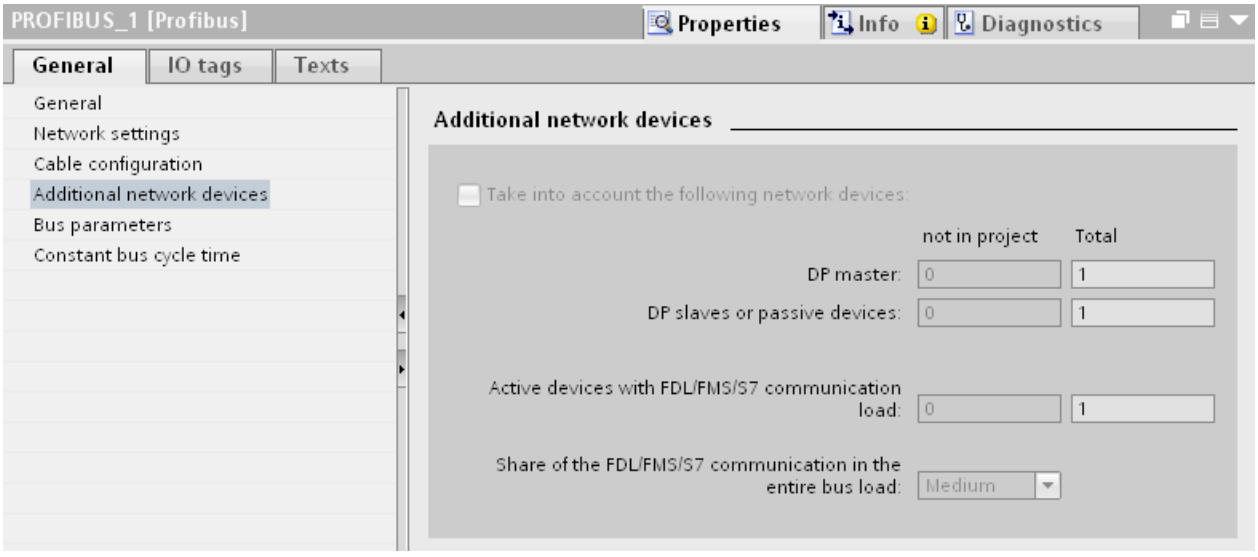


Figure 3-515 Additional network stations

Calculating the bus times

You can specify a network configuration in the parameter group "Additional network stations" for calculation of the bus times that deviates from the configured network configuration.

The network configuration is available for the following profiles:

- Standard
- Universal (DP/FMS)
- User-defined

Quantification of the communication load

The following settings are possible to take the communication load into consideration:

- Number of network stations that are not configured
- Information on the communication load from the user programs for FDL or S7 communication. You can choose from the following levels:
  - Low: Typical for DP, no larger data communication except DP.
  - Medium: Typical for mixed operation of DP and other communication services (e.g., S7 communication), if DP has high time requirements and with medium, acyclical communication volume.
  - High: For mixed operation of DP and other communication services (e.g., S7 communication), if DP has low time requirements and with high, acyclical communication volume.

3.6 Bus parameters

Introduction

Bus parameters control the transmission behavior on the bus. Each device on the bus must correspond with the bus parameters of other devices.

NOTE

The PROFIBUS subnet will only work properly if the parameters for the bus profile have been synchronized. Change the preset values only if you are familiar with the parameter assignment of the bus profile for PROFIBUS.

Cyclical distribution of the bus parameters

If the check box "Activate cyclical distribution of bus parameters" is selected under "Bus parameters" with the selected PROFIBUS subnet in the Inspector window, the bus parameters are sent cyclically during operation by the modules that support this function. This way you can, for example, connect a programming device to the PROFIBUS during operation.

Disable this function in the following cases:

- In constant bus cycle time mode to minimize the bus cycle.
- If third-party devices are connected in the PROFIBUS subnet whose protocol uses the DSAP 63 (Destination Service Access Point) for multicast.

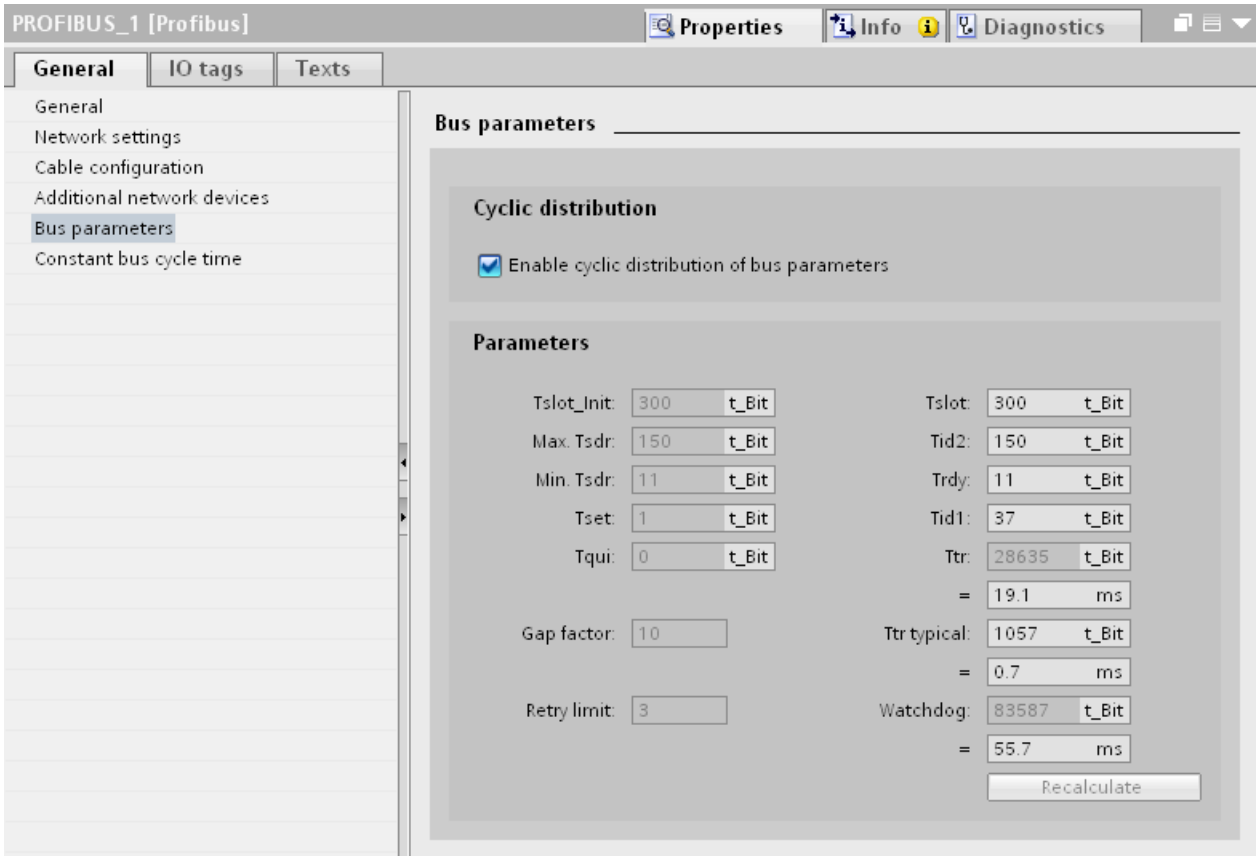


Figure 3-516 Bus parameters

Bus parameters for the bus profile of PROFIBUS subnets

NOTE

Display of offline values

The offline values of the bus parameters are always displayed even if they are connected online with the target system.

Table 3-60 Bus parameters - value ranges

Bus parameters	Adjustable [1]	Limit values
Tslot_Init	Yes	Max. Tsdr + 15 <= Tslot_Init <= 16.383 t_Bit
Max. Tsdr	Yes	35 + 2*Tset + Tqui <= Max. Tsdr <= 1,023 t_Bit
Min. Tsdr	Yes	11 t_Bit <= Min. Tsdr <= MIN(255 t_Bit, ... Max. Tsdr - 1, 34 + 2*Tset + Tqui)
Tset	Yes	1 t_bit <= Tset <= 494 t_bit
Tqui	Yes	0 t_bit <= Tqui <= MIN(31 t_bit, Min. Tsdr - 1)
GAP factor	Yes	1 <= GAP factor <= 100
Retry limit	Yes	1 <= Retry limit <= 15
Tslot (slot time)	No	-

[1] depending on bus profile

Bus parameters	Adjustable [1]	Limit values
Tid2	No	Tid2 = Max. Tsdr
Trdy	No	Trdy = Min. Tsdr
Tid1	No	Tid1 = 35 + 2*Tset + Tqui
Ttr (Target Rotation Time)	Yes	256 t_Bit <= Ttr <= 16,777,960 t_bit
Ttr typical	No	This time is for information only and is not transmitted to the devices.
Watchdog		10 ms <= Watchdog <= 650 s

[1] depending on bus profile

User-defined bus profile

Use the following settings to create a user-defined bus profile:

- minimum Target Rotation Time (Ttr) = 5000x HSA (highest PROFIBUS address of an active device)
- minimum watchdog (Watchdog) = 6250x HSA

Recalculate

Use the button "Recalculate" to recalculate the parameters.

3.7 Constant bus cycle time

Constant bus cycle time

The DP master addresses its assigned DP slaves cyclically. S7 communication may cause the intervals to vary. You can enable a "bus cycle with constant bus cycle time" to achieve identical intervals. This ensures data transmission at the same (constant bus cycle time) intervals.

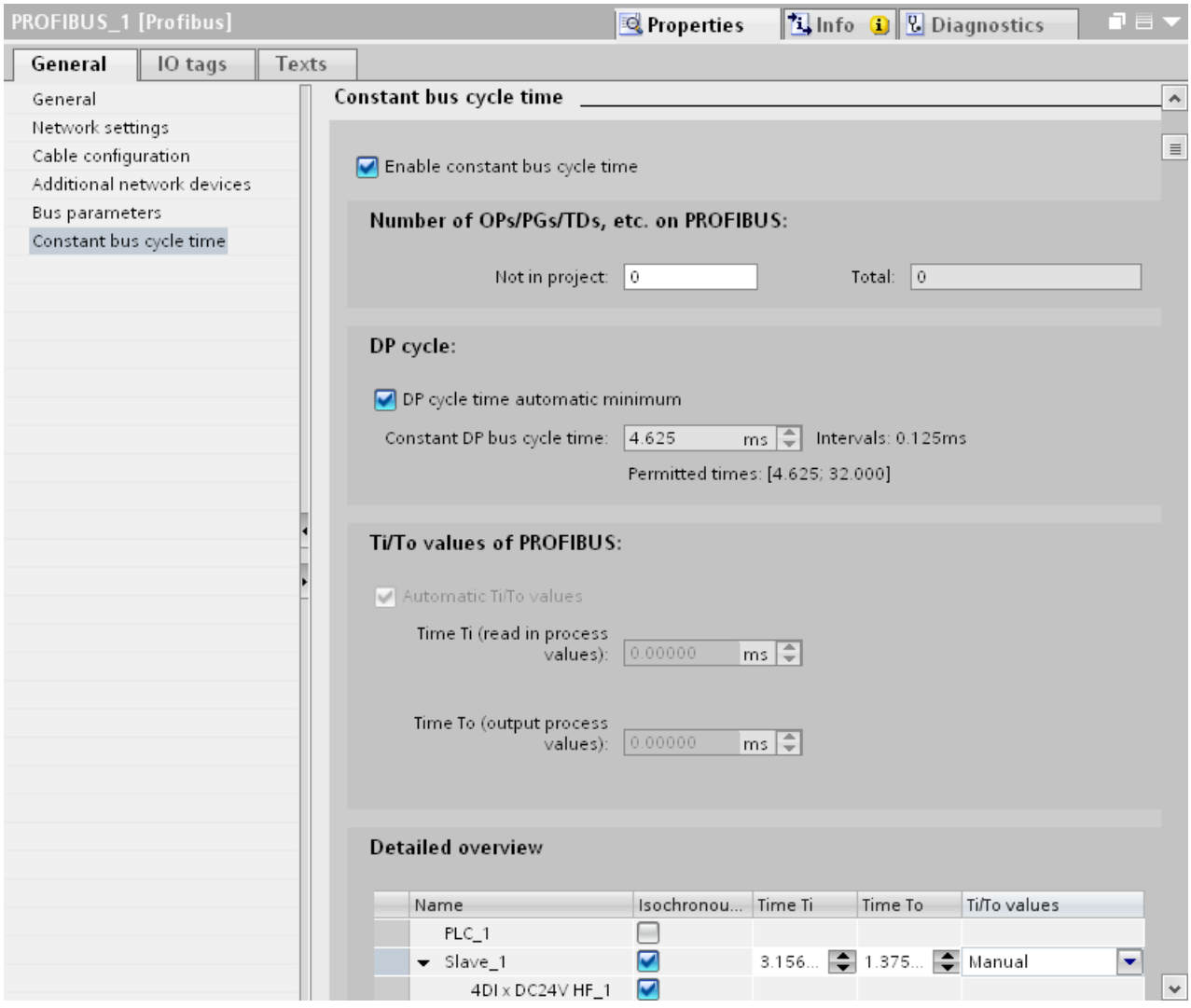


Figure 3-517 Enabling a bus cycle with constant bus cycle time

Number of OPs/PGs/TDs at the PROFIBUS

Here you enter the number of devices that are not configured.

Increasing DP cycle time manually

The following situation can occur especially with very short DP cycle times:
The runtime of the user program is greater than the shortest cycle (see Technical specifications of the CPU, section "Isochronous mode"). You have to manually increase the automatically calculated DP cycle time in this case.

See also

Configuring isochronous mode (Page 59)

Diagnostics

4

4.1 Overview

Diagnostics options

In case of an error you can determine the current status of your automation system and react specifically by using the event-related diagnostics and the evaluation of interrupts.

You can use the following options for diagnostics of the PROFIBUS components:

- Determine the status of the system using the Lifelist in STEP 7.
- Evaluate the module status, error and message texts by using the display of the S7-1500 CPU.
- Run cable diagnostics during operation by means of the diagnostics repeater.
- Evaluate the diagnostics and interrupt behavior in isochronous mode. (Page 62)
- Determine status information for fault localization and fault rectification by using the DP/PA coupler FDC 157-0 configured as PROFIBUS diagnostics slave.

Additional information

Additional information on diagnostics is available in these manuals:

- In the Diagnostics repeater for PROFIBUS-DP (http://support.automation.siemens.com/WW/view/en/7915183) manual for diagnostics with STEP 7, diagnostics in the user program, monitoring function isochronous PROFIBUS, topology display in STEP 7.
- In the Diagnostics (http://support.automation.siemens.com/WW/view/en/59192926) function manual for diagnostics options that are available for the SIMATIC systems S7-1500, ET 200MP, ET 200SP and ET 200AL.
- In the PROFIBUS Network Manual (http://support.automation.siemens.com/WW/view/en/35222591) system manual for diagnostics of fiber-optic cables.
- In the DP/PA Coupler, Active Field Distributors, DP/PA Link and Y Link (http://support.automation.siemens.com/WW/view/en/1142696) operating instructions.
- In the Web Server (http://support.automation.siemens.com/WW/view/en/59193560) function manual for diagnostics options (based on the functionality of the CPU).

4.2 Diagnostics using the display of the S7-1500

Displays

Each CPU in the S7-1500 automation system has a front cover with a display and operating buttons. Control and status information is displayed in different menus on the display. You use the operating buttons to navigate through the menus.

The following states can be evaluated on the display:

- Module status for central and distributed modules
- Error and alarm texts (system diagnostics, user-defined alarms)

Module status

From the station overview you go to the module status for a distributed module via the module overview.



Figure 3-518 Example: Station overview, module overview, module status

Error and alarm texts

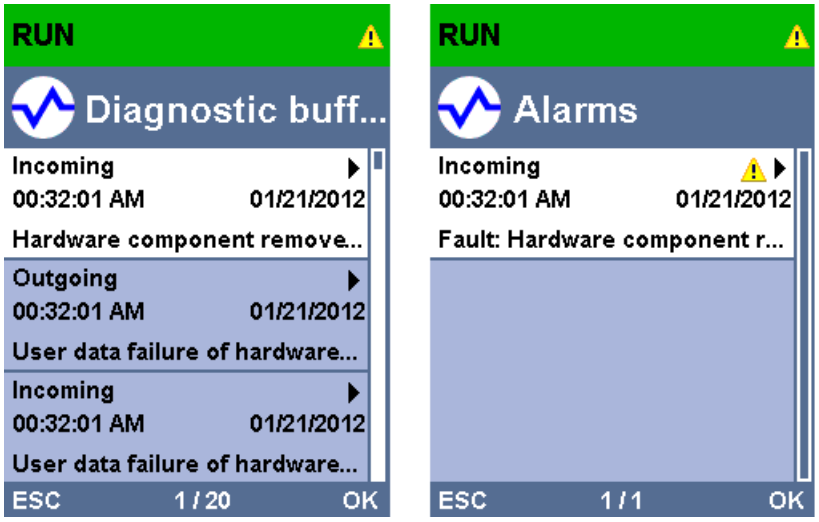


Figure 3-519 Example: Diagnostic buffer, alarms

Additional information

Additional information on the topic "Functions and operation of the display" is available in the documentation for the S7-1500 automation system on theInternet (http://support.automation.siemens.com/WW/view/en/59191792).

4.3 Diagnostics with the diagnostic repeater

Introduction

The diagnostic repeater is a repeater that can monitor two segments of a RS485-PROFIBUS subnet (copper cable) during operation and signal cable faults to the DP master by sending a diagnostic frame. Fault location and the cause of the fault can be displayed in plain text by means of STEP 7 as well as operator control and monitoring devices (SIMATIC HMI).

With its cable diagnostics during operation, the diagnostic repeater allows you to detect and localize cable faults early on. This means plant faults are detected early and plant downtimes can be prevented.

Diagnostic functions

- The diagnostic function provides the location and the cause of cable faults, such as wire break or missing terminating resistors. The fault location is specified relative to the devices present, for example "Break on signal line A and/or B".
- Reading out the saved diagnostic and statistical information.
- Monitoring of the isochronous PROFIBUS, e.g., violation of cycle time.
- Providing identification data.

Additional information

Additional information on diagnostics with STEP 7 and for reading out the diagnostics with the user program is available in the Diagnostic repeater for PROFIBUS DP (http://support.automation.siemens.com/WW/view/en/7915183) manual.

4.4 I&M data (Identification and Maintenance)

Definition and properties

Identification and maintenance data (I&M) is information saved in a module to provide support when:

- Checking the plant configuration
- Locating hardware changes in a plant

Identification data (I data) is module information (some of which may be printed on the module housing) such as the order and serial number. I data is read-only, vendor-specific module information.

Maintenance data (M data) is system-specific information such as the installation location and date. M data is generated in the course of configuration and is written to the module memory.

The modules can be uniquely identified in online mode by means of the I&M data.

Additional information

Information if and to what extent a DP device supports I&M data is available in the respective device manual of the device.

Functions

5

5.1 Isochronous mode

5.1.1 What is isochronous mode?

Why isochronous mode?

Assuming public transport were to operate at maximum speed while reducing stop times at the passenger terminals to absolute minimum, the last thing many potential passengers would notice of the departing contraption are its red tail lights. The overall travel time is, however, decided by the train, bus or underground clock, because well adjusted timing is essential to a good service. This also applies to distributed automation engineering. Not only fast cycles but also the adaptation and synchronization of the individual cycles result in optimum throughput.

Just-In-Time

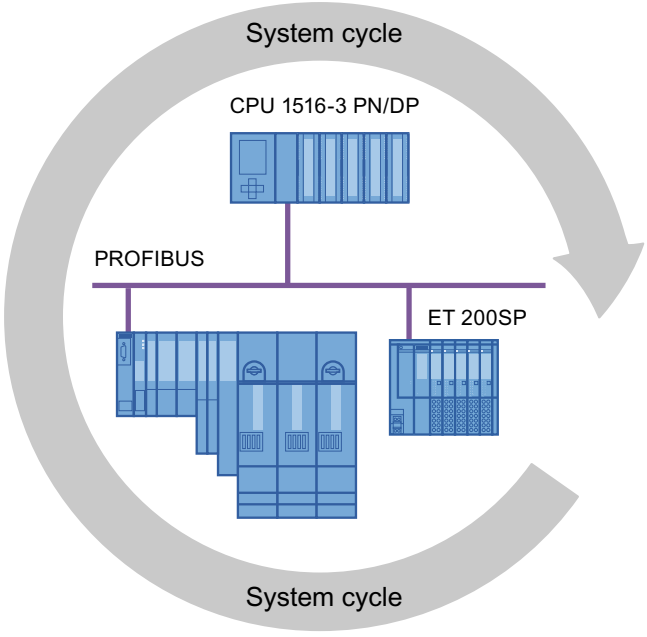


Figure 3-520 System cycle

The high speed and reliable reaction time of a system operating in isochronous mode is based on the fact that all data is provided just-in-time. The constant bus cycle time PROFIBUS DP cycle beats the time here.

Advantages of isochronous mode

The use of isochronous mode provides:

- Optimized controls
- Determinism
- Consistent (simultaneous) reading of input data
- Consistent (simultaneous) output of output data

5.1.2 Use of isochronous mode

The system property "isochronous mode" enables recording of measured values and process data in a defined system cycle. Signal processing takes place in the same system cycle all the way to switching to the "output terminal". This means isochronous mode improves the control quality and provides greater manufacturing precision. Isochronous mode drastically reduces the possible fluctuations of process response times. The time-assured processing can be used for a higher machine cycle.

Isochronous mode is basically always the choice when acquisition of measured values needs to be synchronized, movements need to be coordinated and process reactions need to be defined and take place simultaneously. This means the areas of applications for isochronous mode are manifold.

5.1.3 Isochronous applications

Example: Isochronous measurement at several measuring points

QC requires precise measurement of dimensions within a camshaft production process.

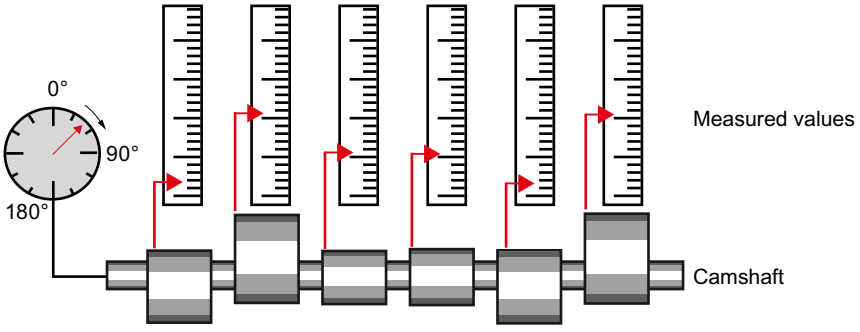


Figure 3-521 Measuring of camshafts

Isochronous workflow

By using the system property "isochronous mode" and the associated simultaneous measured value acquisition, measurement can be performed continuously and the time required for measurement is reduced. Resultant workflow:

- Continuous turning of the camshaft.
- During the continuous turning, measure the positions and cam excursion synchronously.
- Process the next camshaft.

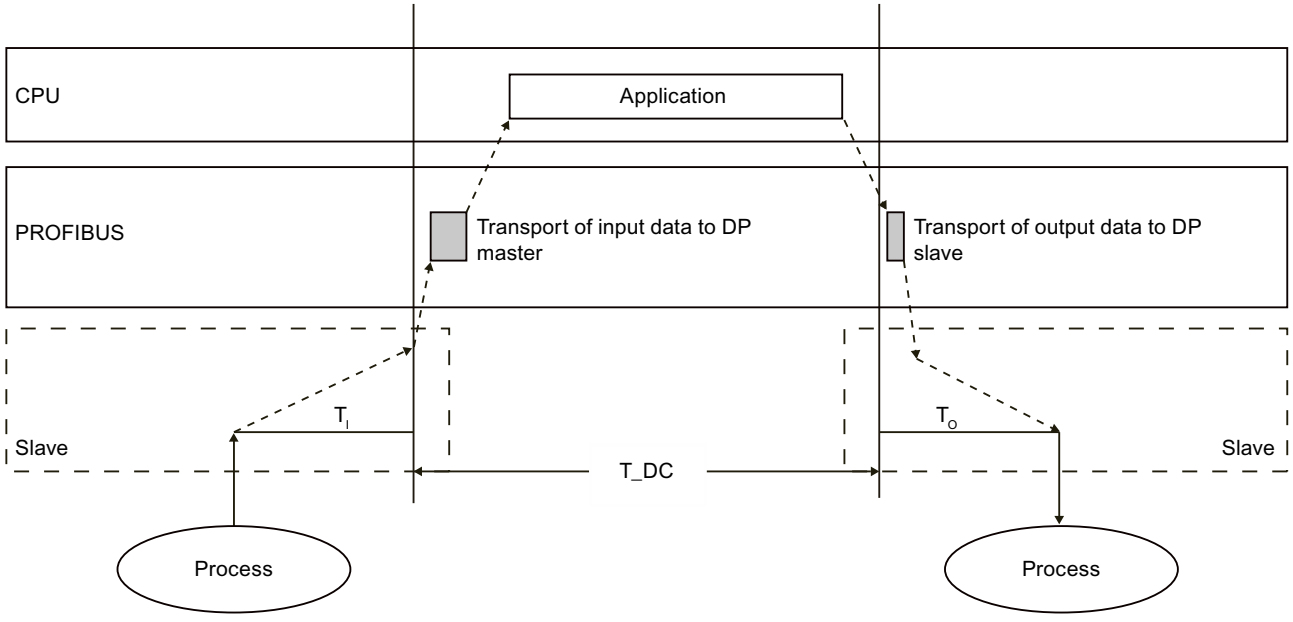
All camshaft positions and the corresponding measured values (red) are measured synchronously within a single rotation of the camshaft. This increases machine output and maintains or enhances precision of the measurement.

5.1.4 Sequence of synchronization

From reading of input data to output of output data

The sequence of all components involved in the synchronization is explained in the paragraphs below:

- Isochronous reading of input data
- Transport of input data by means of the PROFIBUS subnet to the DP master (CPU)
- Further processing in the isochronous application of the CPU
- Transport of output data by means of the PROFIBUS subnet to the output DP slave
- Isochronous output of output data



T_DC Date cycle
T_I Time for reading the input data
T_O Time for output of output data

Figure 3-522 Time sequence of synchronization

To ensure that all input data is ready for transportation via the PROFIBUS DP line when the next PROFIBUS DP cycle begins, the I/O read cycle has a lead time T_I so that it starts earlier. The T_I is the "flash gun" for all inputs. This T_I is necessary to compensate for analog to digital conversion, backplane bus times, etc. The lead time T_I can be configured by STEP 7 or by the user. We recommend that you have T_I assigned automatically by STEP 7 .

The PROFIBUS DP line transports the input data to the DP master. The synchronous cycle interrupt OB SynchronousCycle is called. The user program in the synchronous cycle interrupt

OB decides the process reaction and provides the output data in time for the start of the next data cycle. The length of the data cycle is always configured by the user.

T_o is the compensation from the backplane bus and the digital to analog conversion within the slave. The T_o is the "flash gun" for all outputs. The time T_o can be configured by STEP 7 or by the user. We recommend that you have T_o assigned automatically by STEP 7.

Without isochronous mode, application, data transmission and field devices have their own, unsynchronized processing cycles; these result in a higher total cycle time with high jitter. With isochronous mode, application, data transmission and field device are synchronized resulting in a minimum total cycle with minimum jitter.

Isochronous mode and non isochronous mode distributed I/O

It is possible to combine isochronous mode distributed I/O with non isochronous mode distributed I/O on one DP master.

5.1.5 Requirements for configuration

Note the following requirements for configuration of isochronous mode:

- Isochronous mode cannot be used in optical PROFIBUS networks.
- Constant bus cycle time and isochronous mode are only possible with the bus profiles "DP" and "User-defined".
- Isochronous mode is only possible with the DP interfaces integrated in the CPU. Isochronous mode with CPs for PROFIBUS is not possible.
- Only the constant bus cycle time master is permitted as active station on the isochronous PROFIBUS DP. OPs and PGs (for example, PCs with PG functionality) influence the time behavior of the isochronous DP cycle and are therefore not permitted.
- Isochronous mode is not permitted across lines.
- Isochronous I/O can only be processed in process image partitions. Isochronous consistent data transmission is not possible without the use of process image partitions. The adherence to quantity structures is monitored because the number of slaves and bytes on the DP master system is limited for each process image partition.
- The addresses of isochronous modules must be located in a process image partition.
- Full isochronous mode from "terminal" to "terminal" is only possible if all components involved in the chain support the system property "isochronous mode".

  Make sure you look for the entry "Isochronous mode" or "Isochronous processing" in the information box of the module when you select it in the catalog.
- When you configure isochronous mode, you may not assign a SYNC/FREEZE group to the slave.

5.1.6 Configuring isochronous mode

Introduction

A SIMATIC automation solution can be connected to the isochronous PROFIBUS with the isochronous mode function. Isochronous mode guarantees the synchronous reading of input data, the processing and output of output data at the same (isochronous) intervals.

Basic procedure for configuration of isochronous mode

1. Setting the properties for isochronous mode on the DP slave:
   - Isochronous DP cycle
   - Isochronous mode of the modules
2. Setting the properties for isochronous mode on the modules:
   - Synchronous cycle interrupt (SynchronousCycle)
   - Process image partition
   - Input delay
3. Create user program with access to isochronous I/O

Requirement

- The network view in STEP 7 is open.
- A CPU has been placed (e.g., CPU 1516-3 PN/DP).
- An interface module has been placed and networked with the CPU (e.g., IM 151-1 HF).
- I/O modules have been placed (e.g., 2DI x DC24V HF and 2DO x DC24V/0,5A HF).

Configuring isochronous mode on the DP slave

1. Select the DP slave in the network view and navigate to the "isochronous mode" area in the Inspector window.
2. Enable the option for synchronization to the DP cycle for the DP slave.
   Default: The DP slaves get the Ti/To values from the subnet which means the values are automatically the same for all DP slaves of the DP master system.
3. Enable the "Isochronous mode" option the the "Detail view" for all I/O modules you want to operate in isochronous mode.

4. Repeat steps 1 and 3 for all DP slaves that you want to operate in isochronous mode.

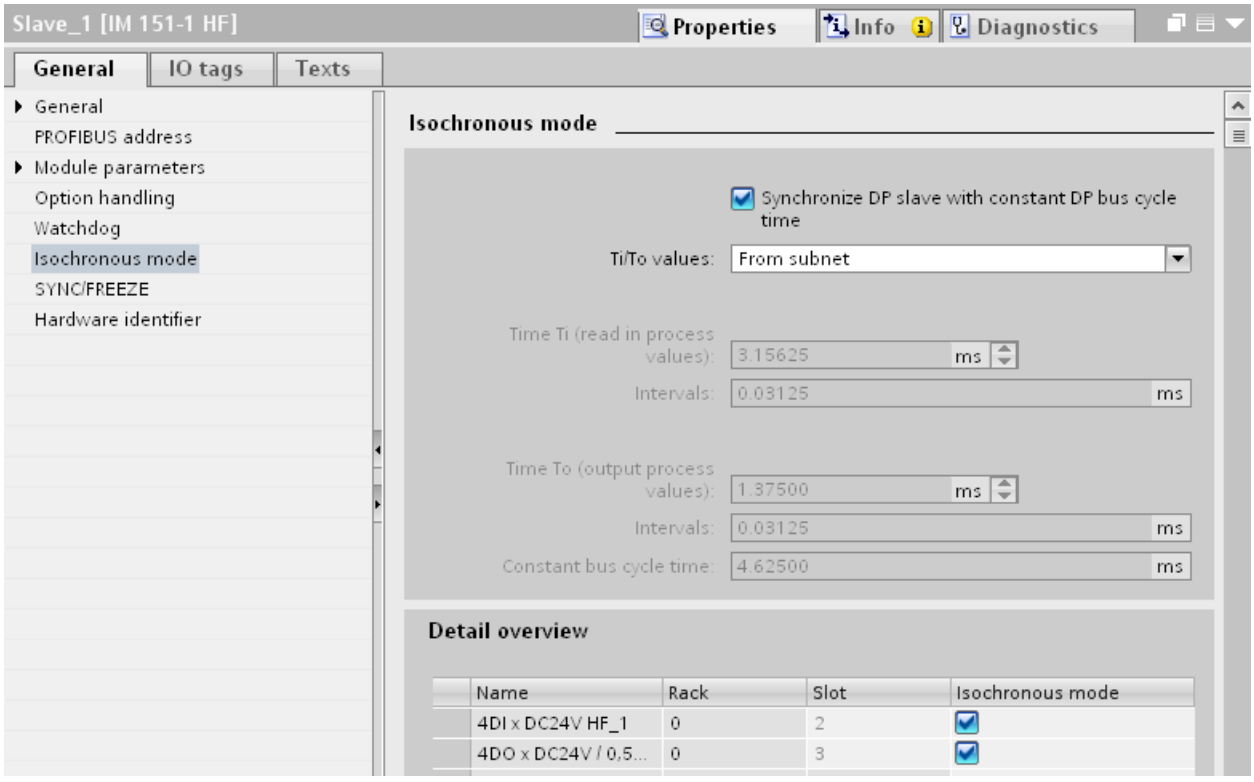


Figure 3-523 Configuring isochronous mode on the DP slave

Configuring synchronous cycle interrupt on the I/O module

1. Select an I/O module in the device view and navigate to the "I/O addresses" area in the Inspector window.
   – The option for isochronous mode is selected.
2. Select the synchronous cycle interrupt in the drop-down list.

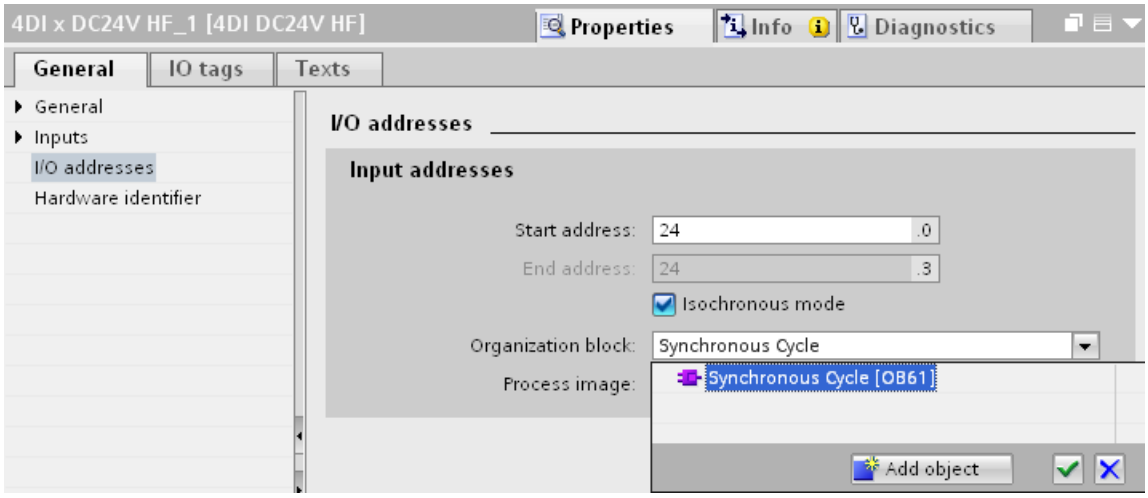


Figure 3-524 I/O addresses - creating the synchronous cycle interrupt OB

3. Assign the process image partition configured in the CPU.

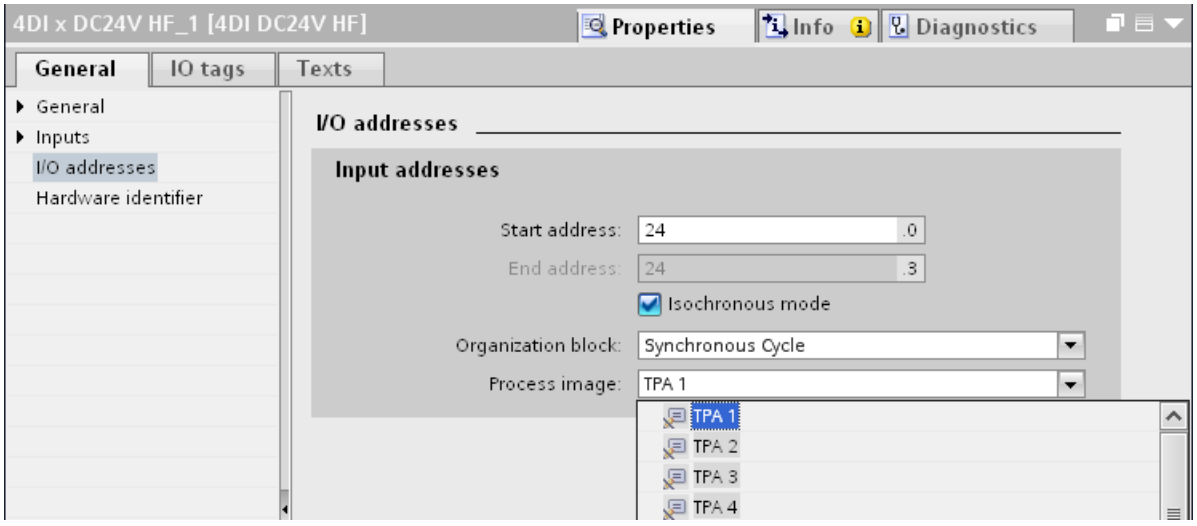


Figure 3-525 I/O addresses - assigning process image partitions

4. Repeat steps 1 and 3 for all I/O modules that you want to operate in isochronous mode.

Programming isochronous mode

To operate your plant in isochronous mode, the user program must be structured accordingly. This means you have to add a synchronous cycle interrupt in the STEP 7 project tree.

You access the isochronous I/O by means of a process image partition, which means the addresses of the isochronous modules must be located in a process image partition. You program access to isochronous I/O with the "SYNC_PI" instructions (updating the process image partitions of the inputs) and "SYNC_PO" (updating the process image partition of the outputs) in the synchronous cycle interrupt OB.

You call the "SYNC_PI" instruction at the start of the synchronous cycle interrupt OB, provided you have selected the automatic setting for the delay time. You call the "SYNC_PO" instruction at the end of the synchronous cycle interrupt OB.

5.1.7 Diagnostics and interrupt functions

The diagnostic and interrupt functions of STEP 7 are available for isochronous mode. These reduce downtimes and simplify localization and elimination of faults.

Events, causes of errors and remedies

Below, you will find the events for diagnostic and interrupt functions and remedies for the problem.

Table 3-61 Events, causes of errors and remedies

Event	Cause of the error	Remedy
• Synchronous cycle interrupt OB is started with the input parameter EventCount > 0 (number of lost OB calls since last OB call) If configured: • Call of the time error OB • Diagnostic buffer entry "Buffer overflow for OB6x events"	The synchronous cycle interrupt OB takes too long.	• Shorten the synchronous cycle interrupt OB. • Increase the DP cycle. • Reduce the delay time setting (setting with isochronous mode at synchronous cycle interrupt OB).
Error (negative RetVals) when updating the isochronous process image partition with SYNC_PI / SYNC_PO: • Consistency warning • Update time is after / before the permitted access window.	SYNC_PI / SYNC_PO are not called in the permitted access window in the synchronous cycle interrupt OB, which means they are called or processed during the I/O data transfer on PROFIBUS.	• Increase the delay time. • Increase the DP cycle. • Adapt the program.
Error when updating the isochronous process image partition with SYNC_PI / SYNC_PO: • Access error	DP slave / module does not respond / is not available.	

5.1.8 Parameter settings for isochronous mode

Parameter changes as task of the field service technician

The task of a field service technician is to maintain the production process.

In this context the technician has to detect, localize and eliminate errors and performance losses of isochronous mode.

All parameters which influence isochronous mode can be checked and configured using the "Isochronous mode" dialog box.

Parameters should only be changed by experienced users or service technicians.

5.1.8.1 Viewing isochronous mode parameters

"Isochronous mode" dialog box

1. Select "Properties > Isochronous mode" in the Inspector window.
   The "isochronous mode" dialog box opens with an overview of parameters which influence isochronous mode.
   Information on the individual parameters is available under "Detail overview".
2. Compare the values shown with the values in the documentation, or with the value specified by a technician.

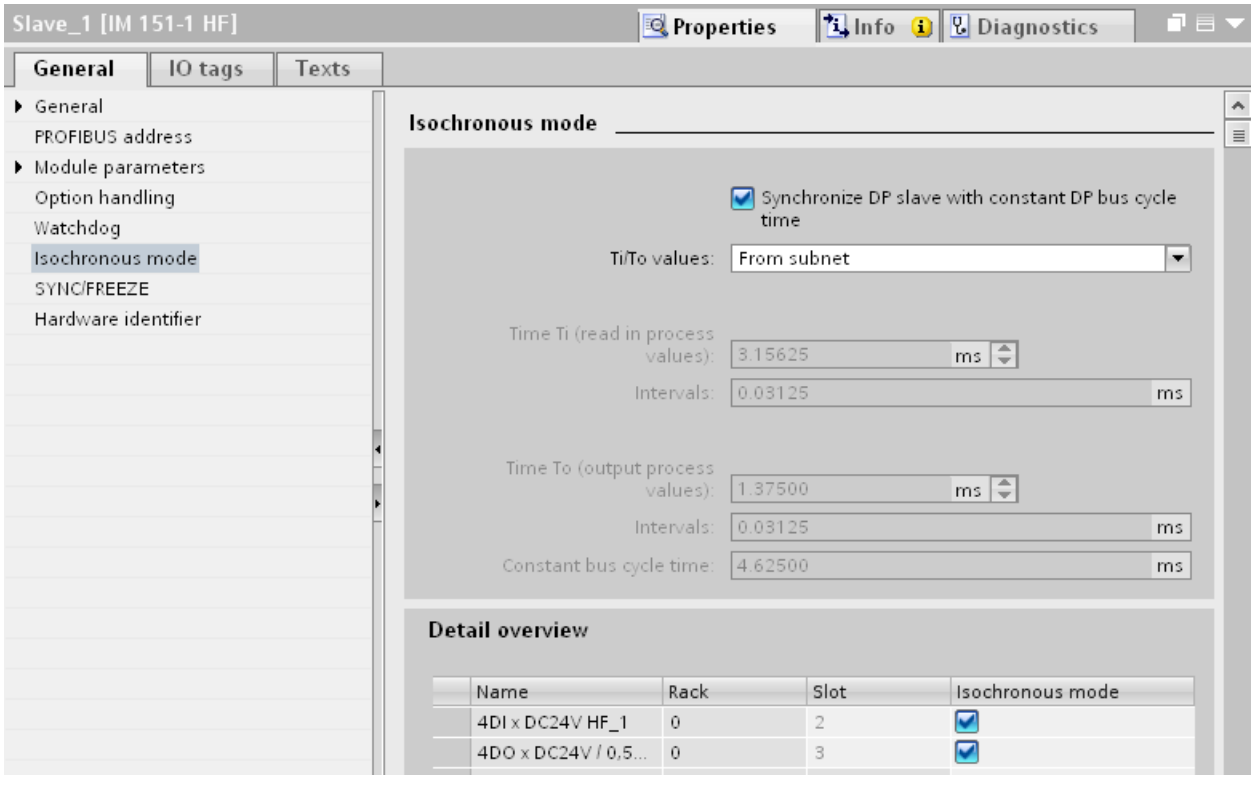


Figure 3-526 Viewing parameters for isochronous mode

5.1.8.2 Change parameters

Changing parameters for the DP master system

You can change the parameters for isochronous mode in the "Constant bus cycle time" dialog box.

1. Select the DP master system in the network view.
2. Select the section "Constant bus cycle time" in the Inspector window.
3. Change the parameters according to the received instructions.

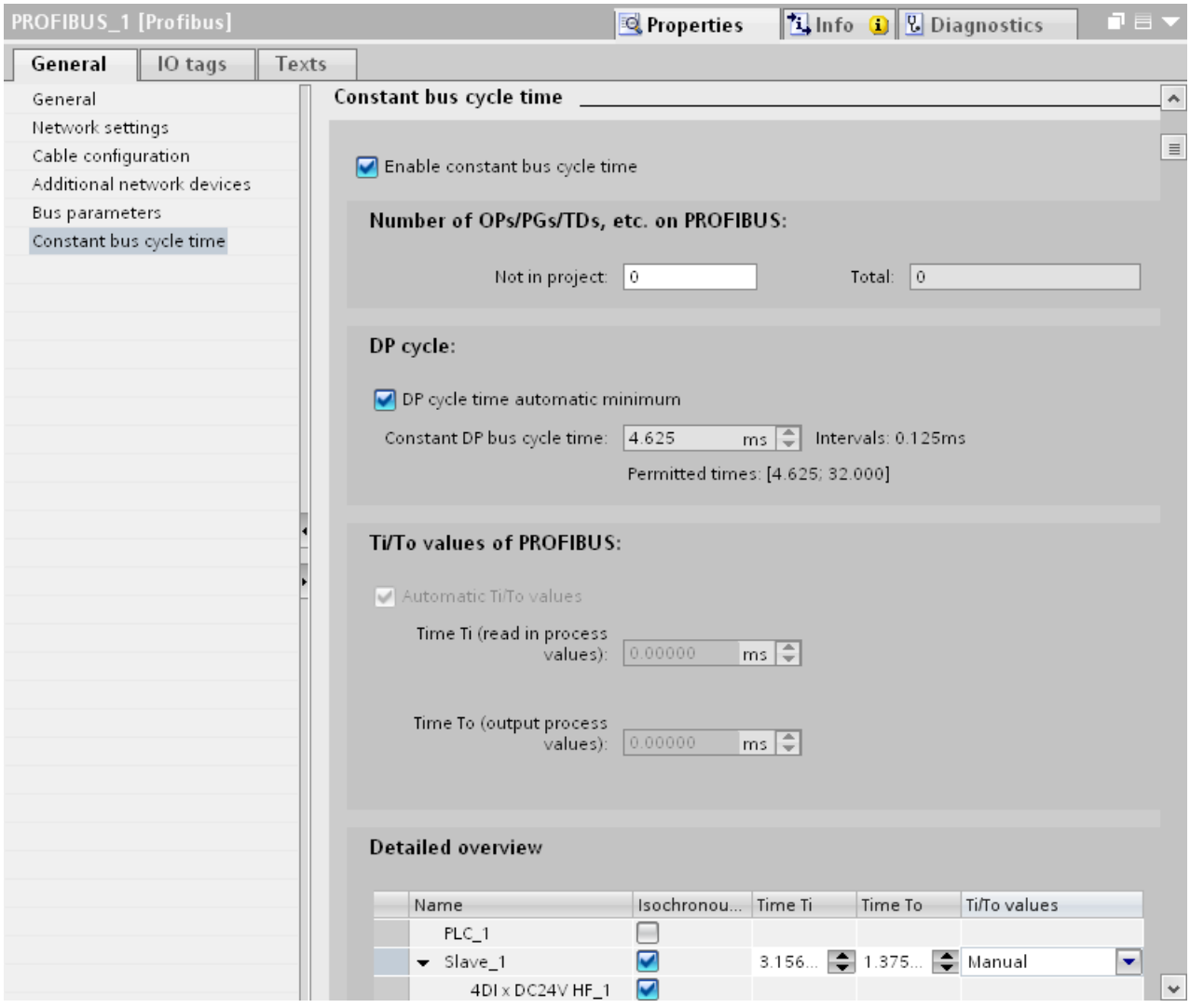


Figure 3-527 Changing parameters for the DP master system

Adapting the input delay

1. Select the input module in the device view.
2. Select the section "Inputs" in the Inspector window.
3. Adapt the input delay.

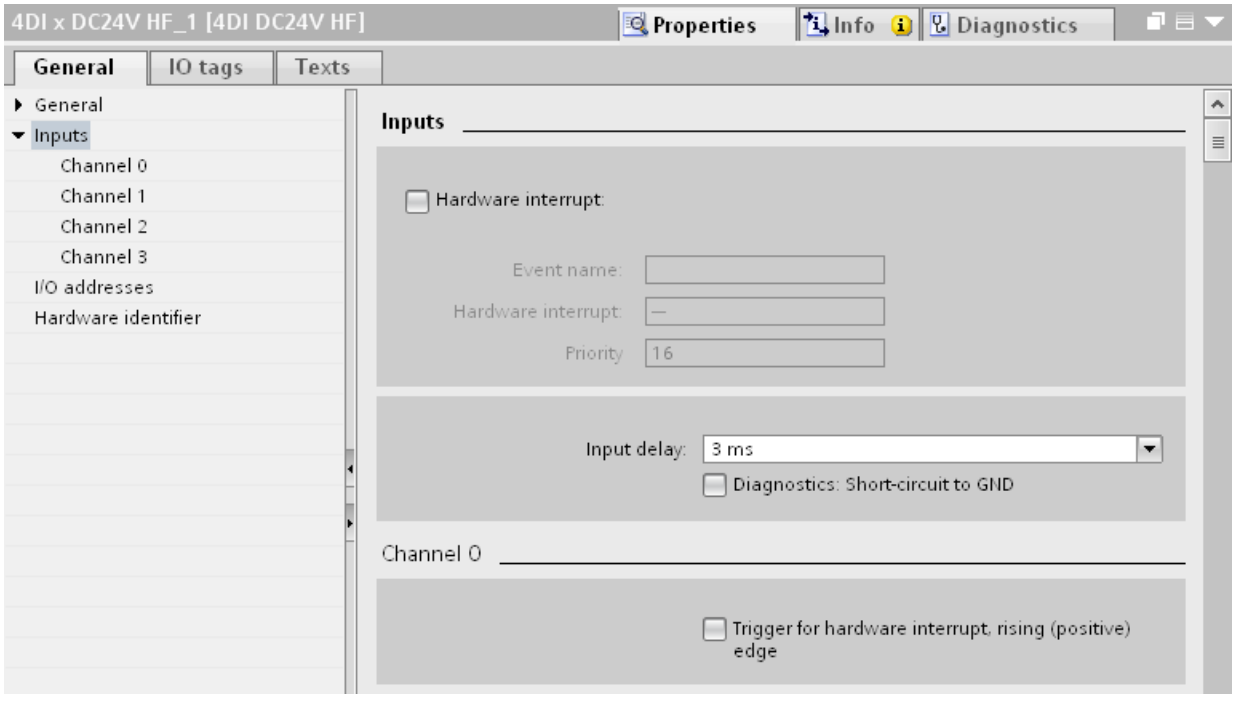


Figure 3-528 Adapting the input delay

Compile, load and save the changed configuration

1. Put the plant out of operation.
2. Select the CPU in the project navigator.
3. Select "Compile > Hardware" in the shortcut menu.
4. Select "Download to device" in the shortcut menu.
5. Save the project.

5.2 Acyclical data exchange

Additional functionality with DPV1 devices (DP master/DP slaves)

DP masters and DP slaves that support DPV1 have the following additional functions compared to the devices that support only DPV0:

- The acyclic data exchange between master and slave is supported.
- Interrupts can be set by a DPV1 slave which ensure handling of the interrupt-triggering event in the master CPU.

Acyclic data exchange

Read/write data record, for example, to change the parameters of a slave during operation. The data records of a module and the structure of these data records is available in the documentation for the respective module.

The table below contains the instructions with their functions for access to DPV1 slaves. Detailed information is available in the STEP 7 online help.

Table 3-62 Instructions for access to DPV1 slaves

Instructions	Function (DPV1)
RDREC	Read data record
WRREC	Write data record
RALRM	Receive interrupt from a DP slave. (The instruction must be called in the OB that triggers the interrupt.)

5.3 SYNC/FREEZE groups

Assigning the SYNC/FREEZE group to the DP slave

A DP master with the corresponding functionality can send the control commands SYNC and/or FREEZE for synchronization of the DP slaves simultaneously to a group of DP slaves. You must assign SYNC/FREEZE groups to the DP slaves for this purpose.

Requirement: A DP master system has been created in the project.

Procedure

To assign a DP slave to a SYNC/FREEZE group, follow these steps:

1. Select the DP interface of the DP slave you want to assign to a group in the device view or network view.
2. Select the check boxes for the required SYNC/FREEZE groups under the group "SYNC/FREEZE" in the Inspector window.

   You can assign each DP slave to only one SYNC/FREEZE group.

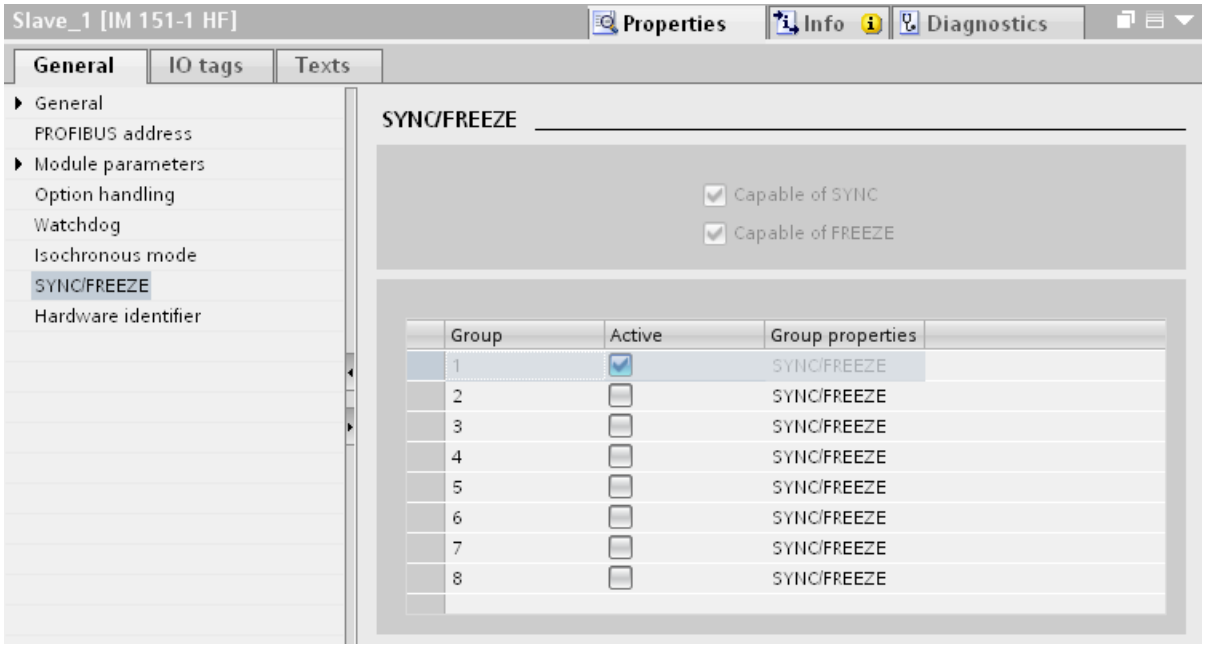


Figure 3-529 Assigning the DP slave to a SYNC/FREEZE group

Important information on the control commands SYNC and FREEZE

You can use the control commands SYNC and FREEZE in the DP master to synchronize the DP slaves event-controlled. The DP master sends the control commands simultaneously to a group of DP slaves in its master system. It does not take into consideration DP slaves that have failed or are currently sending diagnostic information.

Requirement for synchronization using control commands is that you have assigned the DP slaves to SYNC/FREEZE groups.

For a S7 CPU use the instruction DPSYC_FR (SFC 11) to synchronize the DP slaves.

When you select the DP master, you see a list of the eight SYNC/FREEZE groups under "Properties > DP interface > SYNC/FREEZE" in the Inspector window.

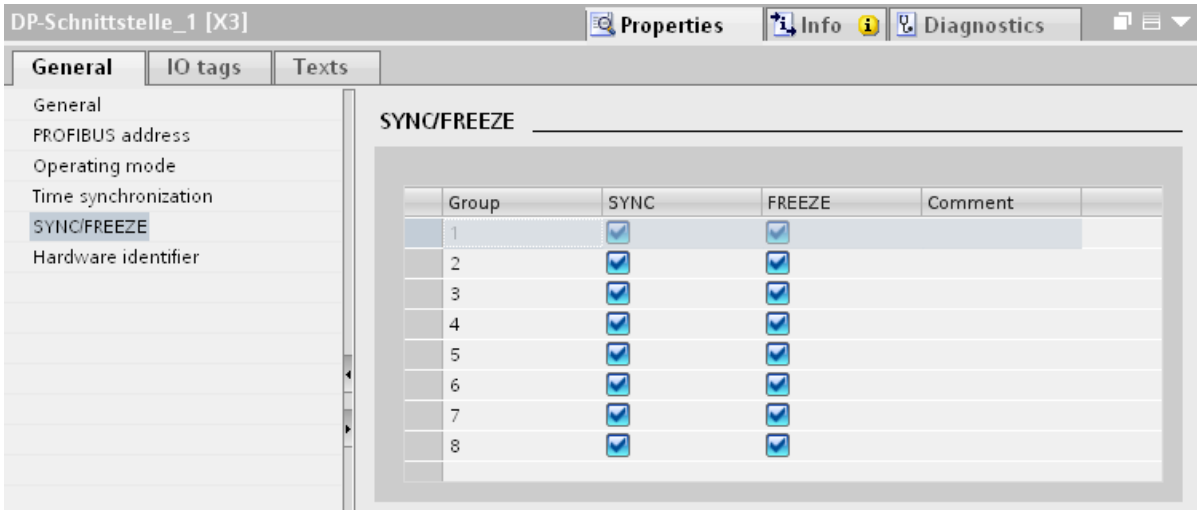


Figure 3-530 SYNC/FREEZE groups on DP master

SYNC control command

The DP master uses the SYNC control command to cause a group of DP slaves to freeze the states of their outputs to the current value.

The DP slaves save the output data of the DP master for the following frames. But the states of the DP slave outputs remain unchanged.

Only after each new SYNC control command does the DP slave set its outputs to the values that it has saved as the output data of the DP master.

The outputs are not updated cyclically again until the DP master has sent a UNSYNC control command.

FREEZE control command

After receiving the FREEZE control command from the DP master, the DP slaves of a group freeze the current status of their inputs. The DP slaves send these frozen input data to the DP master with the following cyclical frames.

The DP slaves freeze the current state of their inputs again after each new FREEZE control command.

The state of the DP slave inputs is only send to the DP master cyclically again when the DP master sends the UNFREEZE control command.

5.4 Interrupts

Interrupts and interrupt OBs for DPV1

Interrupts can be set by a DPV1 slave which ensure handling of the interrupt-triggering event in the master CPU. The interrupt data is evaluated in the CPU and the diagnostics buffer and the module state are updated even in the "STOP" operating mode. The OB is not processed in STOP.

The following DPV1 interrupts are supported:

- Status interrupt
- Update interrupt
- Vendor-specific interrupt

Detailed information is available in the descriptions on the OBs. You can use the corresponding OBs that are provided by the operating system of the S7 CPUs for diagnostic interrupts, hardware interrupts, and pull/plug interrupts.

OB 55 interrupt - Status interrupt

The status interrupt can be triggered when the operating mode of a device or module changes, for example, from RUN to STOP.

OB 56 interrupt - Update interrupt

An update interrupt can be triggered if the parameters of a slot were changed. This may be caused by local access or partner access to the parameters.

OB 57 interrupt - Vendor-specific interrupt

The event that triggers the vendor-specific interrupt can be specified by the manufacturer of a DPV1 slave.

Additional information

A detailed description of the events at which interrupts are triggered is available in the documentation of the respective manufacturer of the DPV1 slave.

5.5 Intelligent DP slaves (I-slaves)

5.5.1 I-slave functionality

I-slave functionality

The "I-slave" (intelligent DP slave) functionality of a CPU supports the exchange of data with a DP master and thus allows the CPU to be used, for example, as intelligent preprocessing unit of subprocesses. The I-slave is connected in its role as DP slave to a "higher-level" DP master.

The preprocessing is handled by the user program in the I-slave. The process values acquired by the I/O modules are preprocessed by the user program and made available to the DP master.

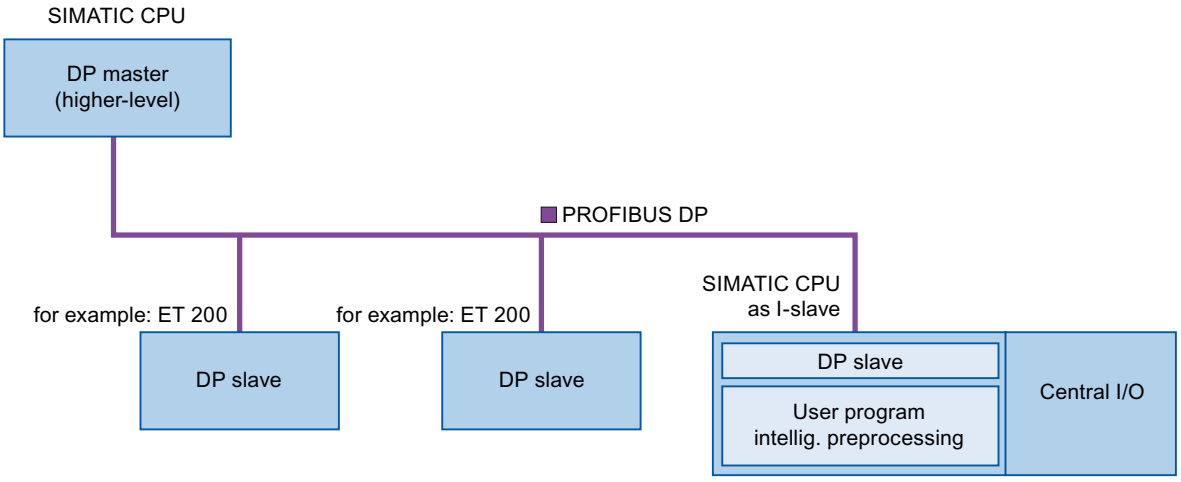


Figure 3-531 I-slave functionality

"I-slave" naming convention

In the remainder of this description, a CPU or a CP with I-slave functionality is simply called an "I-slave".

Advantages of configurations with I-slaves

The I-slave offers the following advantages:

- Simple coupling of CPUs with PROFIBUS interface
- Real-time communication between CPUs and PROFIBUS interface
- Distributed processing

  A complex automation task can be divided into smaller units/subprocesses. This results in manageable processes which lead to simplified subtasks.
- Relieving the DP master by distributing the computing capacity to I-devices
- Lower communication load by processing process data locally

- Separating subprocesses

  Complicated, widely distributed and extensive processes can be subdivided into several subprocesses with manageable interfaces by using I-slaves. These subprocesses can be stored in individual STEP 7 projects if necessary, which can later be merged to form one master project.
- Separating STEP 7 projects

  Creators and users of an I-device can have completely separated STEP 7 projects. The GSD file together with the configuration of the transfer areas of the I-slave form the interface between the STEP 7 projects. This allows coupling to standard DP masters via a standardized interface.
- Know-how protection

  Plant units can now only be delivered with a GSD file and the configuration of the transfer areas instead of with a STEP 7 project for the I-slave interface description. This means that you no longer have to disclose the user program know-how.

Difference: DP slave - I-slave

In the case of a DP slave, the DP master accesses the distributed inputs/outputs directly.

In the case of an I-slave, the DP master accesses a transfer area in the I/O address space of the preprocessing CPU instead of accessing the connected inputs/outputs of the I-slave. The user program running on the preprocessing CPU is responsible for ensuring data exchange between the operand area and inputs/outputs.

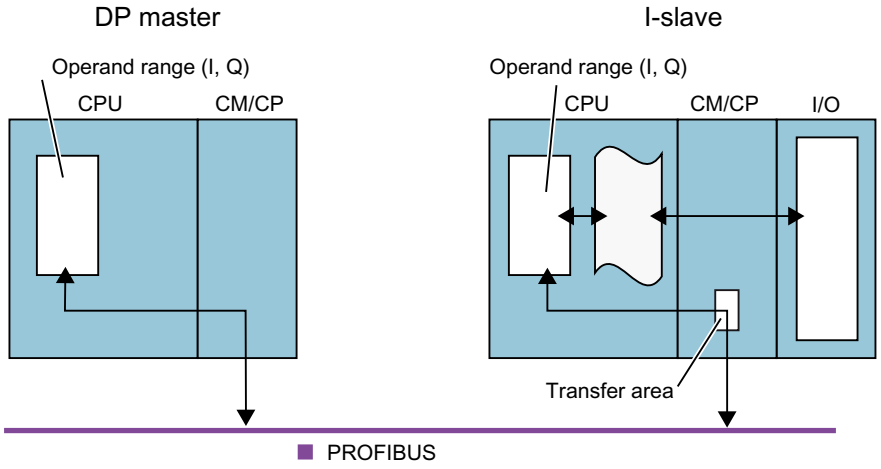


Figure 3-532 Data access to an I-slave

NOTE

DP master or DP slave

Note: The communication modules of the S7-1500 CPUs/ET 200SP CPUs, for example the CP 1542-5, support the operation as DP master or DP slave only as alternative.

NOTE

The I/O areas configured for data exchange between the DP master and DP slaves must not be used by I/O modules.

5.5.2 Data exchange with higher-level DP master

Introduction

The following section describes the data exchange between the I-slave and the higher-level DP master.

Transfer areas

Transfer areas are an interface to the user program of the I-slave CPU. Inputs are processed in the user program and outputs are the result of the processing in the user program.

The data for communication between DP master and I-slave is made available in the transfer areas. A transfer area contains an information unit that is exchanged consistently, in terms of bytes, words or overall, between DP master and I-slave. You can find more information on configuration and use of transfer areas in the section Configuring transfer areas (Page 74).

The following figure shows the data exchange between the I-slave and the higher-level DP master. The individual communication relations are explained below based on the numbers.

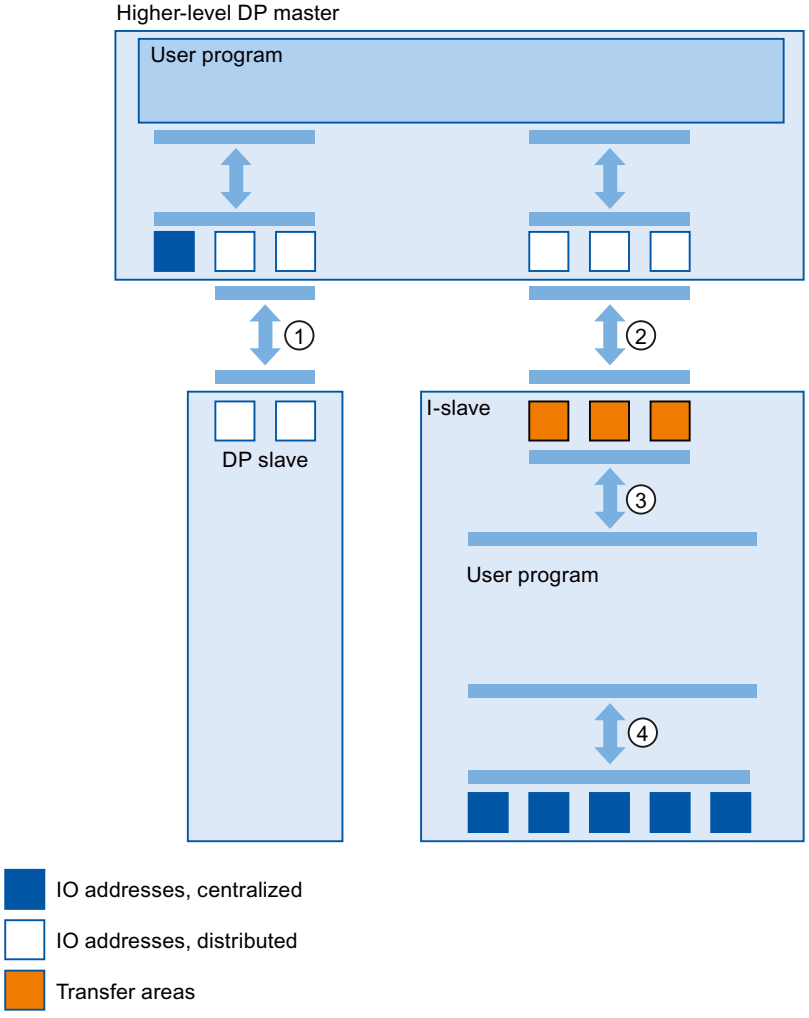


Figure 3-533 Data exchange with the DP master

① **Data exchange between higher-level DP master and normal DP slave**
In this way, the DP master and the DP slave exchange data through PROFIBUS.

② **Data exchange between higher-level DP master and I-slave**
In this way, the DP master and the slave exchange data through PROFIBUS.

The data exchange between a higher-level DP master and an I-slave is based on the conventional DP master/DP slave relationship.

For the higher-level DP master, the transfer areas of the I-slave represent submodules of a DP slave.

The output data of the DP master is the input data of the I-slave. Analogously, the input data of the DP master is the output data of the I-slave.

③ **Transfer relationship between the user program and the transfer area**
In this way, the user program and the transfer area exchange input and output data.

④ **Data exchange between the user program and the I/O of the I-slave**
In this way, the user program and the centralized I/O of the I-slave exchange input and output data.

5.5.3 Configuring an I-slave

Requirements for configuring an I-slave

The I-slave consists of:

- A CPU from S7-1500 and a communications module CM 1542-5/CP 1542-5 (STEP 7 as of V12)
- A CPU from ET 200SP and a communications module CM DP (STEP 7 as of V13 SP1)

Procedure for configuring an I-slave

This section shows how to configure an I-slave in STEP 7 based on the example of a CPU 1512SP-1 PN. The procedure for the CPUs from S7-1500 with CM 1542-5/CP 1542-5 and for the CPU 1510SP-1 PN with CM DP is the same.

To configure an I-slave, follow these steps:

1. Drag a CPU 1512SP-1 PN from the hardware catalog to the network view.
2. Open the device view of the CPU.
3. Double-click on the CM DP communications module in the hardware catalog.
   STEP 7 creates the CM DP in the device view.
4. Select the PROFIBUS interface of the CM DP communications module.
5. In the Inspector window in the area navigation, select the "Operating mode" entry and enable the "DP slave" check box.

6. Now you can select the DP master in the "Assigned DP Master" drop-down list.
   Once you have selected the DP master, the networking and the DP master system between both devices are displayed in the network view.

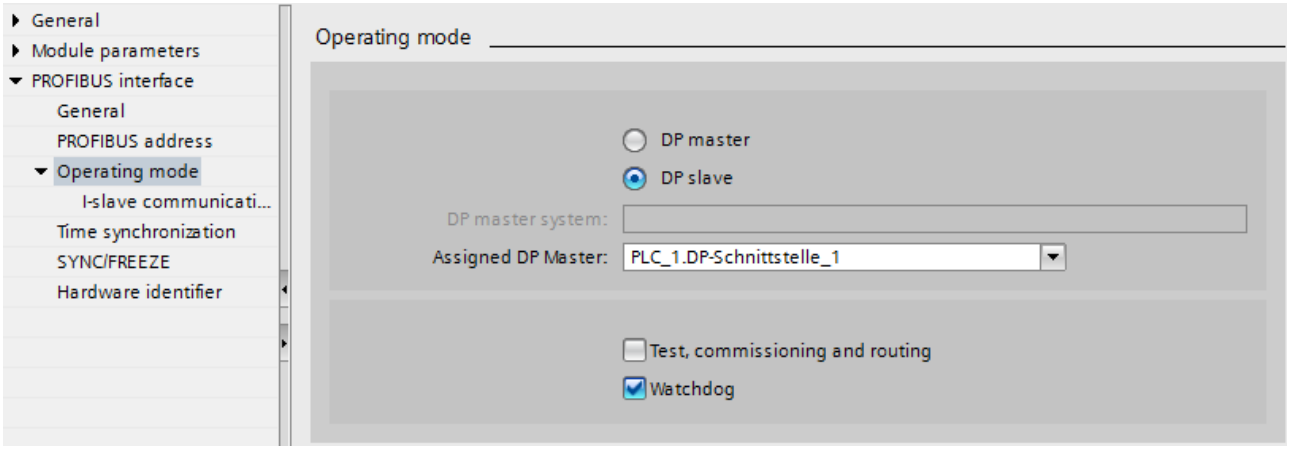


Figure 3-534 Configuring an I-slave

NOTE

Operation using a GSD file

If you operate an I-slave using a GSD file, you should not select the "Test, commissioning and routing" check box.

Create a DP subnet on the PROFIBUS interface of the I-slave.

Result

You have configured an I-slave.

5.5.4 Configuring transfer areas

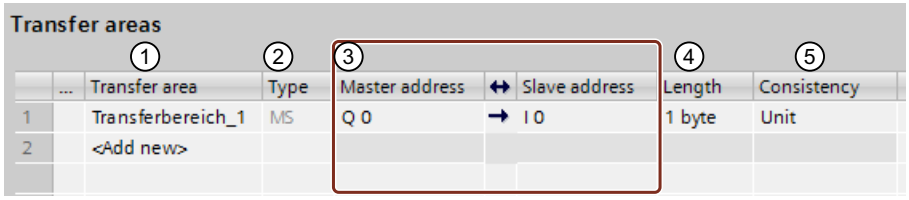
Requirements for configuring transfer areas

- You have configured an I-slave in STEP 7.
- You are in the device view of the I-device and have selected the PROFIBUS interface of the communications module.

Procedure for configuring transfer areas

To configure transfer areas for an I-slave in STEP 7, follow these steps:

1. In the area navigation, go to the section "Operating mode" > "I-slave communication" > "Transfer areas".
2. Create transfer areas. Set the properties of the created transfer areas.



① Click in the first cell of the "Transfer area" column. STEP 7 assigns a default name that you can change.

② Select the type of communication relation: Currently, you can only select MS for "master-slave communication relation".

③ STEP 7 assigns the addresses for the transfer area automatically. Correct the addresses if necessary.

④ Set the length of the transfer area. Specify the length of the transfer area in the cell in the following format: [1...64] Byte/Word.
Examples: "32 Byte", "64 Word"

⑤ Specify whether the transfer area is exchanged in units of bytes or words or consistently over the entire length between the DP master and I-slave.

Figure 3-535 Configuring transfer areas

A separate entry is created in the area navigation for each transfer area. If you select one of these entries, you can adjust the details of the transfer area, or correct them and comment on them.

5.5.5 Sample program

Introduction

This simple sample program shows how you use the transfer areas of an I-slave.

Requirement

You have configured an I-slave.

Task

The result of an "AND logic operation" of two inputs (preprocessing) in the I-slave is to be provided to the higher-level DP master. This result is to be assigned to a local output in the DP master (further processing).
Use a transfer area with the following addresses for this purpose:

- Address in the I-slave: Q568
- Address in the DP master: I68

Required steps

The following steps are necessary to solve the task:

1. Configuring the transfer area
2. Programming the I-slave
3. Programming the DP master

Configuring the transfer area

Configure a transfer area with the following properties in the I-slave:

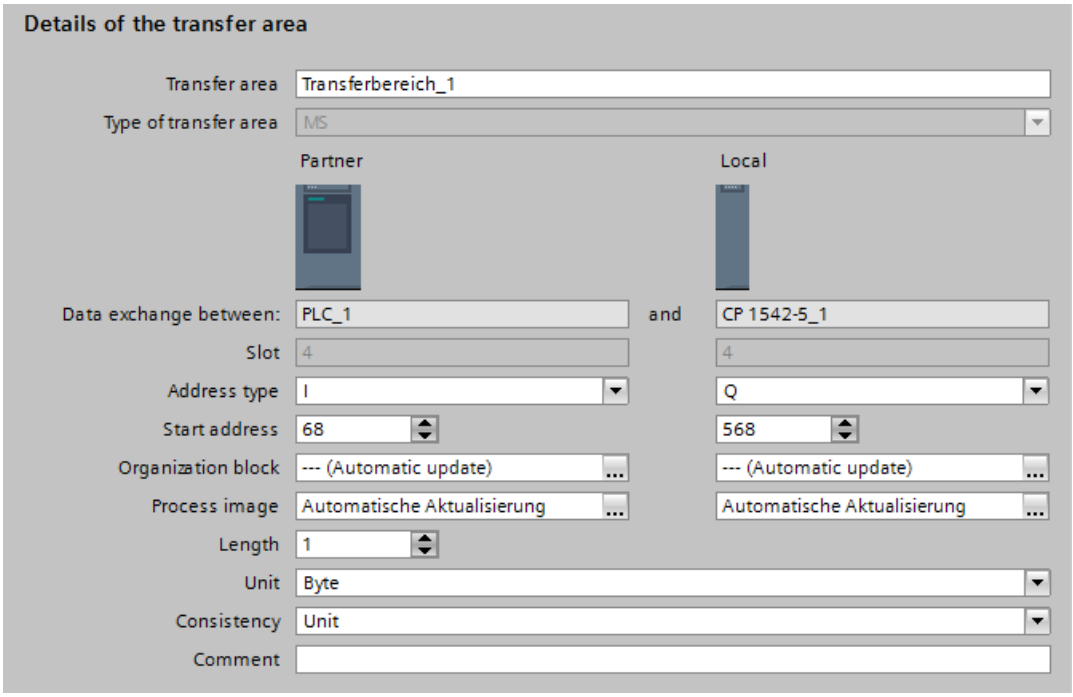


Figure 3-536 Transfer area, I-slave sample program

Programming the I-slave

To program the sample program for the I-slave, follow these steps:

1. Using the SCL programming language, create a new function with the name "preprocessing" in the project tree under "Program blocks" > "Add new block". Open the function.
2. In the interface of the function "preprocessing", create the following tags:

Name	Data type	Input/output type
input 1	bool	Input
input 2	bool	Input
result	bool	Output

3. In the instruction window of the function "preprocessing", write the following program code:
   #result:=#input 1&#input 2;
4. Call the function "preprocessing" in a cycle OB, for example, in OB1.
5. Wire the function "preprocessing" in the cycle OB as follows:

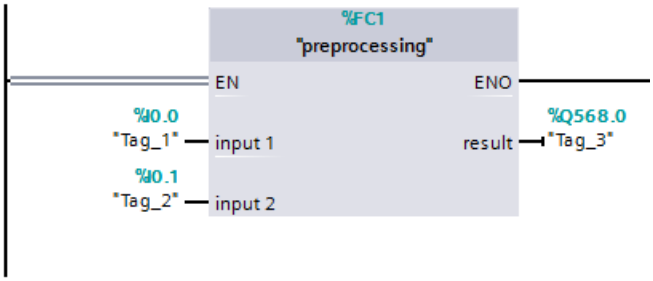


Figure 3-537 I-slave sample program

Programming the DP master

To program the sample program for the DP master, follow these steps:

1. Using the SCL programming language, create a new function with the name "further processing" in the project tree under "Program blocks" > "Add new block". Open the function.
2. In the interface of the function "further processing", create the following tags:

Name	Data type	Input/output type
result	bool	Input
output	bool	Output

3. In the instruction window of the function "further processing", write the following program code:
   #output:=#result;
4. Call the function "further processing" in a cycle OB, for example, in OB1.
5. Wire the function "further processing" in the cycle OB as follows:

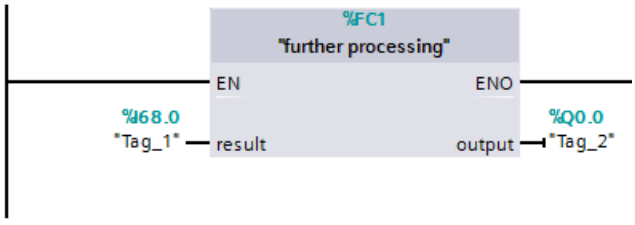


Figure 3-538 DP master sample program

Result

You mastered the task successfully.

5.5.6 Diagnostics and interrupt behavior

Diagnostics and interrupt behavior

S7 CPUs have numerous diagnostics and interrupt functions that can, for example, report errors/faults or failures of underlying DP systems. These diagnostics alarms reduce downtimes and simplify localization and elimination of problems.

Diagnostics options in the higher-level DP master and in the I-slave

The following diagnostics mechanisms are available to the higher-level DP master and the I-slave:

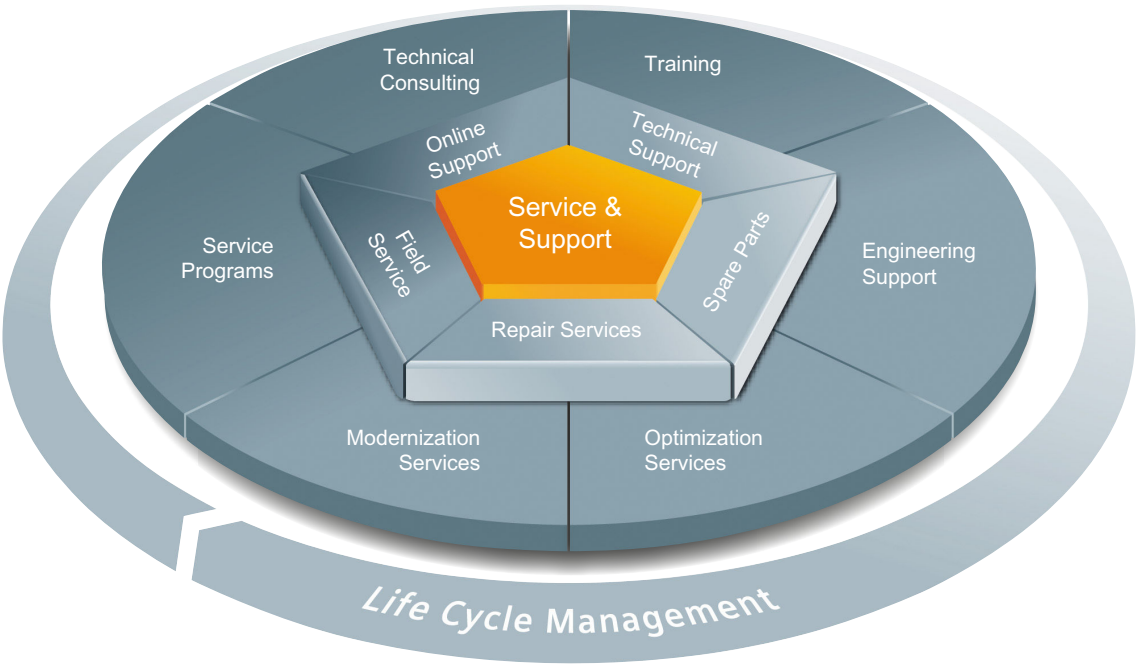
- OB 82 (diagnostic interrupt)
  When the I-slave changes mode, the DP master calls OB 82 (diagnostic interrupt).
  When the DP master changes mode, the I-slave calls OB 82 (diagnostic interrupt).
- OB 86 (rack failure)
  If the bus connection to the I-slave is interrupted, the DP master calls OB 86 (rack failure).
  If the bus connection to the DP master is interrupted, the I-slave calls OB 86 (rack failure).
- OB 122 (I/O access error)
  If you have not set the attribute "Handle errors within block" for OB 122, the following applies:
  - If the bus connection to the I-slave is interrupted, the DP master calls OB 122 (I/O access error) if there is direct access to the relevant transfer areas.
  - If the bus connection to the DP master is interrupted, the I-slave calls OB 122 (I/O access error) if there is direct access to the relevant transfer areas.

Reaction of the transfer areas to mode changes

Table 3-63 Reaction of the transfer areas to mode changes

DP master	I-slave	Reaction of DP master input transfer areas	Reaction of I-slave input transfer areas
RUN→STOP	RUN	No updating of the process image	The input transfer areas retain their current values. (no access error)
STOP→RUN	RUN	The input transfer areas are updated by the cyclic user program via the process image.	The input transfer areas are updated via the process image.
RUN	RUN→STOP	The I-slave sets the input transfer areas on the DP master to "0".	No updating of the process image
RUN	STOP→RUN	The I-slave sets the input transfer areas on the DP master to "0". After the startup program of the I-slave, the input transfer areas of the DP master are updated via the process image.	Prior to processing of the startup program, the input transfer areas are updated via the process image.

Service & Support



The unmatched complete service for the entire life cycle

For machine constructors, solution providers and plant operators: The service offering from Siemens Industry Automation and Drive Technologies includes comprehensive services for a wide range of different users in all sectors of the manufacturing and process industry.

To accompany our products and systems, we offer integrated and structured services that provide valuable support in every phase of the life cycle of your machine or plant – from planning and implementation through commissioning as far as maintenance and modernization.

Our Service & Support accompanies you worldwide in all matters concerning automation and drive technology from Siemens. We provide direct on-site support in more than 100 countries through all phases of the life cycle of your machines and plants.

You have an experienced team of specialists at your side to provide active support and bundled know-how. Regular training courses and intensive contact among our employees – even across continents – ensure reliable service in the most diverse areas.

Online Support

The comprehensive online information platform supports you in all aspects of our Service & Support at any time and from any location in the world.

You can find Online Support on the Internet at the following address: Internet (http://www.siemens.com/automation/service&support).

Technical Consulting

Support in planning and designing your project: From detailed actual-state analysis, definition of the goal and consultation on product and system questions right through to the creation of the automation solution.

Technical Support

Expert advice on technical questions with a wide range of demand-optimized services for all our products and systems.

You can find Technical Support on the Internet at the following address: Internet (http://www.siemens.com/automation/support-request).

Training

Extend your competitive edge – through practical know-how directly from the manufacturer.

You can find the training courses we offer on the Internet at the following address: Internet (http://www.siemens.com/sitrain).

Engineering Support

Support during project engineering and development with services fine-tuned to your requirements, from configuration through to implementation of an automation project.

Field Service

Our Field Service offers you services for commissioning and maintenance – to ensure that your machines and plants are always available.

Spare parts

In every sector worldwide, plants and systems are required to operate with constantly increasing reliability. We will provide you with the support you need to prevent a standstill from occurring in the first place: with a worldwide network and optimum logistics chains.

Repairs

Downtimes cause problems in the plant as well as unnecessary costs. We can help you to reduce both to a minimum – with our worldwide repair facilities.

Optimization

During the service life of machines and plants, there is often a great potential for increasing productivity or reducing costs.

To help you achieve this potential, we are offering a complete range of optimization services.

Modernization

You can also rely on our support when it comes to modernization – with comprehensive services from the planning phase all the way to commissioning.

Service programs

Our service programs are selected service packages for an automation and drives system or product group. The individual services are coordinated with each other to ensure smooth coverage of the entire life cycle and support optimum use of your products and systems.

The services of a Service Program can be flexibly adapted at any time and used separately.

Examples of service programs:

- Service contracts
- Plant IT Security Services
- Life Cycle Services for Drive Engineering
- SIMATIC PCS 7 Life Cycle Services
- SINUMERIK Manufacturing Excellence
- SIMATIC Remote Support Services

Advantages at a glance:

- Reduced downtimes for increased productivity
- Optimized maintenance costs due to a tailored scope of services
- Costs that can be calculated and therefore planned
- Service reliability due to guaranteed response times and spare part delivery times
- Customer service personnel will be supported and relieved of additional tasks
- Complete service from one source: fewer interfaces and more know-how

Contact

At your service locally, around the globe: your partner for consultation, sales, training, service, support, spare parts... for the entire range of products supplied by Industry Automation and Drive Technologies.

You can find your personal contact in our contacts database at: Internet (http://www.siemens.com/automation/partner).

SIEMENS

SIMATIC

MultiFieldbus

Function Manual

Documentation guide 1

System overview 2

EtherNet/IP 3

Modbus TCP 4

MF Shared Device 5

Firmware update with MFCT 6

01/2022

A5E46329959-AB

Preface

Purpose of the documentation

This function manual provides an overview and a detailed description of the individual MultiFieldbus functions. The function manual supplements the description of the system manuals and product manuals of the MultiFieldbus devices (MF devices).

This function manual includes all the information you need to configure and commission the above-mentioned devices on other fieldbuses (EtherNet/IP and Modbus TCP).

Basic knowledge required

The following knowledge is required in order to understand the manual:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge about the use of Windows-based computers
- Knowledge of
  - PROFINET
  - EtherNet/IP
  - Modbus TCP

Scope of the documentation

This documentation is the basic documentation for MF devices from Siemens. The product documentation is based on the content of this Function Manual.

Conventions

Also observe notes labeled as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product, or on the section of the documentation to which particular attention should be paid.

Recycling and disposal

For environmentally sustainable recycling and disposal of your old equipment, contact a certified electronic waste disposal service and dispose of the equipment according to the applicable regulations in your country.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Table of contents

1 Documentation guide 7

2 System overview 8

2.1 System overview 8

2.2 MultiFieldbus engineering 8

2.3 Detect active fieldbus 9

3 EtherNet/IP 10

3.1 EtherNet/IP functions 10
3.1.1 EtherNet/IP 10

3.2 Integration in the automation system 10
3.2.1 Overview 10
3.2.2 Configuring with MFCT 12
3.2.2.1 Requirements 12
3.2.2.2 Settings 13
3.2.2.3 Assigning network parameters 14
3.2.2.4 Resetting the MF device 15
3.2.2.5 Creating new MultiFieldbus project in MFCT 16
3.2.2.6 Open MultiFieldbus project in MFCT 16
3.2.2.7 Selecting a station 17
3.2.2.8 Configuring modules of a station 19
3.2.2.9 Configuring IO modules of a station 22
3.2.2.10 Parameter assignment of the station 23
3.2.2.11 Transfer the configuration 25
3.2.2.12 Sending user feedback 27
3.2.3 Configuration in the engineering system 27
3.2.3.1 Import EDS station description 27
3.2.3.2 Importing a user-defined type (UDT) 28
3.2.3.3 Configuring the MF device 28
3.2.3.4 I/O data mapping 29
3.2.3.5 Examples of I/O data mapping for coupler 31
3.2.3.5.1 Example of I/O data mapping for I/O data alignment Byte 31
3.2.3.5.2 Example of I/O data mapping for I/O data alignment Word 32
3.2.3.6 Configuring the module from the user program 34
3.2.3.7 Configuration as generic EtherNet/IP module 36

3.3 Diagnostics 37
3.3.1 Reading diagnostics via CIP EtherNet/IP 37
3.3.2 Reading diagnostics with MFCT 39
3.3.3 Reading hardware interrupt via CIP EtherNet/IP 40
3.3.4 PULL/PLUG event EtherNet/IP 42
3.3.5 Reading service data 42

3.4 Supported CIP objects for EtherNet/IP ... 43
3.4.1 Identity Object ... 43
3.4.2 Assembly Object ... 45
3.4.3 Connection Manager Object ... 47
3.4.4 TCP/IP Interface Object ... 48
3.4.5 EtherNet Link Object ... 50
3.4.6 LLDP Management Object ... 55
3.4.7 LLDP Data Table Object ... 56
3.4.8 Param Object ... 58

4 Modbus TCP ... 61

4.1 Modbus TCP functions ... 61
4.1.1 Modbus TCP ... 61
4.2 Integration in the automation system ... 61
4.2.1 Overview ... 61
4.2.2 Configuring with MFCT ... 63
4.2.2.1 Requirements ... 63
4.2.2.2 Settings ... 64
4.2.2.3 Assigning network parameters ... 65
4.2.2.4 Resetting the MF device ... 66
4.2.2.5 Creating new MultiFieldbus project in MFCT ... 67
4.2.2.6 Open MultiFieldbus project in MFCT ... 67
4.2.2.7 Selecting a station ... 68
4.2.2.8 Configuring a station ... 70
4.2.2.9 Parameter assignment of the station ... 73
4.2.2.10 Transfer the configuration ... 74
4.2.2.11 Sending user feedback ... 77
4.2.3 Configuration in the engineering system ... 77
4.2.3.1 Services ... 77
4.2.3.2 Register addresses ... 77
4.2.3.3 Behavior of the inputs and outputs ... 82
4.2.3.4 I/O data mapping ... 82
4.2.3.5 Data record interface ... 83
4.2.3.5.1 Overview ... 83
4.2.3.5.2 User interface ... 84
4.2.3.5.3 Read data record ... 85
4.2.3.5.4 Write data record ... 86
4.2.3.5.5 Example: Read I&M0 data ... 86
4.2.3.5.6 Example: Write I&M1 data ... 87
4.2.3.5.7 Example: Read diagnostics (multiple data packets) ... 88
4.2.3.5.8 Example: Write parameter data record (multiple data packets) ... 89
4.3 Diagnostics ... 91
4.3.1 Reading diagnostics with MFCT ... 91
4.3.2 Reading hardware interrupts via event interface ... 92
4.3.3 PULL/PLUG event modbus TCP ... 93
4.3.4 Reading service data ... 94

5 MF Shared Device ... 95

5.1 Configuration ... 96
5.2 Example ... 98

6 Firmware update with MFCT 100
6.1 Settings 100
6.2 Updating the firmware 101
6.3 Updating firmware in multiple subnets 103
6.4 Activating the firmware 104

Documentation guide

1

Documentation

Various MultiFieldbus devices are available from Siemens. Each of these MultiFieldbus devices has a separate documentation. The MultiFieldbus devices are embedded in systems, e.g. ET 200SP. The documentation for the system consists of the respective system manual, function manuals and manuals.

MultiFielbus devices from Siemens

Detailed information on the MultiFieldbus devices can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109779189).

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- ET 200SP (https://support.automation.siemens.com/WW/view/en/84133942)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109781058)

System overview 2

2.1 System overview

Properties

The following properties are available. You can find out which features the MF Device supports in the respective system and equipment manuals.

- Connection to various fieldbuses as
  - PROFINET IO device
  - EtherNet/IP adapter
  - Modbus TCP server
- MF Shared Device (Page 95)
- All fieldbuses can be operated over the same Ethernet cable.
- Integrated 2-port switch

If you use the EtherNet/IP or Modbus TCP fieldbus protocol, one application relation (AR) is used for each fieldbus protocol.

2.2 MultiFieldbus engineering

MultiFieldbus Configuration Tool (MFCT)

You can create the configuration and parameter assignment of the MultiFieldbus Devices with MFCT. You download the configuration and parameter assignment to the MF Device with MFCT. The configuration and parameter assignment are stored retentively in the MF Device. For structured access to the I/O data with EtherNet/IP, you can export a UDT file (file extension *.l5x).

MFCT is available for download (https://support.industry.siemens.com/cs/ww/en/view/109773881) on the Internet.

NOTE

For commissioning with MFCT, the MF Device must be connected via an Ethernet connection with **100 Mbps full duplex**.

NOTE

Only one instance of MFCT or PRONETA may be active in a network.

If PRONETA and MFCT are simultaneously active in the network, you must deactivate cyclic scanning in PRONETA.

Installation requirements for MFCT

You also need to install the following software for MFCT:

- Microsoft .NET Framework 4.6.1 (Offline Installer) (https://www.microsoft.com/en-US/download/confirmation.aspx?id=49982)
- WinPcap from directory "Misc"
- Microsoft C++ Redistributable:
  - For x86 systems (https://aka.ms/vs/15/release/vc_redist.x86.exe)
  - For x64 systems (https://aka.ms/vs/15/release/vc_redist.x64.exe)

Electronic Data Sheet (EDS)

For integration in EtherNet/IP configuration systems, a generic EDS file according to CIP specification Vol.1 is available for download (https://support.industry.siemens.com/cs/ww/en/ps/27993).

See also

Import EDS station description (Page 27)
Configuring with MFCT (Page 12)

2.3 Detect active fieldbus

For exclusive operation on a fieldbus (not MF Shared Device) you can recognize the active fieldbus by the number of green LEDs on the MF Device.

This requires that there are no errors and that the MF Device is in cyclic data exchange with a controller.

Active fieldbus:	RN/NS	ER/MS	MT/IO
PROFINET	■ Green	□ Off	□ Off
Modbus TCP	■ Green	■ Green	□ Off
EtherNet/IP	■ Green	■ Green	■ Green

EtherNet/IP

3

3.1 EtherNet/IP functions

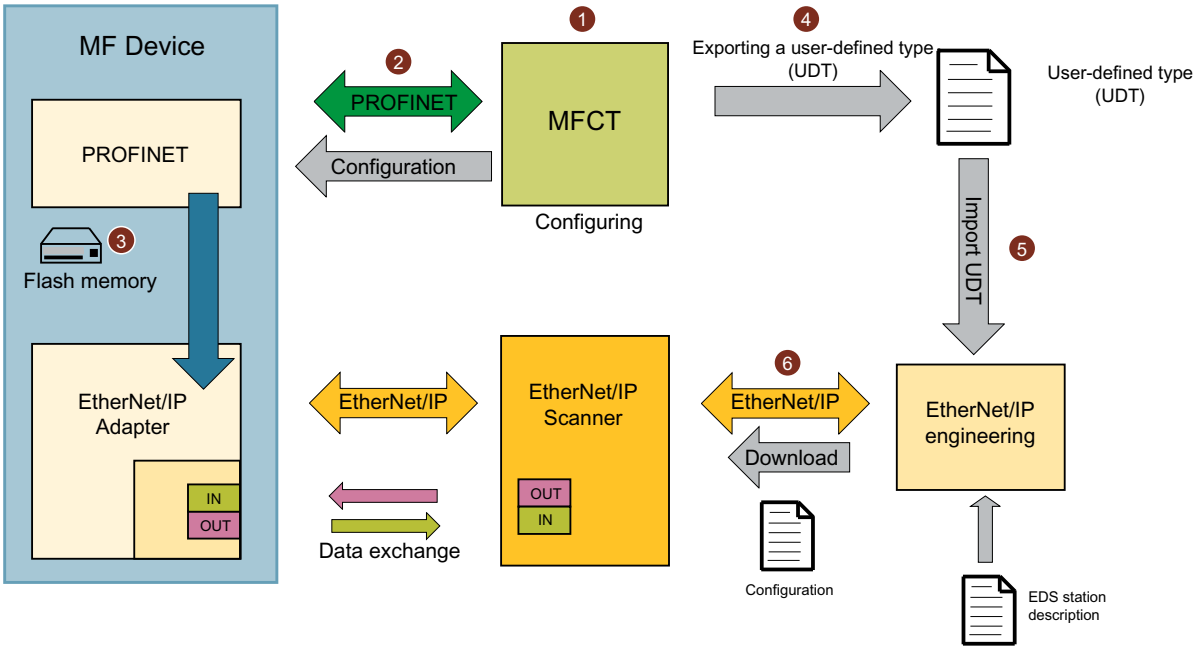
3.1.1 EtherNet/IP

MultiFieldbus supports the following EtherNet/IP functions:

- I/O communication with scanner
- Configuring from the user program
- Read diagnostics (interrupts are not supported)
- Normative CIP objects
- Resetting interface module to factory setting
- Diagnostics bit in data status of cyclic I/O data per submodule

3.2 Integration in the automation system

3.2.1 Overview



In the MultiFieldbus Configuration Tool (MFCT), you configure the MF device and assign an IP address and a device name to the MF device ①. You then download the configuration to the MF device with PROFINET IO mechanisms ②. The configuration is saved on the MF device ③. You generate and export the I/O data mapping of the MF device as user-defined type (UDT) as

I5x file for EtherNet/IP in MFCT ④. You then import the I5x file to your engineering system ⑤. Download the project to the EtherNet/IP scanner with the engineering system ⑥.
Import the generic EDS station description to your engineering system once.

Procedure

For commissioning, follow these steps:

1. Scan the network in MFCT and assign an IP address for the MF device.
2. Configure the MF device.
3. Select EtherNet/IP as fieldbus for the Ethernet interface.
4. Load the MultiFieldbus project to the MF device.
5. Export the I/O data mapping of the MF device as user-defined type (UDT) from MFCT.
6. Import the user-defined type (UDT) to your EtherNet/IP engineering system.
7. Configure the interface module in the EtherNet/IP engineering system.
8. Download the project to the EtherNet/IP scanner.
9. (Optional) Configure the modules from inside the user program.

NOTE
For MF devices, there might be modules displayed in engineering systems starting with slot 1000.
These merely reflect the retentively stored project in the MF device consisting of configuration and parameter assignment.

3.2.2 Configuring with MFCT

3.2.2.1 Requirements

Information on which MFCT version is required for which MF Device can be found in the Equipment Manual of the MF Device.

You can find version information for MFCT on the "About" tab.

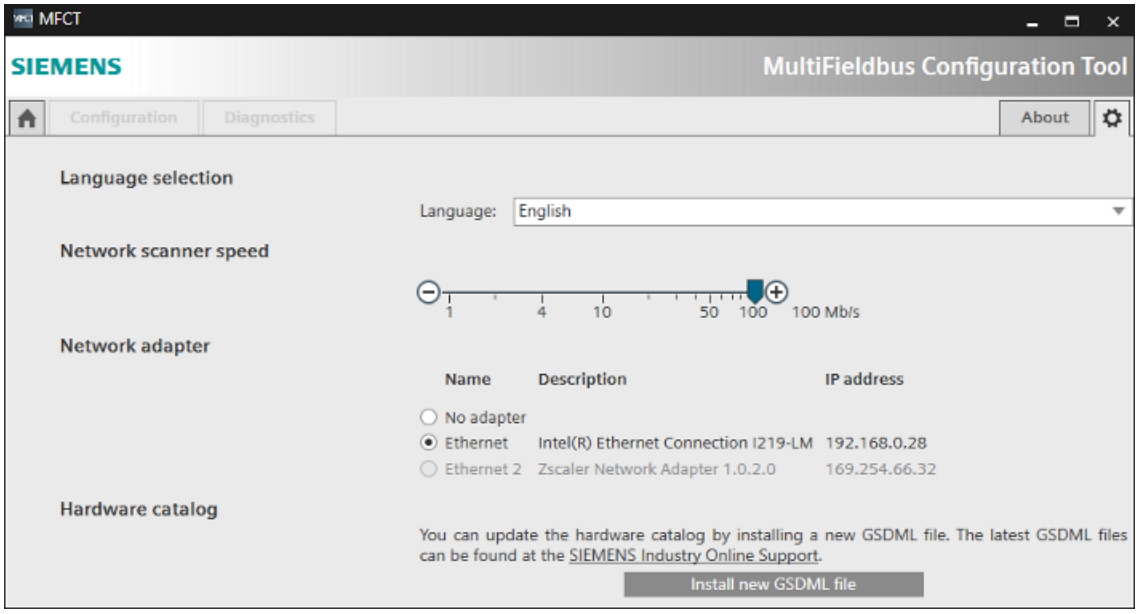


3.2.2.2 Settings

In the "Settings" tab, you can specify basic properties of the MultiFieldbus Configuration Tool:

- Select the user interface language.
- Select the network adapter.

You can also update the GSD file used.



Language selection

Under "Language selection", select the user interface language for the MFCT.

Network scanner speed

Under "Network scanner speed", select the speed of the network scanner.

Network adapter

Under "Network adapter", select the interface you want to use to connect to MF devices.

Hardware catalog

In the "Hardware catalog" section, you can update the GSD module description in the MFCT using the "Install new GSDML file" button.

To do this, proceed as follows:

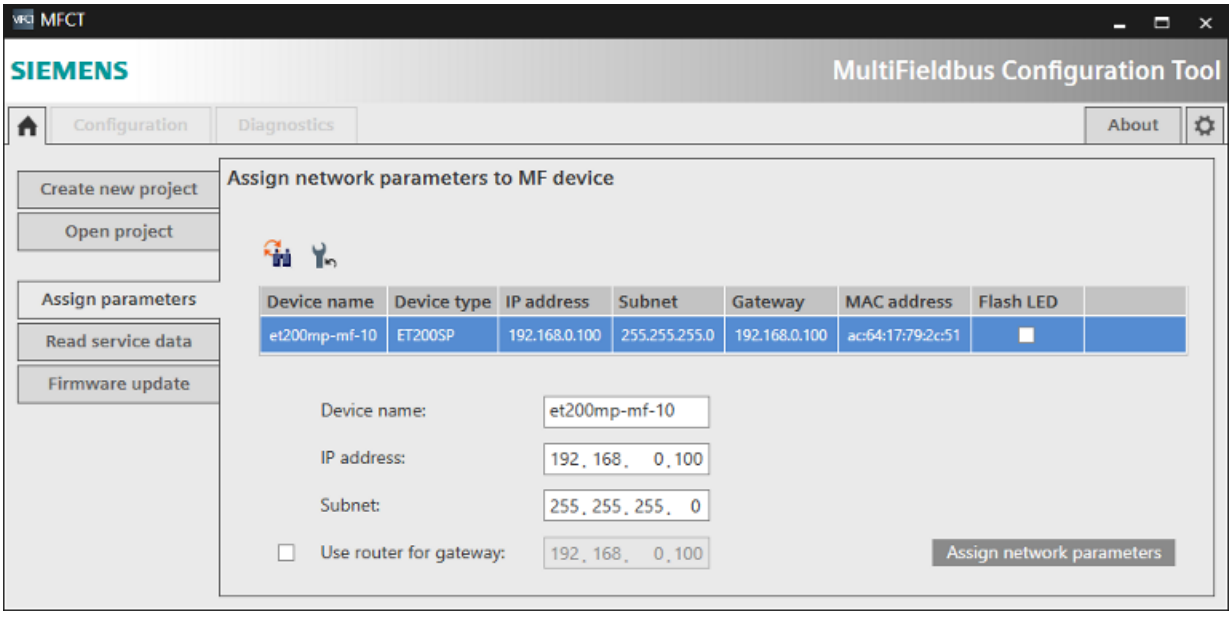
1. Click the link in the text.
2. Download the zipped GSD file and save it locally.
3. Unzip the GSD file.
4. Click "Install new GSDML file" and select the unzipped GSD file.

3.2.2.3 Assigning network parameters

In the "Home" tab, you can assign the network parameters for MF devices under "Assign parameters":

1. Click the "Start scan" button to find MF devices via the preset network interface.
2. Select an MF device.
   (You can make the LEDs of the MF device flash for identification with "Flash LED".)
3. Enter a device name, valid IP address and the subnet mask.
4. If you use a gateway, you can enable the "Use router for gateway" option and enter the router address.
5. Click "Assign network parameters".

The network parameters are assigned.

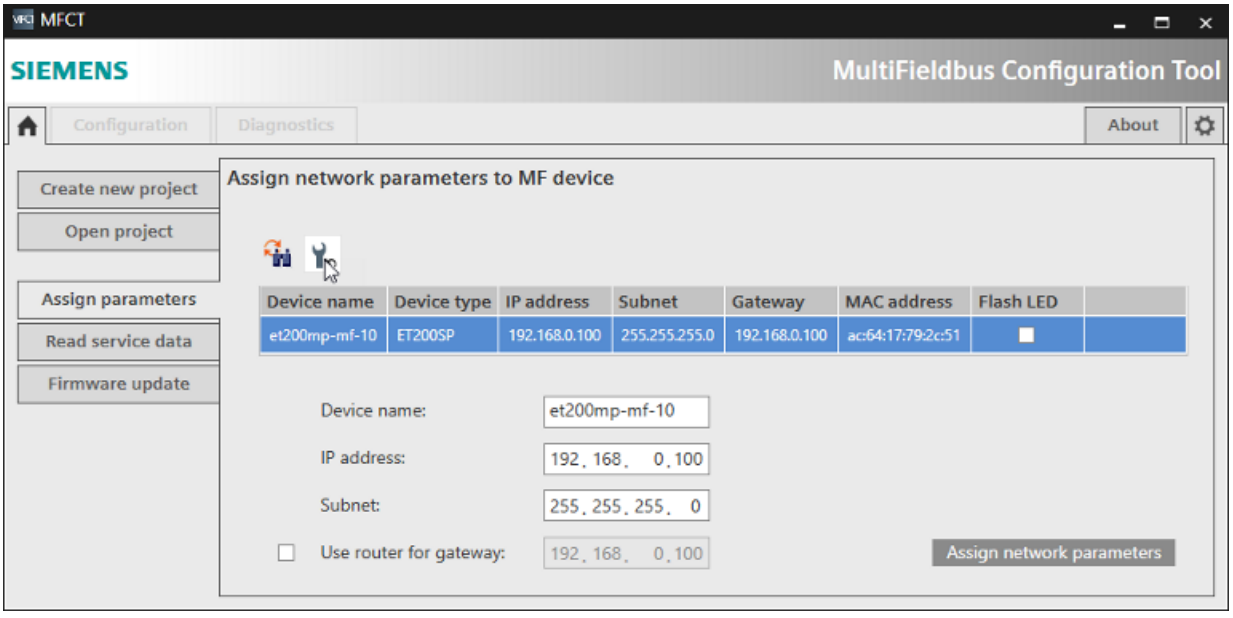


3.2.2.4 Resetting the MF device

In the "Home" tab, you can reset the MF device to the factory settings under "Accessible MF devices":

1. Click the "Start scan" button to find MF devices via the preset network interface.
2. Select an MF device.
3. Click "Reset network parameters".

The network parameters and the MultiFieldbus project are deleted.

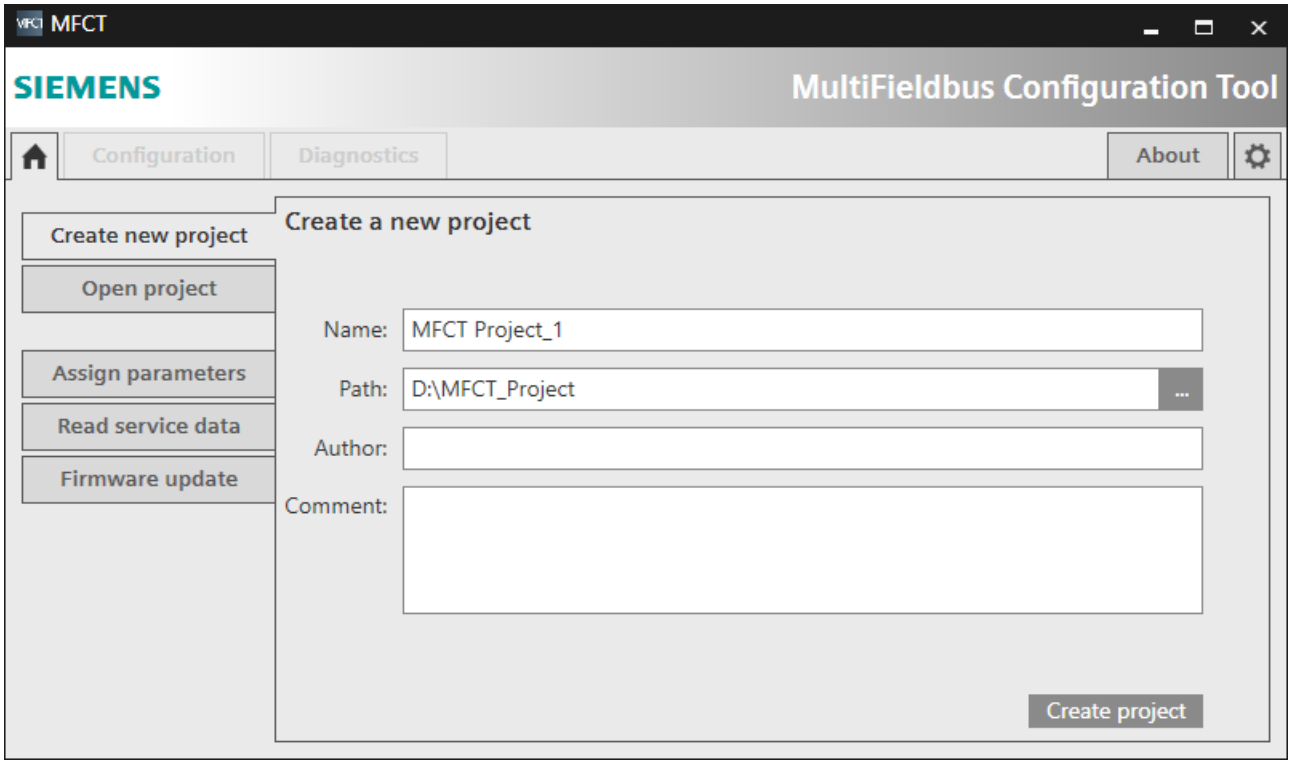


3.2.2.5 Creating new MultiFieldbus project in MFCT

You can create a new MultiFieldbus project in the "Home" tab:

1. Select "Create new project" and enter a name and a path for the new MultiFieldbus project.
   Optionally, you can describe the project in more detail by entering the author and comments.
2. Click "Create project".

The MultiFieldbus project is created as a file with the extension ".mfp1". The MFCT then goes to the next step in the "Configuration" tab.



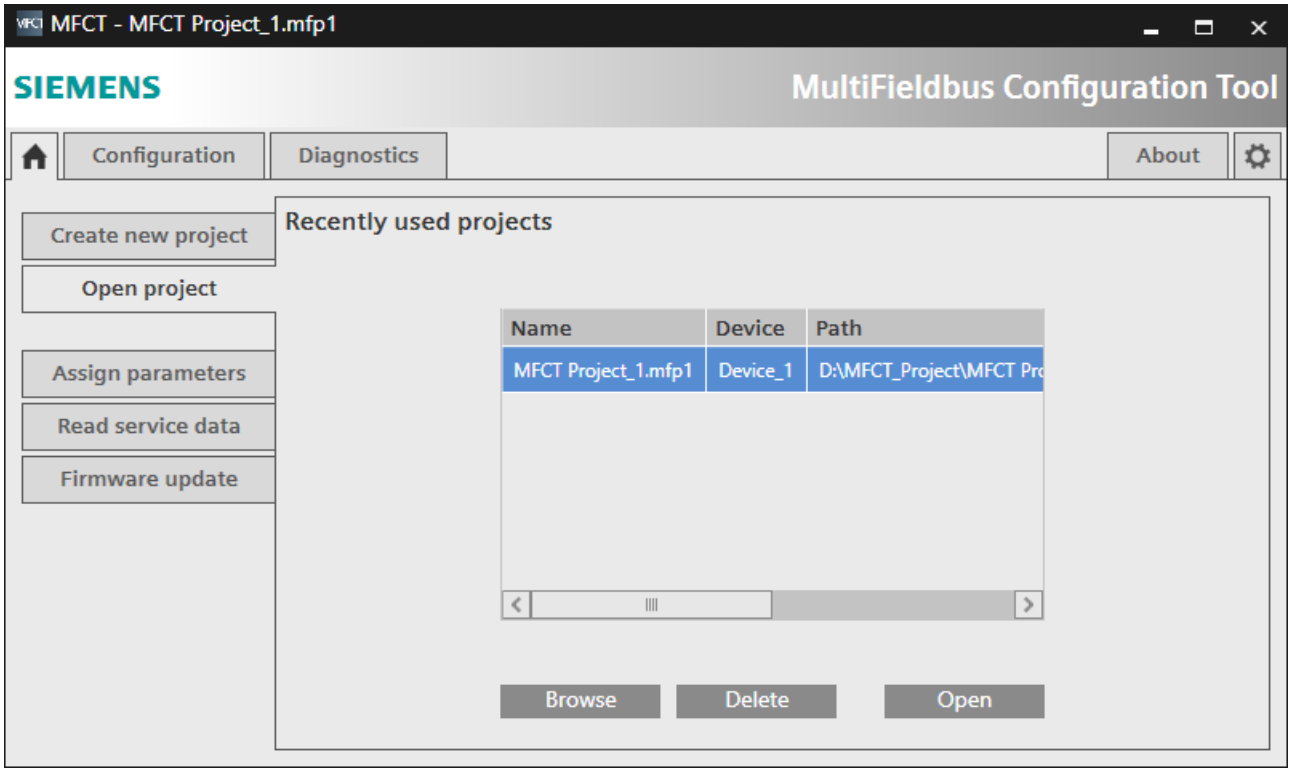
3.2.2.6 Open MultiFieldbus project in MFCT

You can open an existing MultiFieldbus project in the "Home" tab:

1. Select "Open project".
   - Under "Recently Used Projects", you can select a recently edited project and read it in directly by double-clicking it or using the "Open" button.
   - Alternatively, you can use the "Browse" button to open a project file.

The project is opened and the MFCT switches to the "Configuration" tab.

NOTE
The "Delete" button allows you to delete an existing project from the "Recently Used Projects" list. The project file itself is not deleted by this action.



3.2.2.7 Selecting a station

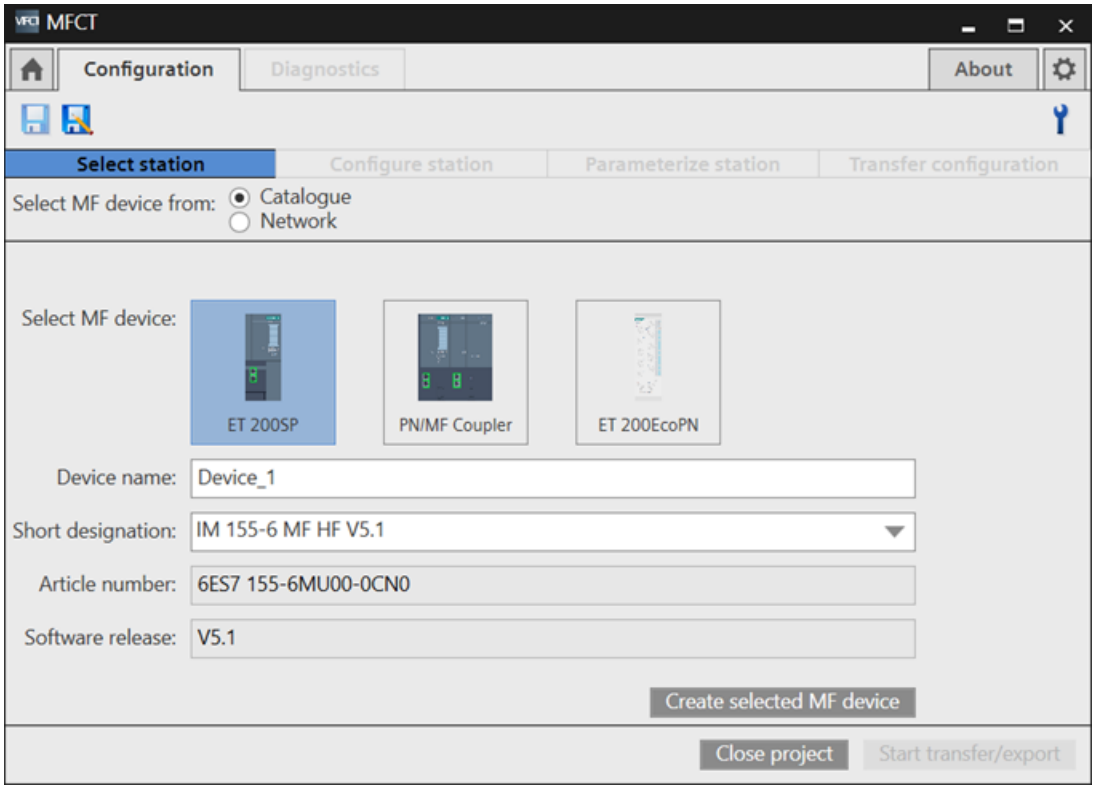
You can create the configuration of the MF device in two ways:

- From the catalog if the real MF station is not available.
- From the network if the MF station is available online.

Selecting MF device from the catalog

1. Select the "Catalogue" option under "Select MF device from".
2. Under "Select MF device", select the desired MF device, e.g. ET 200SP.
3. Assign a name for the MF device under "Device name".
4. Select the desired interface module under "Short designation".
5. Click on the "Create Selected MF Device" button.

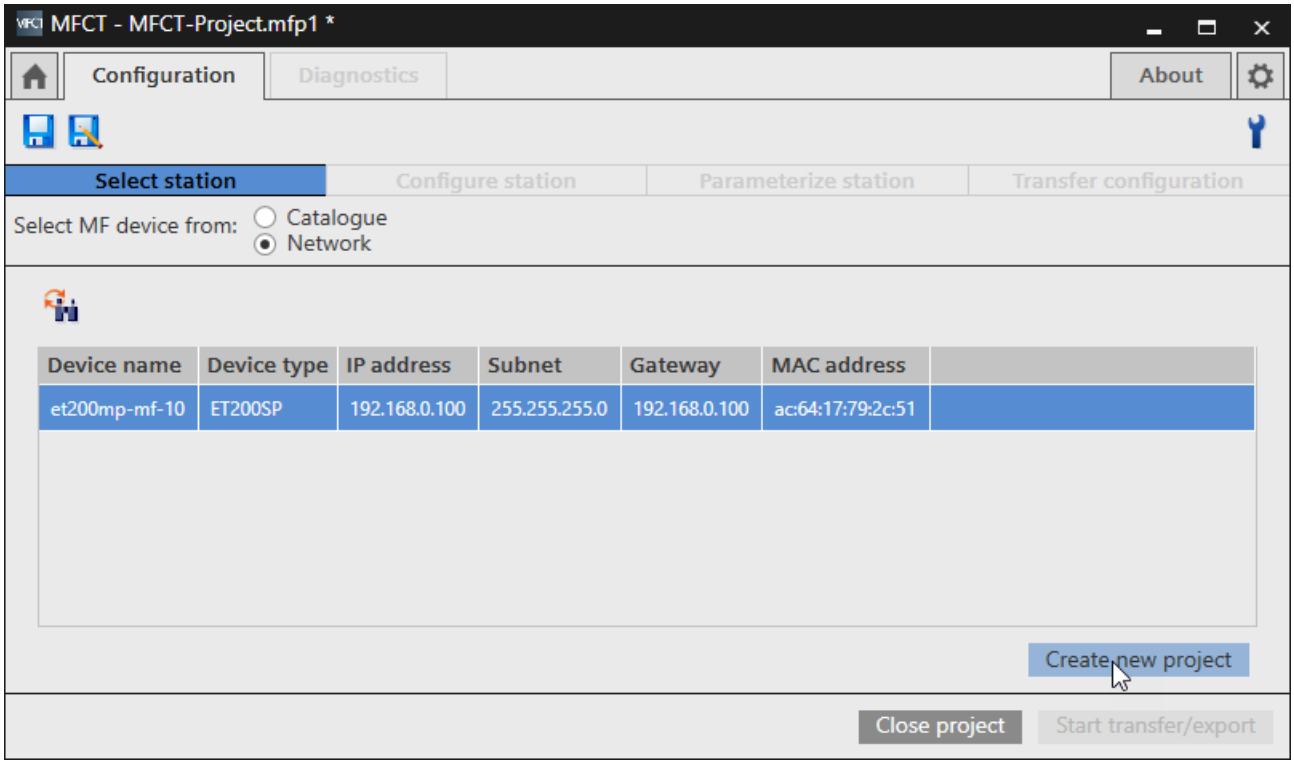
The MFCT automatically goes to the next step, "Configure Station".



Selecting MF device from the network and loading the configuration

1. Ensure that the network interface selected in the "Settings" tab is connected to the desired MF device.
2. Select the "Network" option under "Select MF device from".
3. Click "Start scan".
4. Select the desired MF device from the list. Devices without MultiFieldbus support cannot be selected and are grayed out.
5. Click "Create new project".

The current configuration is read out from the MF device and added to the MultiFieldbus project. MFCT then goes to the next step "Configure Station" for review and editing.



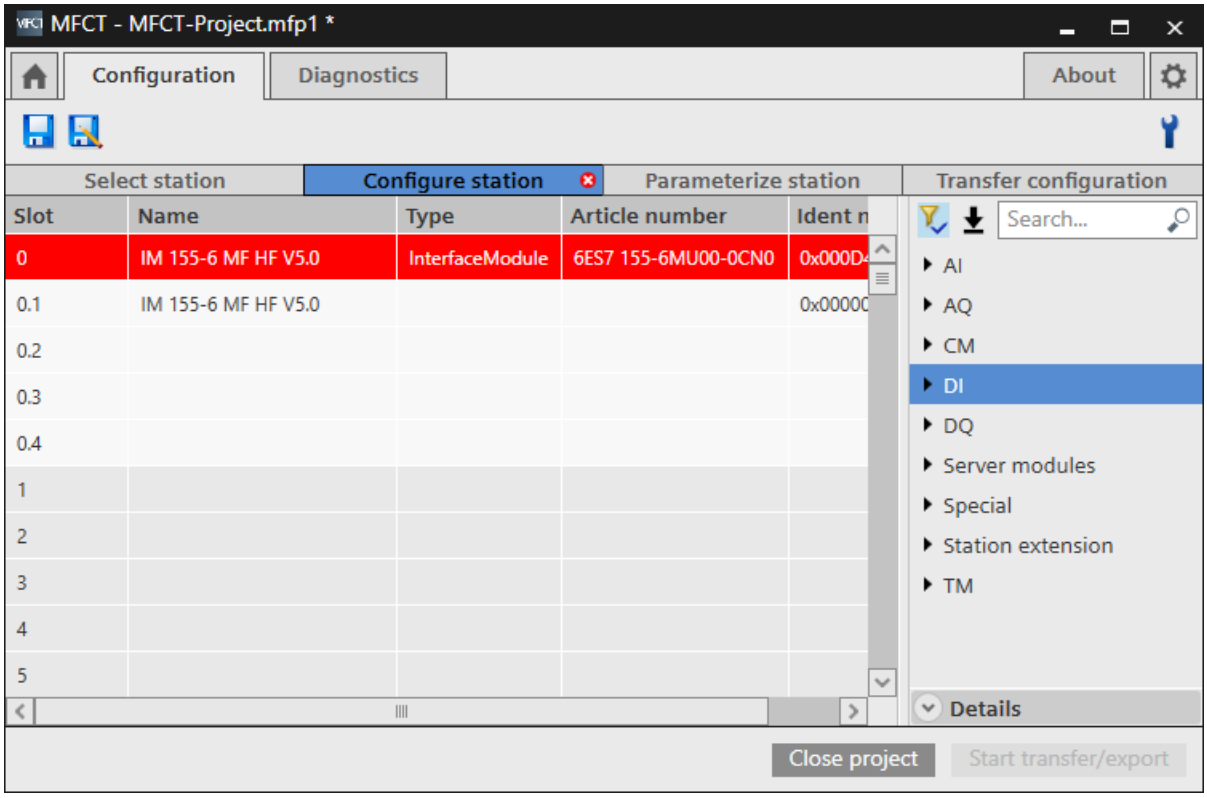
3.2.2.8 Configuring modules of a station

Under "Configure Station", assemble the station with modules and submodules from the hardware catalog based on the GSDML.

The composition of the station is shown as a list on the left, sorted in ascending slot order. The modules and submodules of the hardware catalog based on the installed GSDML are shown on the right.

Additional information on the selected module and potential application at the fieldbuses is shown below the hardware catalog in the "Details" area.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

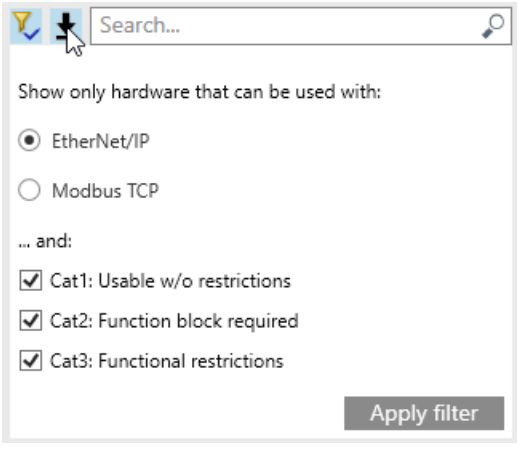


Filter function

You use the filter function to restrict the hardware catalog depending on the fieldbus and the category.

To activate the filter function, follow these steps:

1. Expand the list with the filter criteria.



2. Select the desired fieldbus.

3. Select the desired categories.
4. Activate the filter function using the "Apply filter" button.

To deactivate the filter function, follow these steps:

1. Click the filter icon.



Selecting modules

1. Select the module in the desired version and operating mode from the catalog for each slot and drag it onto the slot.

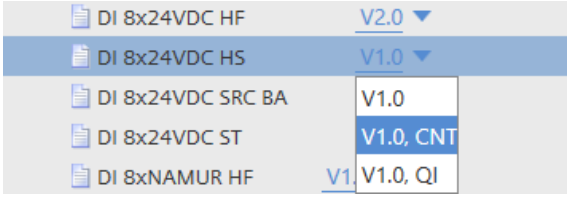
NOTE
The possible slots for the selected module are highlighted in green.

2. Finally, add a server module.

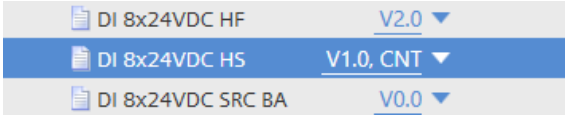
NOTE
The MF device is highlighted in red until you have added the server module.

Selecting submodules

1. Select one of the available submodules from the drop-down list of the module in the hardware catalog.



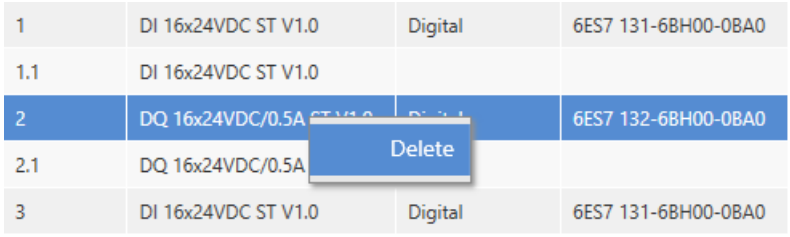
2. Select the submodule and drag it onto a slot.



NOTE
The possible submodule slots are highlighted in green.

Deleting modules/submodules

1. Select the module/submodule to be deleted.
2. Click "Delete" in the shortcut menu.

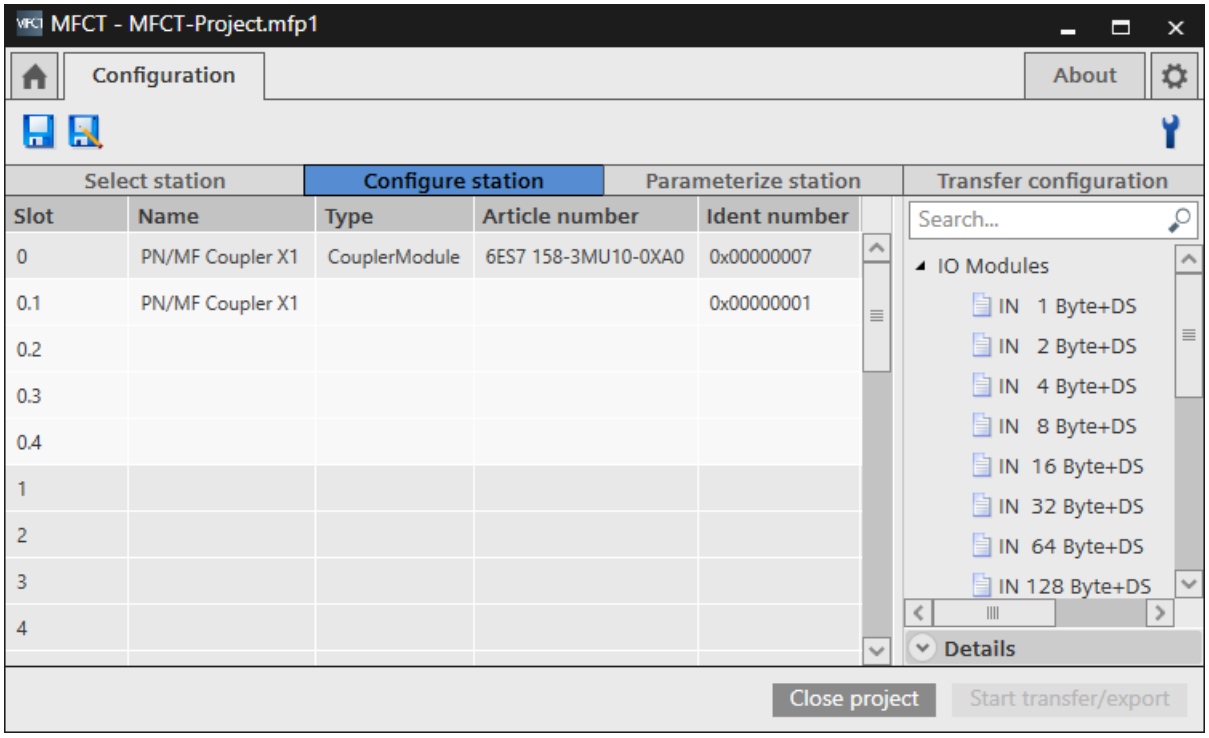


3.2.2.9 Configuring IO modules of a station

Under "Configure Station", assemble the station with IO modules from the hardware catalog based on the GSDML.

The composition of the station is shown as a list on the left, sorted in ascending slot order. The IO modules of the hardware catalog based on the installed GSDML are shown on the right.

Additional information on the selected IO module is shown below the hardware catalog in the "Details" area.



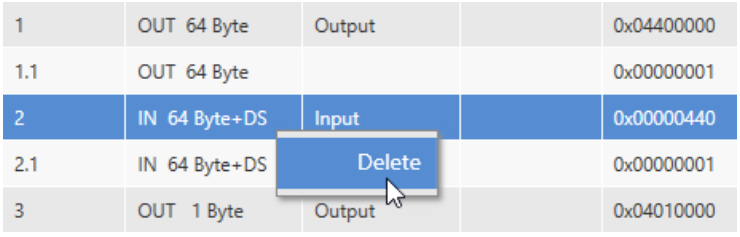
Selecting IO modules

1. Select the IO module from the hardware catalog for each slot and drag it onto the slot.

NOTE
The possible slots for the selected IO module are highlighted in green.

Deleting IO modules

1. Select the IO module to be deleted.
2. Click "Delete" in the shortcut menu.



Example

Assuming that you want to read 128 bytes and write 64 bytes on network side X1 from network side X2, you need to configure the following for network side X1 in MFCT:

1	OUT 64 Byte	Output		0x04400000
1.1	OUT 64 Byte			0x00000001
2	IN 128 Byte+DS	Input		0x00000480
2.1	IN 128 Byte+DS			0x00000001

Information on how to configure network side X2 with STEP 7 (TIA Portal) with GSD file is available in the "PN/MF Coupler (https://support.industry.siemens.com/cs/ww/en/view/109781406)" hardware installation and operating manual.

3.2.2.10 Parameter assignment of the station

Under "Assign Station Parameters", set the parameters of the previously configured station.

The composition of the station is shown as a list on the left, sorted in ascending slot order. The parameters for the MF device and the modules/submodules are shown on the right.

For MF devices that support the "MF Shared Device" function, you can configure various fieldbuses for the MF device and for each module.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

Procedure

1. Select the MF device on slot 0.
2. If the MF device supports the "MF Shared Device" function and you want to configure different fieldbuses for the MF device and the modules, activate the "MF Shared Device" parameter on the right under "Multi fieldbus parameters".



Multi fieldbus features	
Parameter	**Value**
MF Shared Device	☑

3. Select the desired fieldbus for the MF device under "Multi fieldbus connection".
4. Use the "I/O data alignment" parameter to select a supported format, "Byte" or "Word" for I/O data mapping (Page 29).
5. Under "MultiFieldbus modbus TCP", you can set for each modbus TCP connection separately the hold time for the connection and the time for "Hold time after connection reset" from 1 to 30,000 ms.

   This parameter is not relevant for EtherNet/IP.
6. Assign parameters for the remaining modules and submodules by selecting the slot and setting the parameter values on the right side.
7. When you have activated the "MF Shared Device" parameter, you can select a fieldbus for each module under "MultiFieldbus connection".

NOTE

Observe restrictions in the manuals of the MF device used.

Slot	Name	Type	Article number	Fieldbus connection
0	IM 155-6 MF HF V5.2	InterfaceModule	6ES7 155-6MU00-0CN0	PROFINET
0.1	IM 155-6 MF HF V5.2			
0.1				
0.2				
0.3				
1	DI 16x24VDC ST V0.0	Digital	6ES7 131-6BH01-0BA0	EtherNet/IP #0 (0x301, 0x300)
2	DQ 16x24VDC/0.5A BA V0.0	Digital	6ES7 132-6BH00-0AA0	ModbusTCP #0 (0x000, 0x2D0)
3	F-AI 4xU 0..10V HF, XP	FAnalog	6ES7 136-6AB00-0CA1	PROFINET
4	F-DQ 8x24VDC/0.5A PP HF, BP	FDigital	6ES7 136-6DC00-0CA0	PROFINET
5	Server module V1.2 (0 bytes)	ServerModule	6ES7 193-6PA00-0AA0	PROFINET

NOTE

A parameterization error can be displayed during reconfiguration of PROFINET to EtherNet/IP or Modbus TCP in connection with changing the BusAdapter type. You can only remedy the parameterization error with a reset to factory settings (Page 15) and reconfiguration with MFCT.

3.2.2.11 Transfer the configuration

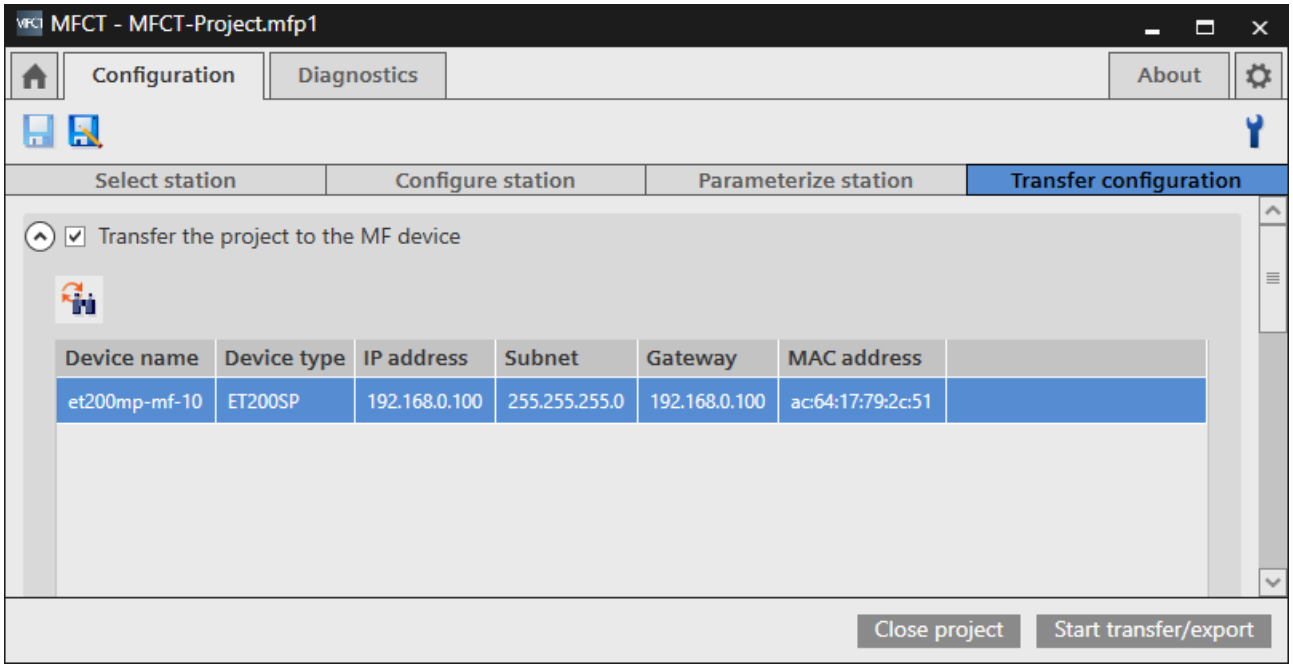
The "Transfer configuration" area offers you the following options:

- Transfer the project to the MF device
- Export the configuration for use in other engineering tools.

Transferring the project to the MF device

To transfer the MF project to the MF device, follow these steps:

1. Select the "Transfer the project to the MF device" check box.
2. Click the "Start scan" button to search via the preset network interface for MF devices for the project download. Devices without MultiFeldbus support cannot be selected and are grayed out.
3. Select an MF device and start the download to the MF device using the "Start transfer/export" button.

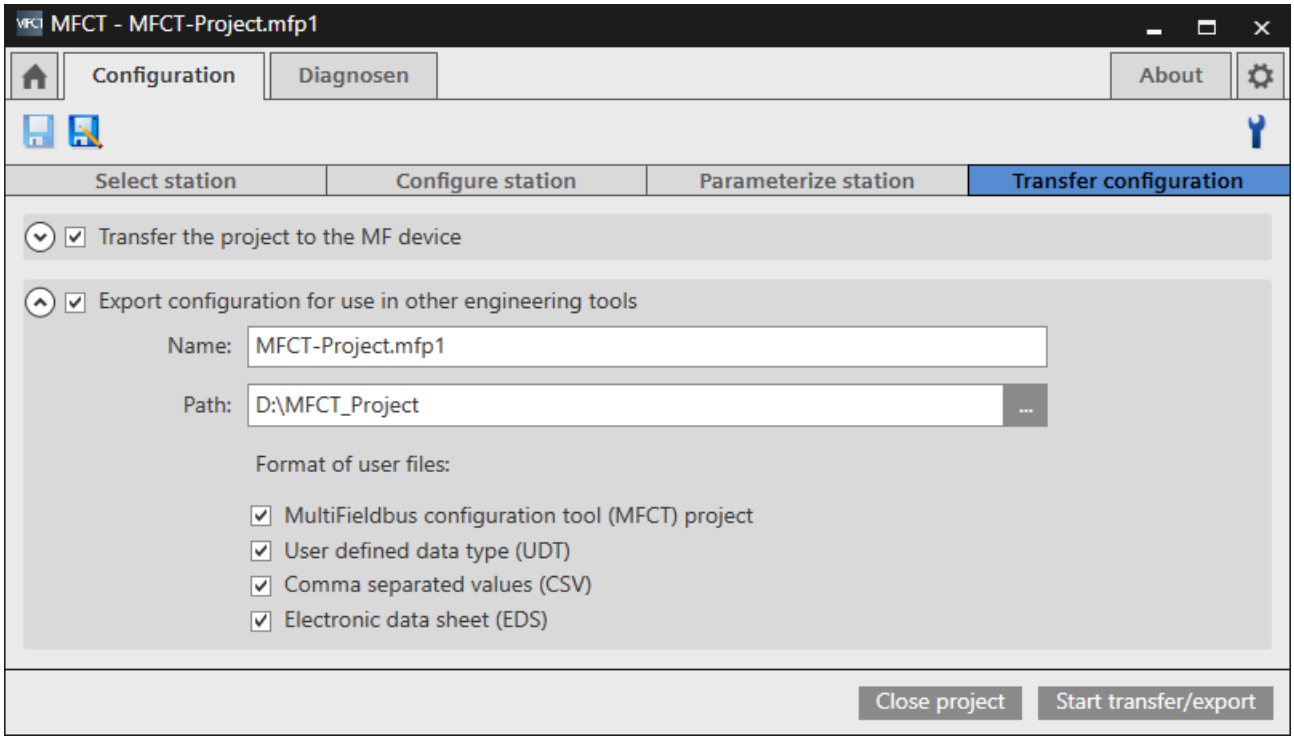


Fault rectification of the timeout on transfer to the MF device

- Check the accessibility of the MF device via the network interface selected in MFCT.
- Disconnect the connection of the MF device to PROFINET IO controllers.
- If you have selected the "Use router for gateway" option in the network parameters, check the network parameters of the device.

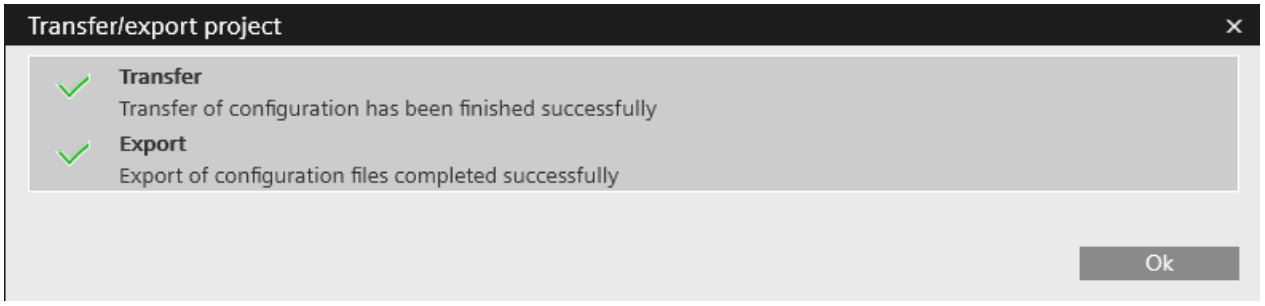
Export of configuration

1. Select the "Export configuration for use in other engineering tools" check box.
2. Assign a name and a path for the export
3. Select the file formats to be exported:
   - MultiFieldbus Configuration Tool (MFCT) project
   - User Defined Data Type (UDT) (as l5x file)
   - Comma Separated Values (CSV)
   - Electronic Data Sheet (EDS)
4. Start the export using the "Start transfer/export" button.



Transfer/export status

The progress and result of the file export and project download are each displayed. The fieldbus activated in the MF device as well as any differences between the configured and real hardware are also displayed.



3.2.2.12 Sending user feedback

You have the option of sending us feedback on MFCT in the "About" tab:

1. Click on the "Send feedback" button.
   MFCT collects diagnostics data and attaches it to the open email.
2. Enter your feedback on MFCT in the email.
3. Send the email.



3.2.3 Configuration in the engineering system

3.2.3.1 Import EDS station description

To import the EDS station description into the engineering system, proceed as described in the documentation of the engineering system.

If the EDS station description cannot be imported, configure a generic EtherNet/IP module (Page 36).

3.2.3.2 Importing a user-defined type (UDT)

To import the user-defined type (UDT) as an l5x file into the engineering system, proceed as described in the documentation of the engineering system.

3.2.3.3 Configuring the MF device

To configure the MF device, follow these steps:

1. Create a new module under "Ethernet" with the "New module" shortcut menu.
2. Select the module type from the catalog and click "Create".
3. Assign a name and IP address under "General".
4. Click "Change" and adjust the input and output sizes to the station configuration.

NOTE

Because there are engineering systems that can only manage one EDS station description per device type, the maximum possible input and output sizes for the device type are modeled in the EDS station description.
For the specific station configuration, you can reduce the input and output sizes of a device instance to the byte length described in the User Defined Type (UDT) in order to optimize the bandwidth needed in the network.

Some MF devices support advanced IP settings. These settings are only possible before the implied communication with the controller. With this setting, the gateway IP address does not have to match the IP address of the MF device.

The following figure shows an example of the setting options.

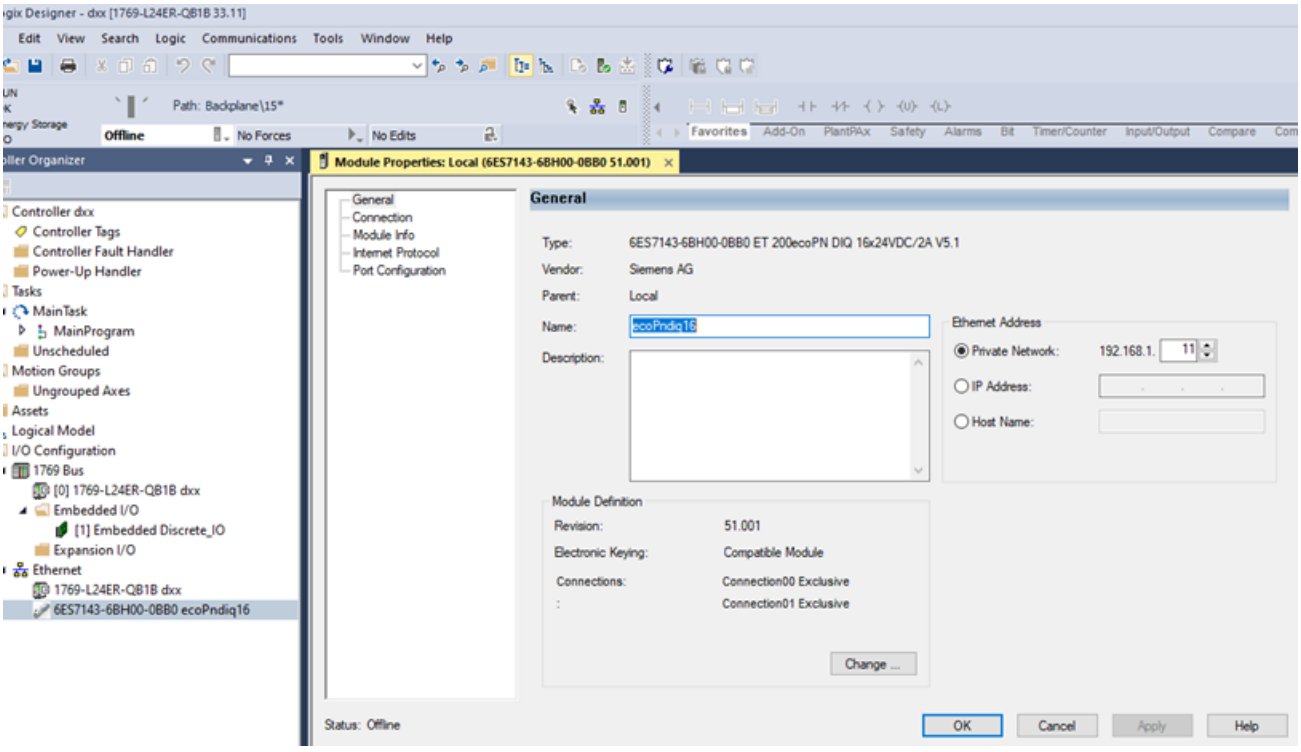


Figure 3-539 Possible IP settings

3.2.3.4 I/O data mapping

I/O data mapping

During parameter assignment of the MF Device (Page 23), you can choose between two formats for the I/O data mapping:

- With the "Byte" format, the input or output data of the modules of an I/O connection are lined up by increasing slot address (Slot.Subslot).
- With the "Word" format, the input or output data of the modules of an I/O connection are lined up by increasing slot address (Slot.Subslot). If the submodule has an odd data length, a fill byte (content 0x00) is inserted after the submodule. This aligns the following data status bytes (IDS, ODS) to word limits. A padding byte (content 0x00) is also inserted after the data status byte (IDS, ODS). Subsequent submodules will then also start at an even byte offset.

The image of the outputs contains only the output data (with padding bytes if necessary), while the input image also supplies additional status bytes together with the input data (with padding bytes if necessary).

An Output Data Status Byte (ODS) is available for each output submodule in the image of the inputs.

There is an Input Data Status Byte (IDS) for each input submodule that follows the respective input data of the submodule in the input image.

Submodules with a data length of 0 for input and output data are treated as input submodules. Only an Input Data Status Byte (IDS) is entered in the input image.

NOTE
You can find the I/O data mapping for your configuration in the exported CSV file (Page 25).

NOTE
For information about data mapping, see the system and equipment manuals.

I/O data status

The following table shows the coding of the status bytes for IDS and ODS:

Field	Bit number	Bit mask	Default	Bit value = '0'	Bit value = '1'
IOValid	7	0x80	0	I/O data invalid	I/O data valid*
Problem	6	0x40	0	Initial status	Module problem: • Module not plugged • Incorrect module plugged • Module with incorrect parameter assignment • I/O data temporarily invalid after station startup
NoCoupling	5	0x20	0	Initial status	No I/O data from coupling partner (MSO Local or PN/MF Coupler)
Reserved	4...2	0x1E	000	-	
ProcessEvent	1	0x02	0	No process event	Process event available
Diagnosis	0	0x01	0	No diagnostics	Diagnostics available

* With the PN/MF Coupler, output data is always displayed as valid (ODS = 0x80).

NOTE
The following applies to the PN/MF coupler:
The input data of the data record modules are always valid (IDS = 0x80) and their content indicates the availability of the data record coupling.
If the PROFINET communication of coupled modules fails on the X2 interface, EtherNet/IP input data is reset to zero and the IDS data status is set to invalid.

NOTE
For MSI and MSO submodules, the IDS.Diagnosis bit is 0. Comparable to the diagnostic interrupt of PROFINET, the diagnostics for MSI and MSO are only signaled in the IDS.Diagnosis bit for the default submodule (subslot = 1).

3.2.3.5 Examples of I/O data mapping for coupler

Example of I/O data mapping for I/O data alignment Byte

Configuration example

The example uses the following IO modules:

Slot	Module/IO module
0	PN/MF Coupler X1
1	OUT 2 Byte
2	IN 1 Byte+DS
3	OUT 2 Byte
4	OUT 1 Byte
5	IN 2 Byte+DS
6	PROFIsafe IN/OUT 6 Byte / 12 Byte

Input buffer

The following table shows the input buffer for the example configuration for the I/O data alignment Byte:

Slot	Name*	Data type	Byte offset	Description
0	Slot0_1_Id_0_IDS	Byte	0	Input Data State for the PN/MF Coupler
2	Slot2_1_Id_0_Inputs	Byte	1	IN 1 Byte+DS
	Slot2_1_Id_1_IDS	Byte	2	Input Data State for IN 1 Byte+DS
5	Slot5_1_Id_0_Inputs	Byte	3	IN 2 Byte+DS
	Slot5_1_Id_1_Inputs	Byte	4	
	Slot5_1_Id_2_IDS	Byte	5	Input Data State for IN 2 Byte+DS
6	Slot6_1_Id_0_Inputs	Byte	7	PROFIsafe IN/OUT 6 Byte / 12 Byte
	Slot6_1_Id_1_Inputs	Byte	8	
	Slot6_1_Id_2_Inputs	Byte	9	
	Slot6_1_Id_3_Inputs	Byte	10	
	Slot6_1_Id_4_Inputs	Byte	11	
	Slot6_1_Id_5_Inputs	Byte	12	
	Slot6_1_Id_6_IDS	Byte	13	Input Data State for PROFIsafe IN/OUT 6 Byte / 12 Byte
1	Slot1_1_Id_0_ODS	Byte	14	Output Data State for OUT 2 Byte
3	Slot3_1_Id_0_ODS	Byte	15	Output Data State for OUT 2 Byte
4	Slot4_1_Id_0_ODS	Byte	16	Output Data State for OUT 1 Byte
6	Slot6_1_Id_0_ODS	Byte	17	Output Data State for PROFIsafe IN/OUT 6 Byte / 12 Byte

The sum of the input data is 18 bytes.

Output buffer

The following table shows the output buffer for the example configuration for the I/O data alignment Byte:

Slot	Name*	Data type	Byte offset	Description
1	Slot1_1_Id_0_Outputs	Byte	0	OUT 2 Byte
	Slot1_1_Id_1_Outputs	Byte	1	
3	Slot3_1_Id_0_Outputs	Byte	2	OUT 2 Byte
	Slot3_1_Id_1_Outputs	Byte	3	
4	Slot4_1_Id_0_Outputs	Byte	4	OUT 1 Byte
	Slot6_1_Id_0_Outputs	Byte	5	PROFIsafe IN/OUT 6 Byte / 12 Byte
	Slot6_1_Id_1_Outputs	Byte	6	
	Slot6_1_Id_2_Outputs	Byte	7	
	Slot6_1_Id_3_Outputs	Byte	8	
	Slot6_1_Id_4_Outputs	Byte	9	
	Slot6_1_Id_5_Outputs	Byte	10	
	Slot6_1_Id_6_Outputs	Byte	11	
	Slot6_1_Id_7_Outputs	Byte	12	
	Slot6_1_Id_8_Outputs	Byte	13	
	Slot6_1_Id_9_Outputs	Byte	14	
	Slot6_1_Id_10_Outputs	Byte	15	
	Slot6_1_Id_11_Outputs	Byte	16	
-	-	Byte	17	Reserved

* The name is formed according to the following scheme: Slot<Slot#>_<Subslot#>_Id_<Id#>_<DataItem-TextId>

The sum of the output data is 18 bytes.

Example of I/O data mapping for I/O data alignment Word

Configuration example

The example uses the following IO modules:

Slot	Module/IO module
0	PN/MF Coupler X1
1	OUT 2 Byte
2	IN 1 Byte+DS
3	OUT 2 Byte
4	OUT 1 Byte
5	IN 2 Byte+DS
6	PROFIsafe IN/OUT 6 Byte / 12 Byte

Input buffer

The following table shows the input buffer for the example configuration for the I/O data alignment Word:

Slot	Name*	Data type	Byte offset	Description
0	Slot0_1_Id_0_IDS	Byte	0	Input Data State for the PN/MF Coupler
	Slot0_1_Id_1_Padding	Byte	1	*Padding byte*
2	Slot2_1_Id_0_Inputs	Byte	2	IN 1 Byte+DS
	Slot2_1_Id_1_Padding	Byte	3	*Padding byte*
	Slot2_1_Id_2_IDS	Byte	4	Input Data State for IN 1 Byte+DS
	Slot2_1_Id_3_Padding	Byte	5	*Padding byte*
5	Slot5_1_Id_0_Inputs	Byte	6	IN 2 Byte+DS
	Slot5_1_Id_1_Inputs	Byte	7	
	Slot5_1_Id_2_IDS	Byte	8	Input Data State for IN 2 Byte+DS
	Slot5_1_Id_3_Padding	Byte	9	*Padding byte*
6	Slot6_1_Id_0_Inputs	Byte	10	PROFIsafe IN/OUT 6 Byte / 12 Byte
	Slot6_1_Id_1_Inputs	Byte	11	
	Slot6_1_Id_2_Inputs	Byte	12	
	Slot6_1_Id_3_Inputs	Byte	13	
	Slot6_1_Id_4_Inputs	Byte	14	
	Slot6_1_Id_5_Inputs	Byte	15	
	Slot6_1_Id_6_IDS	Byte	16	Input Data State for PROFIsafe IN/OUT 6 Byte / 12 Byte
	Slot6_1_Id_7_Padding	Byte	17	*Padding byte*
1	Slot1_1_Id_0_ODS	Byte	18	Output Data State for OUT 2 Byte
	Slot1_1_Id_1_Padding	Byte	19	*Padding byte*
3	Slot3_1_Id_0_ODS	Byte	20	Output Data State for OUT 2 Byte
	Slot3_1_Id_1_Padding	Byte	21	*Padding byte*
4	Slot4_1_Id_0_ODS	Byte	22	Output Data State for OUT 1 Byte
	Slot4_1_Id_1_Padding	Byte	23	*Padding byte*
6	Slot6_1_Id_8_ODS	Byte	24	Output Data State for PROFIsafe IN/OUT 6 Byte / 12 Byte
	Slot6_1_Id_9_Padding	Byte	25	*Padding byte*

The sum of the input data is 26 bytes.

Output buffer

The following table shows the output buffer for the example configuration for the I/O data alignment Word:

Slot	Name*	Data type	Byte offset	Description
1	Slot1_1_Id_0_Outputs	Byte	0	OUT 2 Byte
	Slot1_1_Id_1_Outputs	Byte	1	
3	Slot3_1_Id_0_Outputs	Byte	2	OUT 2 Byte
	Slot3_1_Id_1_Outputs	Byte	3	

* The name is formed according to the following scheme: Slot<Slot#>_<Subslot#>_Id_<Id#>_<DataItem-TextId>

Slot	Name*	Data type	Byte offset	Description
4	Slot4_1_Id_0_Outputs	Byte	4	OUT 1 Byte
	Slot4_1_Id_1_Padding	Byte	5	*Padding byte*
6	Slot6_1_Id_0_Outputs	Byte	6	PROFIsafe IN/OUT 6 Byte / 12 Byte
	Slot6_1_Id_1_Outputs	Byte	7	
	Slot6_1_Id_2_Outputs	Byte	8	
	Slot6_1_Id_3_Outputs	Byte	9	
	Slot6_1_Id_4_Outputs	Byte	10	
	Slot6_1_Id_5_Outputs	Byte	11	
	Slot6_1_Id_6_Outputs	Byte	12	
	Slot6_1_Id_7_Outputs	Byte	13	
	Slot6_1_Id_8_Outputs	Byte	14	
	Slot6_1_Id_9_Outputs	Byte	15	
	Slot6_1_Id_10_Outputs	Byte	16	
	Slot6_1_Id_11_Outputs	Byte	17	

* The name is formed according to the following scheme: Slot<Slot#>_<Subslot#>_Id_<Id#>_<DataItem-TextId>

The sum of the output data is 18 bytes.

3.2.3.6 Configuring the module from the user program

Module-specific data records can be read/written as explicit messages from the user program. You can find information on the structure of the data records, for example, in the manual for the respective module.

Message Type	CIP Generic
Service Code	0x32 = ReadRecord 0x33 = WriteRecord
Class	0x66 (param object)
Instance ID	Slot/subslot is coded in the instance ID: Slot number x 256 + Subslot number (access to subslots of the interface module [1, 0x8000, 0x8001, 0x8002] with subslot number [1...4])
Instance Attribute	Record index (see table below)
Source	Param Object Request (length and parameter data record) (Page 58)
Destination	Param Object Response (length and parameter data record) (Page 58)

Table 3-64 Record index

Record type		Record index range	Access via CIP Message
User-specific records		0x0000...0x7FFF	Read/write
Normative PROFINET records		0x8000...0xAFF0	Read-only
	I&M1...3	0xAFF1...0xAFF3	Read/write
		0xAFF4...0xFFFF	Read-only

Example

The following example shows how you read 6 bytes from slot 3 with parameter data record 128.

Table 3-65 CIP Request:

Field	Value	Description
Message Type	CIP Generic	
Service Code	0x32	Read Record
Class	0x66	Param Object
Instance ID	0x301	Slot 3 and Subslot 1
Instance Attribute	128	Record Index
Source Length	4	CIP Request Length
Source Element	0x00, 0x00, 0x00, 0x06	Record Request Length

Table 3-66 CIP Response:

Field	Value	Description
Destination Element	0x00, 0x00, 0x00, 0x06	Record Response Length
	0x01, 0x02, 0x03, 0x04, 0x05, 0x06	Record Response Data

Example

The following example shows how you read 4 bytes from slot 0 with parameter data record 128.

Table 3-67 CIP Request:

Field	Value	Description
Message Type	CIP Generic	
Service Code	0x32	Read Record
Class	0x66	Param Object
Instance ID	0x0001	Slot 0 and Subslot 1
Instance Attribute	128	Record Index
Source Length	4	CIP Request Length
Source Element	0x00, 0x00, 0x00, 0x04	Record Request Length

Table 3-68 CIP Response:

Field	Value	Description
Destination Element	0x00, 0x00, 0x00, 0x04	Record Response Length
	0x01, 0x02, 0x03, 0x04	Record Response Data

3.2.3.7 Configuration as generic EtherNet/IP module

You can use the following parameters to create the interface module in your engineering system as a generic EtherNet/IP module without an EDS station description.

The lengths of the assemblies can be taken from the User Defined Type (UDT) or CSV file exported with MFCT.

Table 3-69 Connection Path Settings - Example for EtherNet/IP Connection #0

☑ Configuration Assembly	Consuming Assembly (O-->T)	Producing Assembly (T-->O)
Class ID 16#4	Class ID 16#4	Class ID 16#4
Instance ID 16#307	Instance ID 16#300	Instance ID 16#301
Attribute ID 16#3	Attribute ID 16#3	Attribute ID 16#3

Table 3-70 Generic Parameters

Connection Name	Generic connection
Transport Type	Exclusive Owner
Connection Path	20 04 25 00 07 03 2D 00 00 03 2D 00 01 03
Timeout Muliplier	4

Table 3-71 Connection Parameters

Scanner to Target (Output)		Target to Scanner (Input)	
O-->T Size (Bytes)	246	T-->O Size (Bytes)	500
RPI (ms)	10	RPI (ms)	10
Trigger Type	Cyclic	Trigger Type	Cyclic
Inhibit Time (ms)	0	Inhibit Time (ms)	0
Config#1 Size (Bytes)	0	Fallback Mode	Go to zero <default>
Config#2 Size (Bytes)	0		
Connection Type	Point to Point	Connection Type	Point to Point
Fixed/Variable	Fixed	Fixed/Variable	Fixed
Transfer Format	32 bit Run/Idle	Transfer Format	pure Data

3.3 Diagnostics

3.3.1 Reading diagnostics via CIP EtherNet/IP

You can read out diagnostics information of MF devices or modules via the CIP Param Object.

To do this, call the Param Object (Page 58) with the RecIndex 0x800C Read (ReadRecord (0x32)).

The diagnostics responds with the following structure:

DiagnosisData

Field		Size	Description
BlockHeader			
	BlockType	Unsigned16	0x0010 = DiagnosisData
	BlockLength	Unsigned16	
	BlockVersionHigh	Unsigned8	0x01
	BlockVersionLow	Unsigned8	0x01
API		Unsigned32	0x00000000
SlotNumber		Unsigned16	
SubslotNumber		Unsigned16	
ChannelNumber		Unsigned16	0x8000 = Whole submodule
ChannelProperties		Unsigned16	
<ChannelDiagnosis> or <ExtChannelDiagnosis>			

ChannelDiagnosis

Field		Size	Description
UserStructureIdentifier		Unsigned16	0x8000 = ChannelDiagnosis
ChannelDiagnosisData			
<Channel>	ChannelNumber	Unsigned16	0x0000 – 0x7FFF: Manufacturer-specific 0x8000: Submodule (only one coding should be used for ChannelProperties.Direction.) 0x8001 – 0xFFFF: Reserved
<Channel>	ChannelProperties	Unsigned16	See the "ChannelProperties" table below
<Channel>	ChannelErrorType	Unsigned16	The error code for the MF device can be found in the section "Channel diagnostics" of the manuals. The error code for I/O modules can be found in the "Error code" column in section "Diagnostics alarms" of the manuals.

ExtChannelDiagnosis

Field		Size	Description
UserStructureIdentifier		Unsigned16	0x8002 = ExtChannelDiagnosis
ExtChannelDiagnosisData			
<Channel>	ChannelNumber	Unsigned16	0x0000 – 0x7FFF: Manufacturer-specific 0x8000: Submodule (only one coding should be used for ChannelProperties.Direction.) 0x8001 – 0xFFFF: Reserved
<Channel>	ChannelProperties	Unsigned16	See the "ChannelProperties" table below
<Channel>	ChannelErrorType	Unsigned16	The error code for the MF device can be found in the section "Channel diagnostics" of the manuals. The error code for I/O modules can be found in the "Error code" column in section "Diagnostics alarms" of the manuals.
<Channel>	ExtChannelErrorType	Unsigned16	
<Channel>	ExtChannelAddValue	Unsigned32	

ChannelProperties

Bits	Field	Description
0...7	ChannelProperties.Type	0x00: If ChannelNumber == 0x8000 0x01: The data length of the channel is 1 bit. 0x02: The data length of the channel is 2 bits. 0x03: The data length of the channel is 4 bits. 0x04: The data length of the channel is 8 bits. 0x05: The data length of the channel is 16 bits. 0x06: The data length of the channel is 32 bits. 0x07: The data length of the channel is 64 bits. 0x08 - 0xFF: Reserved
8	ChannelProperties.Accumulative	1 = Group diagnostics of more than one channel 0 = Other
9...10	ChannelProperties.Maintenance	0x00: Error 0x01: Maintenance required 0x02: Maintenance demanded 0x03: QualifiedChannelQualifier (indicates that the severity is coded in the field QualifiedChannelQualifier.)
11...12	ChannelProperties.Specifier	0x00: All following outgoing 0x01: Incoming 0x02: Outgoing 0x03: Outgoing, but other still present
13...15	ChannelProperties.Direction	0x00: Manufacturer-specific 0x01: Input 0x02: Output 0x03: Input/output 0x04 - 0x07: Reserved

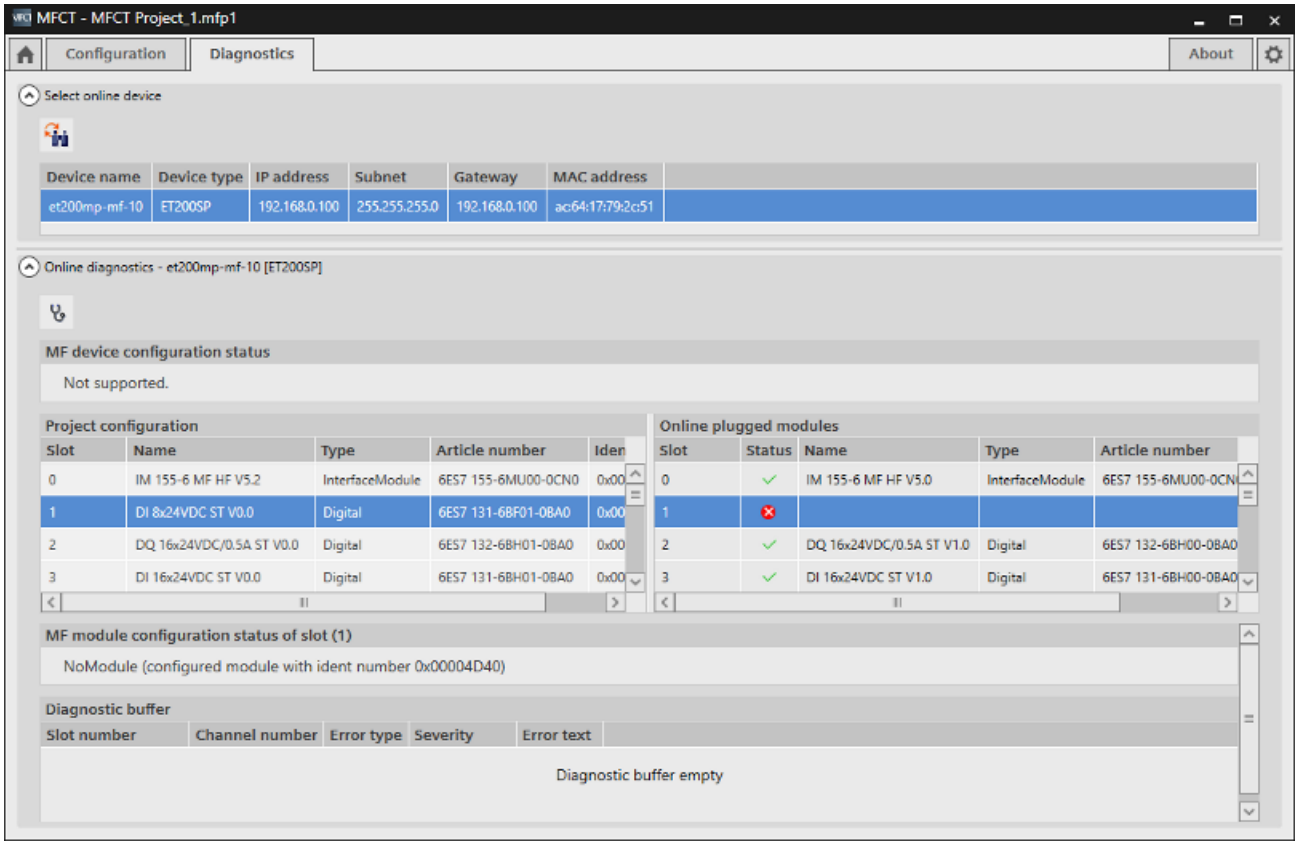
3.3.2 Reading diagnostics with MFCT

In the "Diagnostics" tab, you can read information of selected MF devices:

- The project configuration
- The online plugged modules
- Diagnostics from the diagnostic buffer

Follow these steps:

1. Click the "Start scan" button to find accessible MF devices via the preset network interface.
2. Select an MF device under "Select online device".



You can update the display under "Online plugged modules" with the "Update online status" button.



Project configuration

Under "Project configuration", you will receive information on the configuration of the selected MF device loaded in MFCT.

Online plugged modules

Under "Online plugged modules", you will receive information on the selected MF device, if it is accessible online.

MF module configuration status

Under "MF module configuration status", you can see whether an online plugged module matches the module in the MultiFieldbus project.

Diagnostic buffer

Under "Diagnostic buffer", you can see the content of the diagnostic buffer.

3.3.3 Reading hardware interrupt via CIP EtherNet/IP

Hardware interrupts are reported on EtherNet/IP via the IDS data status via service 34 of the CIP class 66. Service 34 processes the following tasks via acyclic data requests:

- Reading of interrupt information
- Sending of acknowledgements

Notification of hardware interrupts

Field	Bit number	Bit mask	Default	Bit value = '0'	Bit value = '1'
ProcessEvent	1	0x02	0	No process event	Process event available

Reading RALM via the GetAlarmInformation service

Retrieve interrupt information	
Service code	0x34
Class	0x66
Example	Instance index
Attribute	Event (0x0002 = PRAL)
Source data	ReadRequestData
Length of the source	4 bytes
Target data	ReadResponseData

Identifying User Structure Identifier (USI)

Use the following service to determine the USI in use.

Service	Data type	Command	Description
GetAlarmInformation (0x34)	Array of UINT8	**Call:** ReadRequestData [0..3]	Requested length (Big Endian)
		Response: ReadResponseData [0..3] ReadResponseData [4..ReadLength+3]	Length of the data sent Record read data for byte array

Data record response for USI 0x0001

The following table explains the data record response structure for USI 0x0001 with a length of 4 bytes.

Bits	Field	Description
16 ... 31	User Structure Identifier (USI)	0x0001
0 ... 1	Event	Event that triggered the hardware interrupt: 0x1: Rising edge 0x2 Falling edge
8 ... 11	Channel	Triggering channel 0x0 ... 0xF

Data record response for USI 0x8320

The following table explains the data record response structure for USI 0x8320 with a length of 14 bytes.

Bits	Field	Description
2 bytes	User Structure Identifier (USI)	0x8320
2 bytes	ChannelNumber	0x8000 (entire submodule)
2 bytes	PRAL_ChannelProperties	Value: 0x0000 Accumulative: 0x00 (individual) Direction: 0x00 (manufacturer-specific)
2 bytes	PRAL_Reason	0x9500 for event code: 0x0000 ... 0x7FFF 0x9501 for event code: 0x8000 ... 0xFFFF
2 bytes	PRAL_ExtReason	0x0001 ... 0x7FFF (event code)
4 bytes	PRAL_ReasonAddValue	0x0000 0000

3.3.4 PULL/PLUG event EtherNet/IP

The PULL/PLUG event is only supported by the MultiFieldbus IO-Link master.

With a correctly connected and parameterized submodule, the MF IO-Link master makes the configuration and parameterization available to the submodule.

PULL/PLUG event for EtherNet/IP

The PULL interrupt and PLUG interrupt is communicated to the controller by the data status.

PULL interrupt:
The PULL interrupt is triggered when a parameterized module is pulled. The PULL interrupt is triggered via the problem bit and the diagnostic bit in the data status.

PLUG interrupt:
The PLUG interrupt is triggered if the parameterization in the MF IO-Link master is not identical to the plugged module. The PLUG interrupt is triggered via the problem bit and the diagnostic bit in the data status.

Reset:
If the submodule meets the following properties, the interrupt is reset:

- Correctly connected
- Correctly configured
- Ready for cyclic communication

The following table shows the coding of the status bytes for IDS and ODS:

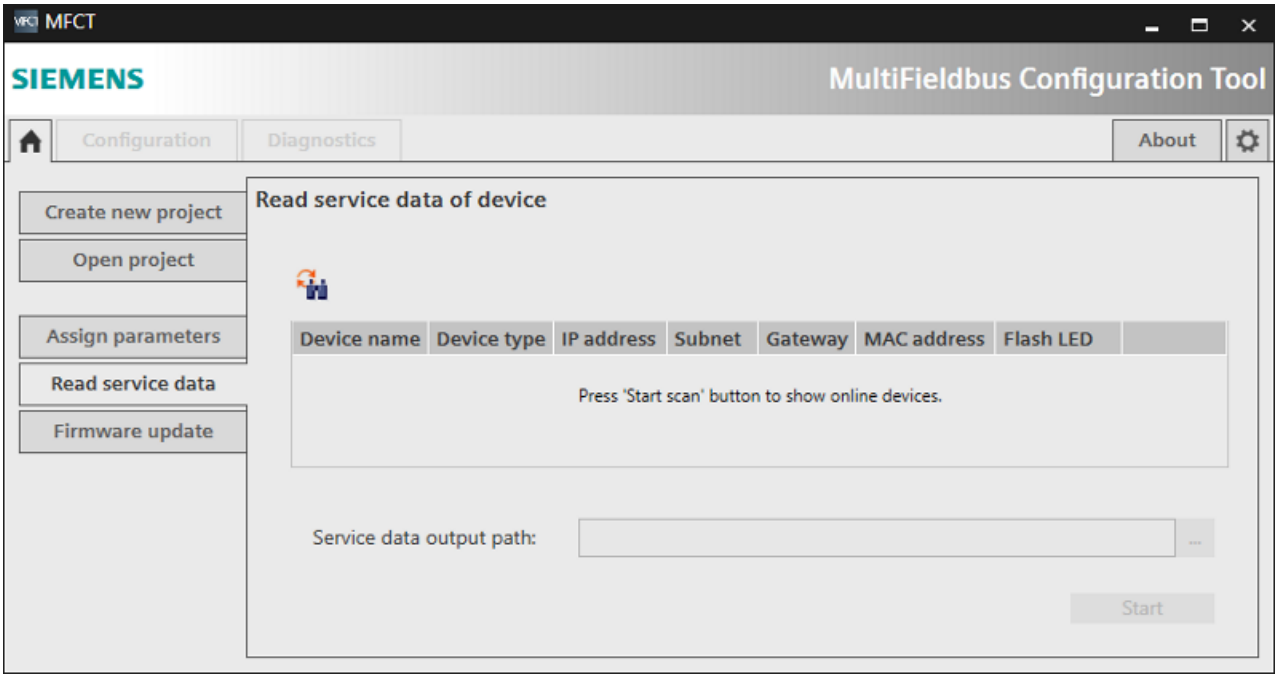
Field	Bit number	Bit mask	Default	Bit value = '0'	Bit value = '1'
Problem	6	0x40	0	Initial status	Module problem: • Module not plugged • Incorrect module plugged • Module with incorrect parameter assignment
Diagnosis	0	0x01	0	No diagnostics	Diagnostics available

3.3.5 Reading service data

In the "Home" tab, you can read out and store the service data provided by an MF device under "Read service data":

1. Click the "Start scan" button to find MF devices via the preset network interface.
2. Select an MF device.
   (You can make the LEDs of the MF device flash for identification with "Flash LED".)
3. Select the path to the location where you want to save the service data under "Service data output path".
4. Click the "Start" button.

The service data is saved under the selected path.



3.4 Supported CIP objects for EtherNet/IP

3.4.1 Identity Object

The following information applies to the Identity Object.

Class code	0x01
Class attributes	1, 2, 3
Class services	0x01, 0x05, 0x0E
Instance attributes	1, 2, 3, 4, 5, 6, 7
Instance services	0x01, 0x05, 0x0E
Number of instances	1

Attributes of instance 1 for the Identity Object

Attribute ID	Access rule	Designation	Data type	Data value
1	Retrieve	Vendor	UINT	0x04E3
2	Retrieve	Device type	UINT	0x000C
3	Retrieve	Product code	UINT	You can find the data value in the technical specifications of the MF device under "Device ID according to ODVA (ProductCode)".

Attribute ID	Access rule	Designation	Data type	Data value
4	Retrieve	Revision Major revision Minor revision	Structure of: USINT USINT	Depending on the firmware Vx.y.z • Major = x*10+y • Minor = z
5	Retrieve	Status	WORD	Defined in the definition table below Device_Status
6	Retrieve	Serial number	UDINT	Last 4 bytes of the MAC address
7	Retrieve	Product label Character string length ASCII character string	Structure of: USINT STRING	The data value is product-specific.

Device_Status definitions for the Identity Object

Bit(s)	Called	Definition	
0	Owned by	TRUE indicates that the device (or an object in the device) has an owner. 0 = No Exclusive Owner IO connection established 1 = At least one Exclusive Owner IO connection established	
1	-	Reserved	
2	Configured	TRUE indicates that the use of this device was configured so that it executes something other than the "Out-of-Box" standard. This does not include configuration of the communication. 0 = No valid MultiFieldbus project saved in the MF device (MF device in status < online) 1 = Active MultiFieldbus project saved in the MF device (MF device in status >= online) (Without a valid MultiFieldbus project with EtherNet/IP modules, the MultiFieldbus driver is offline and the CIP object cannot be accessed. This results in a timeout error.)	
3	-	Reserved	
4 to 7	Extended device status	**Bits 4 to 7**	**Description of the extended device status**
		0 0 0 0	Self-test or unknown.
		0 0 0 1	Ongoing firmware update.
		0 0 1 0	At least one faulty I/O connection. • I/O connection timed out? • I/O module missing? • I/O module IOxS bad?
		0 0 1 1	No I/O connections established.
		0 1 0 0	Non-volatile configuration faulty. • Multi-fieldbus project damaged? • ModuleDiffBlock?
		0 1 0 1	Severe error – either bit 10 or bit 11 is TRUE (1).
		0 1 1 0	At least one I/O connection is in RUN operating state.
		0 1 1 1	At least one I/O connection established, all in idle.
		1 0 0 0	Reserved
		1 0 0 1	
		1 0 1 0 to 1 1 1 1	Manufacturer/product-specific.
8	Minor, correctable error	TRUE indicates that the device has detected an internal problem which it considers to be correctable. The problem prevents the device from entering one of the faulty states. See the note below regarding the behavior.	
9	Minor uncorrectable error	TRUE indicates that the device has detected an internal problem which it considers to be uncorrectable. The problem prevents the device from entering one of the faulty states. See the note below regarding the behavior.	

Bit(s)	Called	Definition
10	Severe, correctable error	TRUE indicates that the device has detected an internal problem which has put the device in the "Severe, correctable error" state. See the note below regarding the behavior.
11	Severe uncorrect-able error	TRUE indicates that the device has detected an internal problem which has put the device in the "Severe, uncorrectable error" state. See the note below regarding the behavior.
12 to 1-5	-	Reserved

NOTE

Response after an error

A device cannot communicate in the "Severe uncorrectable error" state. This means it might also not be able to signal a severe uncorrectable error. A reset service is not processed. The only option to remedy a severe, uncorrectable error is to turn the power supply off and then on again.

General services for the Identity Object

Service code	Implemented for		Service designation
	Class	Instance	
0x01	Yes	Yes	Get_Attributes_All
0x05	Yes	Yes	Reset
0x0E	Yes	Yes	Get_Attribute_Single

3.4.2 Assembly Object

The following information applies to the Assembly object.

Class code 0x04
Class attributes 1, 2, 3
Class services 0x0E
Instance attributes 1, 2, 3
Instance services 0x0E, 0x10
Number of instances 4

Class attributes for the Assembly object

Attribute ID	Access rule	Description	Data type	Default value
1	Retrieve	Revision of this object	UINT	0x0002
2	Retrieve	Maximum permissible instance	UINT	0x0069
3	Retrieve	Number of instances	UINT	0x0004

Instance attributes for the Assembly object:

Output Assembly/Connection Point

Attribute ID	Access rule	Description	Data type	Default value
3	Set	Output data	ARRAY of BYTE	---

Input Assembly/Connection Point

Attribute ID	Access rule	Description	Data type	Default value
3	Retrieve	Input data	ARRAY of BYTE	---

Config Assembly/Connection Point

Attribute ID	Access rule	Description	Data type	Default value
3	Retrieve	Reserved for future use	ARRAY of BYTE	Zero

Instance attributes for the Assembly object:

Attribute ID 3

ConnectionIndex	Output Assembly /Connection Point	Input Assembly /Connection Point	Config Assembly /Connection Point
0	Instance 768 (0x300)	Instance 769 (0x301)	Instance 775 (0x307)
1	Instance 776 (0x308)	Instance 777 (0x309)	Instance 783 (0x30F)

General services for the Assembly object

Service code	Available service		Service designation	Description
	Class	Instance		
0x0E	Yes	Yes	Get_Attribute_Single	Returns contents of all relevant attributes
0x10	No	Yes	Set_Attribute_Single	Changes an attribute value

3.4.3 Connection Manager Object

The following information applies to the Connection Manager object.

Class code	0x06
Class attributes	1, 2, 3
Class services	0x01, 0x0E
Instance attributes	1, 2, 3, 4, 5, 6, 7, 8
Instance services	0x01, 0x0E
Number of instances	1

Attributes of instance 1 for the Connection Manager object

Attribute ID	Required in case of implement-ation	Access rule	NV	Designation	Data type	Description
1	Optional	Set [1]	V	Open Requests	UINT	Number of received Forward Open service requests.
2	Optional	Set [1]	V	Open Format Rejects	UINT	Number of Forward Open service requests that were rejected due to an incorrect format.
3	Optional	Set [1]	V	Open Resource Rejects	UINT	Number of Forward Open service requests that were rejected due to insufficient resources.
4	Optional	Set [1]	V	Open Other Rejects	UINT	Number of Forward Open service requests that were not rejected due to an incorrect format or a lack of resources.
5	Optional	Set [1]	V	Close Requests	UINT	Number of received Forward Close service requests.
6	Optional	Set [1]	V	Close Format Requests	UINT	Number of Forward Close service requests that were rejected due to an incorrect format.
7	Optional	Set [1]	V	Close Other Requests	UINT	Number of Forward Close service requests that were not rejected due to an incorrect format.
8	Optional	Set [1]	V	Close Timeout	UINT	Total number of connection timeouts that occurred in connections controlled by this Connection Manager.

[1] A device can reject a Set request for this attribute with the General Status Code 0x09 (Invalid attribute value) if the sent attribute value is not zero.

General services for the Connection Manager object

Service code	Implemented for		Service designation
	Class	Instance	
0x01	Yes	Yes	Get_Attributes_All
0x0E	Yes	Yes	Set_Attribute_Single

3.4.4 TCP/IP Interface Object

The TCP/IP interface object offers you access to status information and configuration of the TCP/IP network interface.

Class code	0xF5
Class attributes	1, 2, 3
Class services	0x1, 0xE
Instance attributes	1, 2, 3, 4, 5, 6, 13
Instance services	0x1, 0xE, 0x10
Number of instances	1

Class attributes for the TCP/IP interface object

Attribute ID	Access rule	Description	Data type	Default value
1	Retrieve	Revision	UINT	0x0004
2	Retrieve	Maximum permitted number of instances	UINT	0x0001
3	Retrieve	Number of instances	UINT	0x0001

Instance attributes for the TCP/IP interface object

Attribute ID	Access rule	Description	Data type	Default value	Value semantics
1	Retrieve	Interface status (status)	DWORD	0x00000002	See table below: "Table for "interface status", attribute 1"
2	Retrieve	Interface capability bit memory (configurability)	DWORD	0x00000010	Bit 0: BOOTP client (0 = No) Bit 1: DNS client (0 = No) Bit 2: DHCP client (0 = No) Bit 3: DHCP-DNS update (0 = Device cannot send its host name in the DHCP request) Bit 4: Configuration adjustable (0 = Interface configuration is not adjustable, see attributes 3 and 5) Bit 5: Configurable hardware (1 = IP address of the interface configuration can be called using the hardware settings (e.g. push wheel, thumbwheel, flash memory, etc.)) Bit 6: A change of the interface configuration requires a reset (false): 1 = A restart of the device is required for the change of the attribute of the interface configuration to take effect. 0 = the change of the attribute of the interface configuration takes effect immediately. Bit 7: AcdCapable: 0 = The device is not ACD-capable Bit 8...31: Reserved
3	Retrieve	Interface control bit memory (configuration control)	DWORD	0x00000000	Bit 0 to 3: Starting configuration (0 = As saved in flash memory, 1 = Via BOOTP, 2 = Via DHCP, 3 to 15 = Reserved) Bit 4: Enable DNS (False)

Attribute ID	Access rule	Description	Data type	Default value	Value semantics
4	Retrieve	Path to the physical link object	STRUCT from:		Identifies the object that is associated with the underlying physical communication object.
		Path size	UINT	0x0002	Number of 16-bit words in the path.
		Logical segments that identify the physical link	Increased EPATH	Class: = 0xF6 Instance = 1	Path address of the internal port of the embedded switch.
5	Retrieve	Interface configuration	STRUCT from:		Contains parameters that are required for operation as TCP/IP node. To prevent an incomplete or incompatible configuration, the parameters cannot be set individually. Users must first "retrieve" this attribute, change the desired parameters, and then "set" the attribute.
		IP address	UDINT	IP address of the device	The value 0 indicates that no IP address was configured. Otherwise, a valid address of class A, B or C must be set but not the loopback address (127.0.0.1).
		Network mask	UDINT	Network mask of the device	The value 0 indicates that no network mask address was configured.
		Gateway address	UDINT	Standard gateway address	The value 0 indicates that no IP address was configured. Otherwise, a valid address of class A, B or C must be set but not the loopback address (127.0.0.1).
		Primary name server	UDINT	0x00000000	The value 0 indicates that no name server address was configured. Otherwise, a valid A, B or C address must be set.
		Secondary name server	UDINT	0x00000000	The value 0 indicates that no secondary name server address was configured. Otherwise, a valid A, B or C address must be set.
		Domain name	STRING	0x0000 (length = 0, empty CHARACTER STRING)	ASCII characters. Maximum permissible length is 48 characters. Must be increased to an even number of characters (increase is not included in length). The length 0 indicates that no domain name is configured.
6	Set	Host name	STRING	Not supported (length zero)	ASCII characters. The maximum permissible length is 64 characters. Increased to an even number of characters (increase is not included in length). The length 0 indicates that no host name is configured.
13	Set	Encapsulation idle time	UINT	120	0 = disabled 1 to 3600 = timeout in seconds

Table for "Interface status", attribute 1

Bit(s):	Called:	Definition	
0 to 3	Interface configuration status	Displays the status of the interface configuration attribute.	0 = The interface configuration attribute was not configured 1 = The interface configuration attribute contains a valid configuration obtained from BOOTP, DHCP or non-volatile memory. 2 = The interface configuration attribute contains a valid configuration obtained from hardware settings (e.g. push wheel, thumbwheel, flash memory, etc.) 3 to 15 = Reserved for future use

Bit(s):	Called:	Definition
4	Mcast requested	Specifies a requested configuration change in the TTL value and/or in the McastConfig attributes. This bit is set when either the TTL value or the McastConfig attribute is set and deleted later as soon as the device starts.
5	Interface Configuration Pending	Shows a pending configuration change in the Configuration-Attribute interface. The bit turns 1 (TRUE) when the Configuration-Attribute interface is set; the device needs a reset for the configuration change to become effective (as shown in the Configuration-Attribute interface). The reason for the Interface Config Pending bit is to permit the client software to know that the IP configuration has changed but only becomes active after a device reset.
6	AcdStatus	Indicates that an IP address conflict was detected by ACD. The bit is set to 0 (FALSE) by default during startup. When ACD is supported and activated, the bit is set to 1 (TRUE) whenever an address conflict as defined in [ConflictDetected] transition in Figure F-1.1 ACD Behavior of Volume 2 EtherNet/IP Adaptation of CIP, Appendix was detected.
7	AcdFault	Indicates that an IP address conflict was detected by ACD or the defense failed, and the current interface configuration can not be used due to a conflict. The bit turns 1 (TRUE) if an address conflict was detected and the interface is in the ACD status Notification & FaultAction or AcquireNewIpv4Parameters, as defined in Annex F. In other cases, the bit turns 0 (FALSE). Note that if the bit is set, the CIP port can not be used. However, the bit offers a way for devices with several ports to find out whether the port has an ACD error and therefore can not be used.
8	IANA Port Admin Change Pending	Shows a pending configuration change in the IANA Port Admin attribute. The bit is set when the device needs a reset for the configuration change to become effective (as shown in the Admin Capability element of the IANA Port Admin attribute).
9	IANA Protocol Admin Change Pending	Shows a pending configuration change in the IANA Protocol Admin attribute. The bit is set when the device needs a reset for the configuration change to become effective (as shown in the Admin Capability element of the IANA Protocol Admin attribute).
10 to 31	Reserved	Reserved for future use and set to zero.

General services for the TCP/IP interface object

Service code	Available service		Service designation	Description
	Class	Instance		
0x01	Yes	Yes	Get_Attribute_All	Returns contents of all attributes
0x0E	Yes	Yes	Get_Attribute_Single	Returns contents of all relevant attributes
0x10	No	Yes	Set_Attribute_Single	Changes an attribute value

3.4.5 EtherNet Link Object

The EtherNet Link object saves link-specific counters and status information for a IEEE 802.3 communication interface. MF devices have an embedded two-port switch and an instance of the EtherNet Link object for the internally accessible interface.

Values set in instance 1 attribute 6 are valid for both ports.

Class code -
Class attributes 1, 2, 3
Class services 0x1, 0xE, 0x10

Instance attributes 1, 2, 3, 4, 5, 6, 7, 8, 10, 11
Instance services 0x1, 0xE, 0x10
Number of instances 2

Class attributes for the EtherNet Link Object

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
1	Retrieve	Revision	Revision of this object	UINT	1 = The minimum value ≥ 2 = When the instance attribute 6 is implemented 3 = The maximum value
2	Retrieve	Max. instance	Maximum instance number of an object that was currently created on this class level of the device.	UINT	The greatest instance number of a created object on this class hierarchy level.
3	Retrieve	Number of instances	Number of object instances that were currently created on this class level of the device.	UINT	The number of object instances on this class hierarchy level.

Attributes of instance 1 for the EtherNet Link Object

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
1	Retrieve	Interface speed	Currently applied interface speed	UDINT	Speed in Mbps (10, 100, etc.). Default = 100
2	Retrieve	Interface bit memory	Interface status bit memory	DWORD	Bitmap of interface bit memory. See table below, "Interface bit memory attribute".
3	Retrieve	Physical address	MAC layer address	ARRAY of 6 USINTs	MAC layer address in the format "XX-XX-XX-XX-XX-XX."
4	Retrieve	Interface counter	Important for receiving packets	STRUCT from:	See section "Interface counter" below.
5	Retrieve	Media counter	Media-specific counters	STRUCT from:	See "Media counter" section below.
6	Set	Interface control	Configuration for physical interface	STRUCT from:	See the following section, "Interface control".
		Control bits	Interface control bits	WORD	See the following section, "Interface control"
		Forced interface speed	Speed at which the interface is supposed to work	UINT	Speed in Mbps (10, 100, etc.). When the autonegotiation bit is 0, the forced interface speed bits show the speed at which the interface is to operate.
7	Retrieve	Interface type	Interface type: Twisted pair, fiber, internal, etc.	USINT	2 = Twisted pair 3 = Optical fiber
8	Retrieve	Interface status	Current status of the interface: in operation, disabled, etc.	USINT	0 = Unknown 1 = Enabled and ready for sending (default) 2 = Disabled 3 = Testing

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
10	Retrieve	Interface name	Human-readable identifier	SHORT_STRING	"Siemens, SIMATIC S7, Ethernet Port, X1 P1 R" "Siemens, SIMATIC S7, Ethernet Port, X1 P2 R"
11	Retrieve	Interface capability	Shows the capabilities of the interface	STRUCT from:	----
		Function bits	Interface capabilities except speed/duplex	DWORD	Bitmap
		Speed/duplex options	Shows speed/duplex pairs supported by the interface control attribute	STRUCT from:	----
			Speed/duplex array counter	USINT	Number of elements
			Speed/duplex array	ARRAY of STRUCT from:	----
			Interface speed	USINT	The semantics are the same as for the forced interface speed in the interface control attribute: Speed in Mbps.
			Interface duplex mode	USINT	0 = Half-duplex 1 = Full duplex 2 to 255 = Reserved

Interface bit memory attribute

Bit(s):	Called:	Definition
0	Link status	Specifies whether the IEEE 802.3 communication interface is connected to an active network: 0 = Inactive link. 1 = Active link. Specification of the link status depends on the implementation.
1	Half duplex / full duplex	Indicates the currently used duplex mode: 0 = Interface runs at half duplex. 1 = Interface runs at full duplex. Note that the value of the half duplex / full duplex is undefined when the link status bit memory is 0.
2 to 4	Negotiation status	Specifies the status of the link autonegotiation: 0 = Ongoing autonegotiation. 1 = Autonegotiation and speed measurement failed. Use of default values for speed and duplex. 2 = Autonegotiation failed, but speed was measured. Duplex was faulty. 3 = Speed and duplex negotiated successfully. 4 = Autonegotiation not attempted. Forced speed and duplex.
5	Manual setting requires reset.	0 = Interface can automatically activate changes to link parameters (autonegotiate, duplex mode, interface speed). 1 = Device requires that a reset service is output at its Identity object so that the changes will become effective.
6	Local hardware fault	0 = Interface does not detect a local hardware fault. 1 = Local hardware fault detected.
7 to 31	Reserved	Set to 0.

Interface counter (STRUCT from):

Designation	Data type	Attribute description
In Octets	UDINT	Octets received at the interface
In Ucast Packets	UDINT	Unicast packets received at the interface
In NUcast Packets	UDINT	Non-Unicast packets received at the interface
In Discards	UDINT	Incoming packets received at interface but discarded
In Errors	UDINT	Incoming packets containing errors (excluded In Discards)
In Unknown Protos	UDINT	Incoming packets with unknown protocol
Out Octets	UDINT	Octets transmitted by the interface
Out Ucast Packets	UDINT	Unicast packets transmitted by the interface
Out NUcast Packets	UDINT	Non-Unicast packets transmitted by the interface
Out Discards	UDINT	Outgoing packets discarded
Out Errors	UDINT	Outgoing packets containing errors

Media counter (STRUCT from):

Designation	Data type	Attribute description
Alignment Errors	UDINT	Frames received that not only include complete octets
FCS Errors	UDINT	Frames received that do not pass the FCS test
Single Collisions	UDINT	Successfully transmitted frames with exactly one collision
Multiple Collisions	UDINT	Successfully transmitted frames with more than one collision
SQE Test Errors	UDINT	Number of error messages generated by SQE test
Deferred Transmission	UDINT	Frames whose transmission is delayed due to medium overload
Late Collisions	UDINT	Number of cases in which a collision is detected later than after transmission of 512 bits of the packet
Excessive Collisions	UDINT	Frames whose transmission fails due to a very high number of collisions
MAC transmission error	UDINT	Frames whose transmission failed due to an internal transmission error in the MAC sublayer
Carrier Sense Errors	UDINT	Number of carrier tests that failed or were not executed during transmission of a frame
Frame Too Long	UDINT	Frames received that exceed the permissible maximum size
MAC receive error	UDINT	Frames whose receipt at an interface failed due to an internal transmission error in the MAC sublayer

Interface control attribute

The interface control attribute is a structure that consists of bits of the forced interface speed and control bits.

When the autonegotiate bit is 0, the bit of the forced interface speed specifies the speed at which the interface is operating. The speed is given in megabits per second; the interface speed for an Ethernet with 10 Mbps, for example. Interfaces that do not support the required speed, show 0x09 (invalid attribute value). When autonegotiation is enabled, the attempt to set the forced interface speed results in the response 0x0C (object status conflict).

Control bits work as follows:

Bit(s)	Called:	Definition
0	Autonegotiate	0 = 802.3 Link autonegotiation is disabled. 1 = Autonegotiation is enabled. When autonegotiation is disabled, the device uses the settings made by the bits of the forced duplex mode and the forced interface speed.
1	Forced duplex mode	When the autonegotiate bit is 0, the bit of the forced duplex mode specifies whether the interface operates in full duplex or half duplex mode. 0 = Half-duplex 1 = Full duplex Interfaces that do not support the required duplex mode, show 0x09 (invalid attribute value). When autonegotiation is enabled, the attempt to set the bits of the forced duplex mode results in the response 0x0C (object status conflict).

Interface capability

The interface capability attribute displays the number of interface capabilities. The attribute is a structure with two main elements: Function bits and speed/duplex options

Bit(s)	Called:	Definition
0	Manual setting requires reset	Indicates whether a device requires a reset to apply changes of the interface control attribute (#6). 0 = Indicates that changes made to the interface control attribute (#6) will become effective without resetting the device. The bit takes on this value when the interface control attribute (#6) is not implemented. 1 = Indicates that changes made to the interface control attribute (#6) are not applied automatically but will only become effective by resetting the device. Note: This bit is repeated in the interface bit memory attribute (#2) to ensure backward compatibility with earlier object revisions.
1	Autonegotiate	0 = Indicates that the interface does not support link autonegotiation. 1 = Indicates that the interface supports link autonegotiation.
2	Auto-MDIX	0 = Indicates that the interface does not support automatic MDIX mode. 1 = Indicates that the interface supports MDIX mode.
3	Speed/duplex manual	0 = Indicates that the interface does not support manual setting of speed/duplex. The interface control attribute (#6) is not supported. 1 = Indicates that the interface supports manual setting of speed/duplex via the interface control attribute (#6).
4 to 31	Reserved	Set to 0

General services for the EtherNet Link object

Service code	Required in implementation		Service designation	Description
	Class	Instance		
0x01	Optional	Optional	Get_Attribute_All	Returns contents of all attributes.
0x0E	Conditional	Required	Get_Attribute_Single	Returns contents of all relevant attributes.
0x10	Not applicable	Conditional	Set_Attribute_Single	Changes a single attribute.

3.4.6 LLDP Management Object

The object contains management information for LLDP and should be present when LLDP is implemented on the device. Only one instance of the LLDP management object should be implemented.

Referring to ODVA Specification Rel.1911 / Volume 2 (1.25) / 5-15 LLDP Management Object.

Class code 0x109

Instance attributes 1, 2, 3, 4, 5

Number of instances 1

Attributes of instance 1 for the LLDP Management Object

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
1	Setting required	LLDP Enable		STRUCT from:	
		LLDP Enable Array Length	The number of elements in the LLDP Enable Array. Matches the Max Ethernet Link Object Instance Number. This value, divided by 8 and the remainder rounded, specifies the length (in bytes) of the LLDP Enable Array of this structure.	UINT	Class attribute 2 of the Ethernet Link Object (0xF6)
		LLDP Enable Array	Enables the generation of LLDP frames globally or per port and the processing of received LLDP frames globally.	ARRAY from BOOL	Bit number: 0: Enable globally 1-N: Corresponds to the instance number of each port of Ethernet Link Max Instance, N = value of Ethernet Link Max Instance class attribute 2 For every bit: 0 = LLDP deactivated, **1 = LLDP activated (default)** If Enable globally (bit 0) = 0, then the other bits must be ignored and the received LLDP frames are ignored. The values of the elements corresponding to non-existing Ethernet link instances must be set to 0 or are ignored.
2	Setting required	msgTxInterval	From 802.1AB-2016. The interval in seconds after which the LLDP frames were sent from the device	UINT	0-4 = Reserved, 5-32768 = Message Transmission Interval for LLDP frames, 32769-65535 = Reserved **Recommended default setting is** 30. **Default value = 5** (Only acceptable value to be additionally compliant with the PNIO standard.).

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
3	Retrieval required	msgTxHold	From 802.1AB-2016. A factor of msgTxInterval to determine the value of TTL TLV that was sent by the neighboring device	USINT	0 = Reserved, 1-100 = Message Transmission Multiplier for LLDP frames, 101-255 = Reserved **Recommended default setting is 4.**
4	Retrieval required	LLDP Datastore	An indication of the query method that is supported by the service's LLDP database (see Section 9-8.5)	WORD	Bit: **0 = LLDP Data Table Object (Default)** 1 = SNMP 2 = NETCONF YANG 3 = RESTCONF YANG 4-15 = Reserved
5	Retrieval required	Last Change	The number of seconds since the last time an entry in the local LLDP database (without TTL) has changed.	UDINT	Seconds since last change

3.4.7 LLDP Data Table Object

The object contains information about received LLDP frames and should be present when LLDP is implemented on the device and SNMP LLDP MIB has not been implemented.

Referring to ODVA Specification Rel.1911 / Volume 2 (1.25) / 5-16 LLDP Data Table Object.

Class code 0x10A
Class attributes 2, 3
Instance attributes 1, 2, 3, 4, 5, 6, 7, 8, 9
Number of instances 2

Attributes for the LLDP Data Table Object

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
1	Retrieval required	Ethernet Link Instance Number	The local instance number of the Ethernet Link Object that corresponds to the physical Ethernet port of the received instance that makes up the LLDP frame, if available.	UINT	0 = Unknown 1-65535 = Ethernet Link Object (0xF6) instance number
2	Retrieval required	MAC address	The neighboring MAC address received from the CIP MAC address, Chassis ID, or Port ID TLV.	ETH_MAC-_ĀDDR	The MAC address is set with the first occurrence of a MAC ID in the following list: 1. The CIP MAC address (TLV type = 127, subtype = 2) 2. The Chassis ID (TLV type = 1) only if subtype = 2 3. The Port ID (TLV Type = 2) only if subtype = 3 4. All zero
3	Retrieval required	Interface Label	The neighboring Interface Label received from the CIP Interface Label, Chassis ID, or Port ID TLV	Short_String	The Interface Label will be a maximum of 64 characters long. It is set with the first occurrence of an Interface Label which is contained in the following list:

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
					1. The CIP Interface Label (TLV type = 127, subtype = 1) 2. The Chassis ID (TLV type = 1) only if subtype = 6 3. The Port ID (TLV type = 2) only if subtype = 5 4. One zero string
4	Retrieval required	Time to Live	Number of seconds for which the neighborhood information is considered valid.	UINT	(TLV type = 3) 0 = Reserved, 1-65535 = Time To Live (in seconds) Note: A received TTL TLV value = 0 means that the table entry should be removed according to IEEE 802.1AB-2016.
5	Retrieval required	System Capabilities TLV		STRUCT from:	(TLV type = 7) See section 5-16.3.3.1
		System Capabilities	The capabilities that the neighboring device supports based on the currently loaded firmware.	WORD	
		Enabled Capabilities	The capabilities currently activated on the neighboring device.	WORD	
6	Retrieval required	IPv4 Management Addresses	The IPv4 management addresses of the neighboring device.	Struct from:	A list of IPv4-encoded management addresses, as defined by one or more received management addresses TLVs (TLV type = 8). Without non-IPv4 management addresses
		Management Address Count	Number of implemented management addresses	USINT	0-255 = Number of received Management Address TLVs from its neighbor.
		Management Address	IPv4 management addresses of neighboring devices	ARRAY from UDINT	The IP address must be assigned a valid Class A, B or C address and must not consist of just zeros or be the loopback address (127.0.0.1).
7	Retrieval required	CIP Identification	The CIP Identification TLV of the neighboring device, if available.	STRUCT from:	Set by CIP Identification TLV (TLV type = 127, subtype = 01), if available, otherwise 0.
		Vendor ID		UINT	See Volume 1, Appendix C-1.4.2, format 5 for details and semantics
		Device Type		UINT	
		Product Code		UINT	
		Major Revision		BYTE	
		Minor Revision		UINT	
		CIP Serial Number		UDINT	
8	Retrieval required	Additional Ethernet Capabilities	A TLV for Ethernet preemption support from the neighboring device	STRUCT from:	Set by Additional Ethernet Capabilities TLV (TLV type = 127, subtype 7), if available, otherwise 0 See IEEE 802.3-2018 79.3 for more information.
		Preemption Support		BOOL	0 = Not supported 1 = Supported
		Preemption Status		BOOL	0 = Not released 1 = Released

Attribute ID	Access rule	Designation	Description	Data type	Value semantics
8		Preemption Active		BOOL	0 = Not active 1 = Active
		Additional Fragment Size		USINT	0 = 64 octets 1 = 128 octets 2 = 192 octets 3 = 256 octets 4-255 = Reserved
9	Retrieval required	Last Change	The number of seconds since the last time an attribute in this instance has changed.	UDINT	Seconds since last change

3.4.8 Param Object

You can transfer PROFINET data records by accessing the Param Object.
The following information applies to the Param Object of the MF device.

Class code 0x66
Class attributes 1
Class services -
Instance attributes -
Instance services -
Number of instances 256

Class attributes for the Param Object

Attribute ID	Access rule	Description	Data type	Default value
1	Retrieve	Revision of this object	UINT32	

Attributes of instance 1 for the Param Object

Attribute	Service Code	Element	Data type	Data value
Index of the PROFINET data record	ReadRecord (0x32)	**Source:** Read length **Source Length:** 4	UINT32	**Call:** Read length[0..3] = Length of the requested data record to be read. (Big Endian) The maximum read length is 3992 bytes.
		Destination: Read buffer	UINT32 Array of UINT8	**Response:** Read buffer[0..3] = Length of the returned data record (response length in big-endian) Read buffer[4..ResponseLength+3] = Read data record as an array of bytes

Attribute	Service Code	Element	Data type	Data value
Index of the PROFINET data record	WriteRecord (0x33)	**Destination:** Write buffer	UINT32 Array of UINT8	**Call:** Write buffer[0..3] = Length of the data to be written to the data record (*Write length* in big-endian) Write buffer[4..write length+3] = Data of the data record to be written as an array of bytes The maximum write length is 3984 bytes. **Response:** No user data returned.
	GetAlarmInformation (0x34)	**Source:** Read length **Source Length:** 4	UINIT32	**Call:** Read length[0..3] = Length of the requested data record to be read. (Big Endian) The maximum read length is 3992 bytes.
		Destination: Read buffer	UINT32 Array of UINT8	**Response:** Read buffer[0..3] = Length of the returned data record (response length in big-endian) Read buffer[4..ResponseLength+3] = Read data record as an array of bytes

Answer-Record-Mapping

PROFINET ErrorCode1		**EtherNet/IP CIP Status**	
Success:			
0x00	Successful Operation	0x00	Success
Application error:			
0xA0	Read Error	0x1F	Vendor specific error
0xA1	Write Error	0x1F	Vendor specific error
0xA2	Module Failure	0x1F	Vendor specific error
0xA7	Busy	0x1E	Embedded service error
0xA8	Version Conflict	0x1F	Vendor specific error
0xA9	Feature Not Supported	0x14	Attribute not supported
Access error:			
0xB0	Invalid Index	0x09	Invalid attribute value
0xB1	Write Length Error	0x15	Too much data
0xB2	Invalid Slot/Subslot	0x05	Class/Instance unknown
0xB3	Type Conflict	0x0E	Attribute not settable
0xB4	Invalid Area/API	0x16	Object does not exist
0xB5	State Conflict	0x10	Device state conflict
0xB6	Access Denied	0x0F	Privilege violation
0xB7	Invalid Range	0x20	Invalid parameter
0xB8	Invalid Parameter	0x20	Invalid parameter
0xB9	Invalid Type	0x29	Member not settable
Resources error:			
0xC0	Read Constrain Conflict	0x2C	Attribute not gettable
0xC1	Write Constrain Conflict	0x0E	Attribute not settable
0xC2	Resource Busy	0x0C	Object state conflict
0xC3	Resource Unavailable	0x02	Resource unavailable

PROFINET ErrorCode1		**EtherNet/IP CIP Status**	
S7+ module application error:			
0xE0	Invalid Record Struct	0x24	Message Format Error
0xE1	Invalid User Param	0x03	Invalid parameter value
ELSE response error:			
		0x1F	Vendor specific error

When not enough data is provided for the Record Message Source Element, the device always returns CIP Status error 0x06 (Partial Transfer).

Modbus TCP

4

4.1 Modbus TCP functions

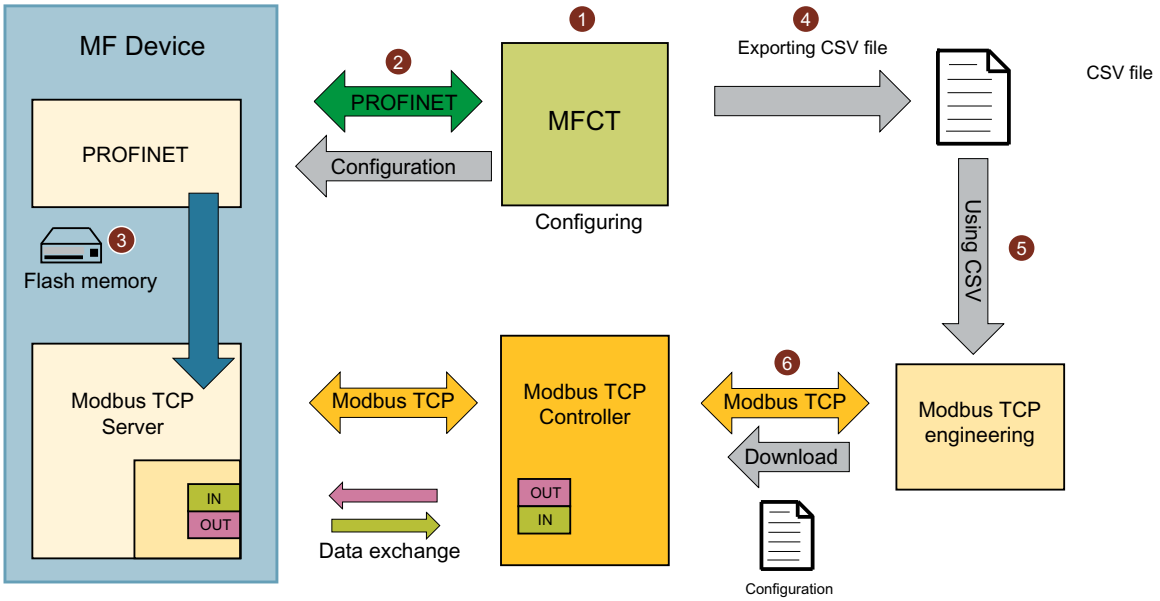
4.1.1 Modbus TCP

MultiFieldbus supports the following Modbus TCP functions:

- I/O communication with Modbus client
- Free user registers (e.g. for coordination of the redundancy)
- Device status register
- Config status tab
- Diagnostics bit in data status of cyclic I/O data per submodule (interrupts are not supported)
- Data record interface

4.2 Integration in the automation system

4.2.1 Overview



In the MultiFieldbus Configuration Tool (MFCT), you configure the MF device and assign an IP address and a device name to the MF device ①. You then download the configuration to the MF device with PROFINET IO mechanisms ②. The configuration is saved on the MF device ③. You generate and export the I/O data mapping of the MF device as CSV file for Modbus TCP in

MFCT ④. You then use the CSV file to implement I/O access in your Modbus TCP application ⑤. Download the project to the Modbus TCP controller with the engineering system ⑥.

Procedure

For commissioning, follow these steps:

1. Scan the network in MFCT and assign an IP address for the MF device.
2. Configure the MF device.
3. Select Modbus TCP as fieldbus for the Ethernet interface.
4. Load the MultiFieldbus project to the MF device.
5. Exporting a CSV file from MFCT.
6. Use the CSV file to implement your Modbus TCP application.
7. Configure the interface module in the Modbus TCP engineering system.
8. Download the project to the Modbus TCP controller.
9. (Optional) Configure the modules from inside the user program.

NOTE

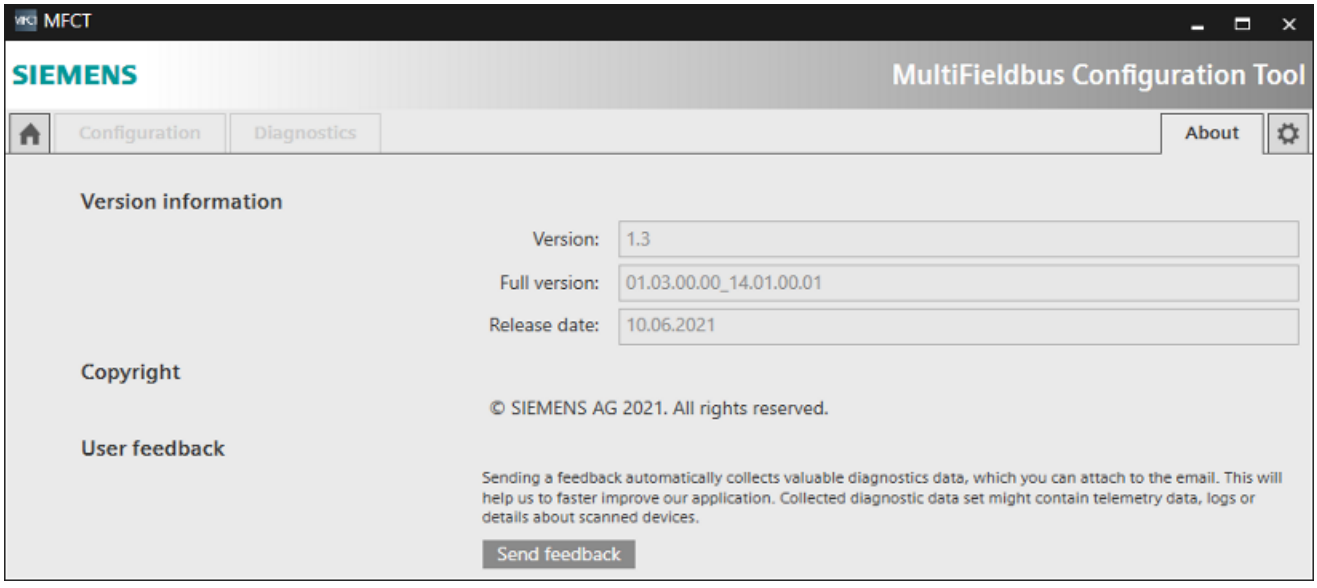
For MF devices, there might be modules displayed in engineering systems starting with slot 1000.
These merely reflect the retentively stored project in the MF device consisting of configuration and parameter assignment.

4.2.2 Configuring with MFCT

4.2.2.1 Requirements

Information on which MFCT version is required for which MF Device can be found in the Equipment Manual of the MF Device.

You can find version information for MFCT on the "About" tab.

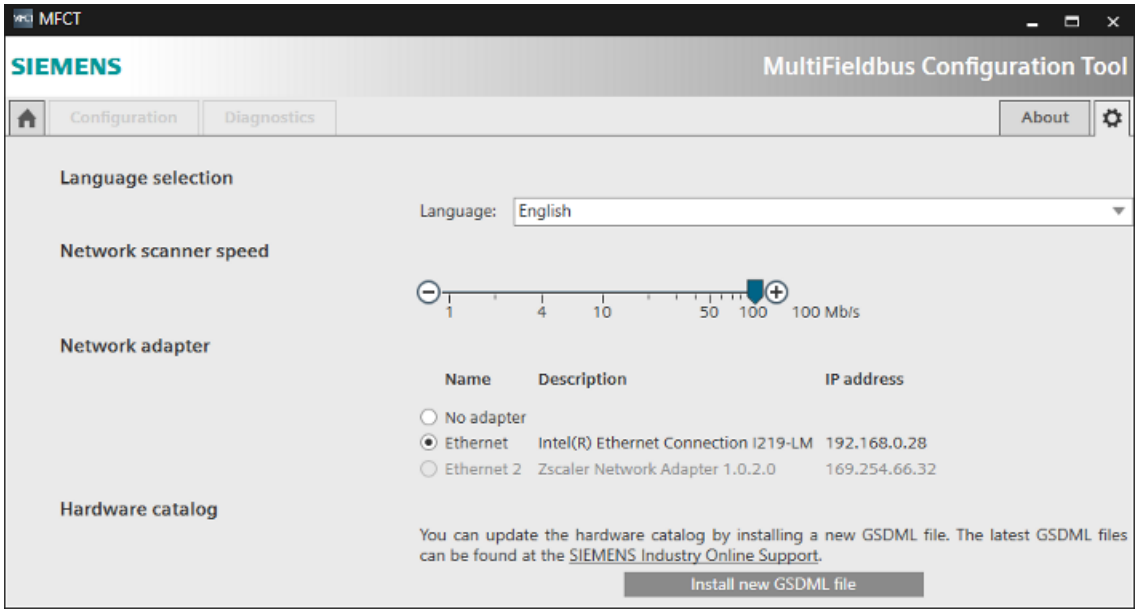


4.2.2.2 Settings

In the "Settings" tab, you can specify basic properties of the MultiFieldbus Configuration Tool:

- Select the user interface language.
- Select the network adapter.

You can also update the GSD file used.



Language selection

Under "Language selection", select the user interface language for the MFCT.

Network scanner speed

Under "Network scanner speed", select the speed of the network scanner.

Network adapter

Under "Network adapter", select the interface you want to use to connect to MF devices.

Hardware catalog

In the "Hardware catalog" section, you can update the GSD module description in the MFCT using the "Install new GSDML file" button.

To do this, proceed as follows:

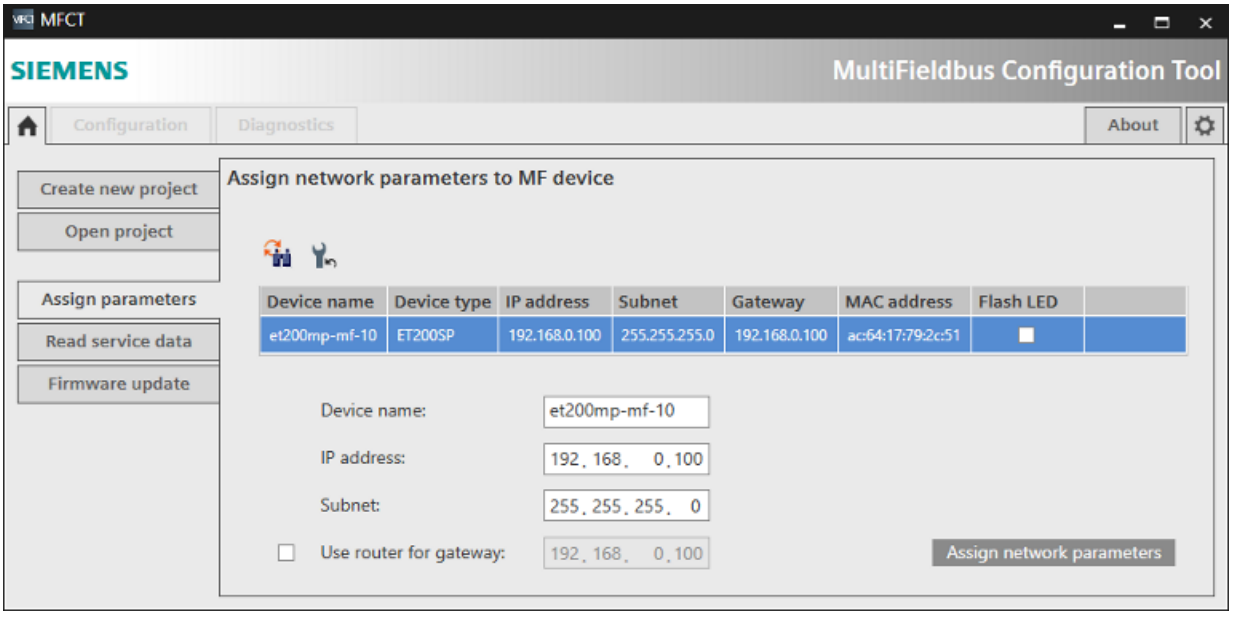
1. Click the link in the text.
2. Download the zipped GSD file and save it locally.
3. Unzip the GSD file.
4. Click "Install new GSDML file" and select the unzipped GSD file.

4.2.2.3 Assigning network parameters

In the "Home" tab, you can assign the network parameters for MF devices under "Assign parameters":

1. Click the "Start scan" button to find MF devices via the preset network interface.
2. Select an MF device.
   (You can make the LEDs of the MF device flash for identification with "Flash LED".)
3. Enter a device name, valid IP address and the subnet mask.
4. If you use a gateway, you can enable the "Use router for gateway" option and enter the router address.
5. Click "Assign network parameters".

The network parameters are assigned.

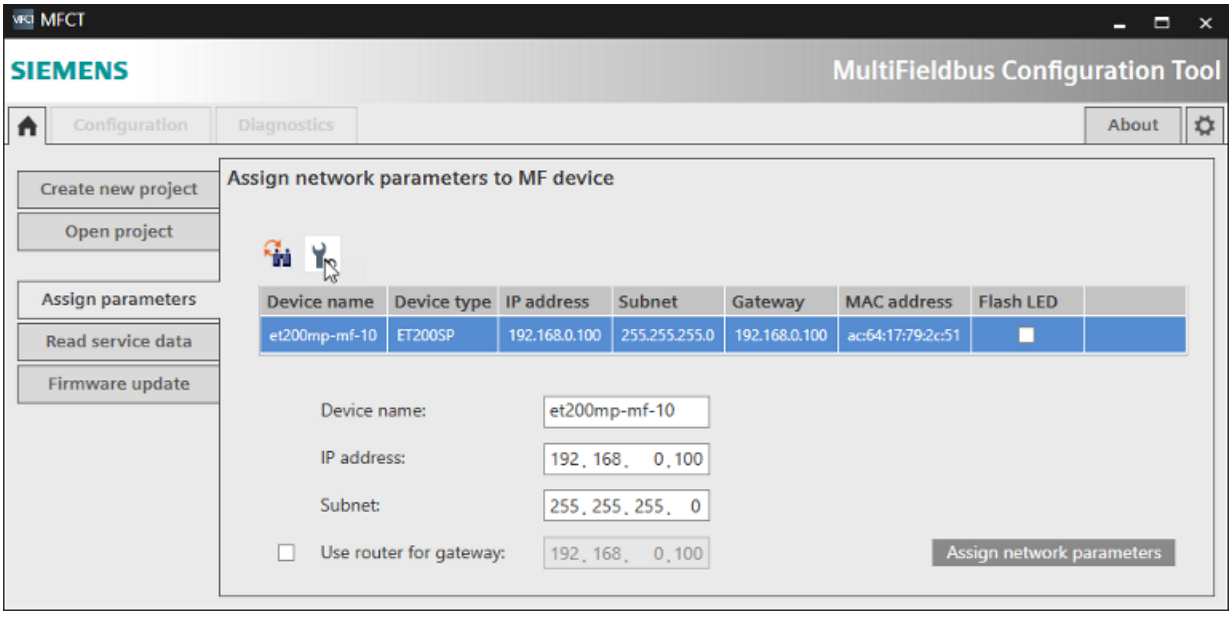


4.2.2.4 Resetting the MF device

In the "Home" tab, you can reset the MF device to the factory settings under "Accessible MF devices":

1. Click the "Start scan" button to find MF devices via the preset network interface.
2. Select an MF device.
3. Click "Reset network parameters".

The network parameters and the MultiFieldbus project are deleted.

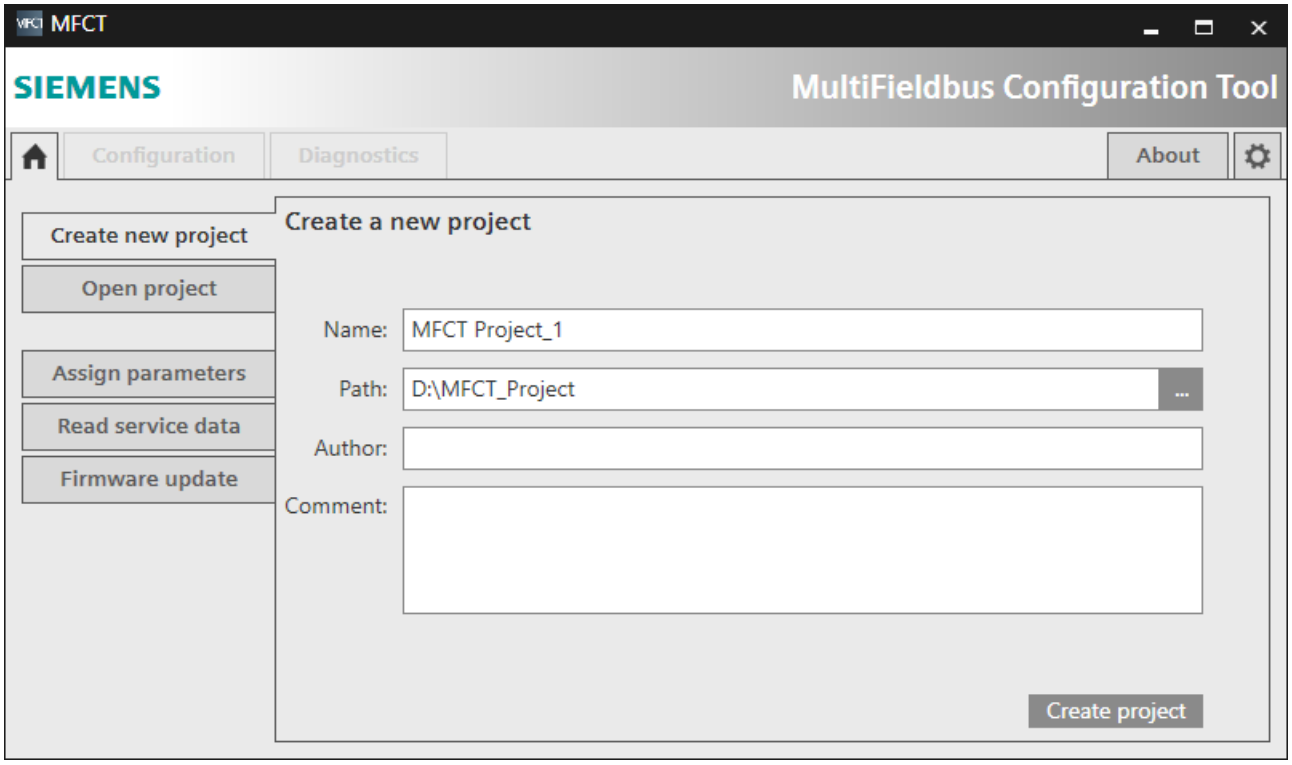


4.2.2.5 Creating new MultiFieldbus project in MFCT

You can create a new MultiFieldbus project in the "Home" tab:

1. Select "Create new project" and enter a name and a path for the new MultiFieldbus project.
   Optionally, you can describe the project in more detail by entering the author and comments.
2. Click "Create project".

The MultiFieldbus project is created as a file with the extension ".mfp1". The MFCT then goes to the next step in the "Configuration" tab.



4.2.2.6 Open MultiFieldbus project in MFCT

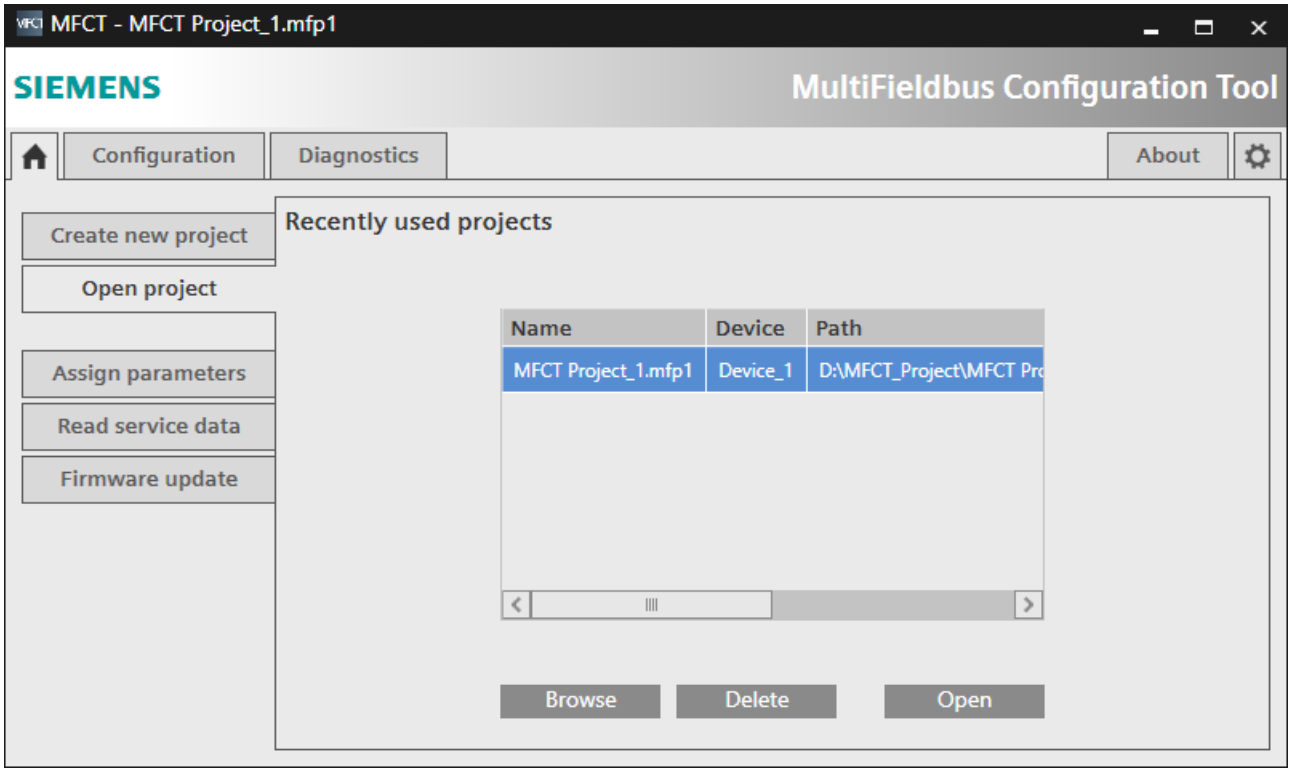
You can open an existing MultiFieldbus project in the "Home" tab:

1. Select "Open project".
   - Under "Recently Used Projects", you can select a recently edited project and read it in directly by double-clicking it or using the "Open" button.
   - Alternatively, you can use the "Browse" button to open a project file.

The project is opened and the MFCT switches to the "Configuration" tab.

NOTE

The "Delete" button allows you to delete an existing project from the "Recently Used Projects" list. The project file itself is not deleted by this action.



4.2.2.7 Selecting a station

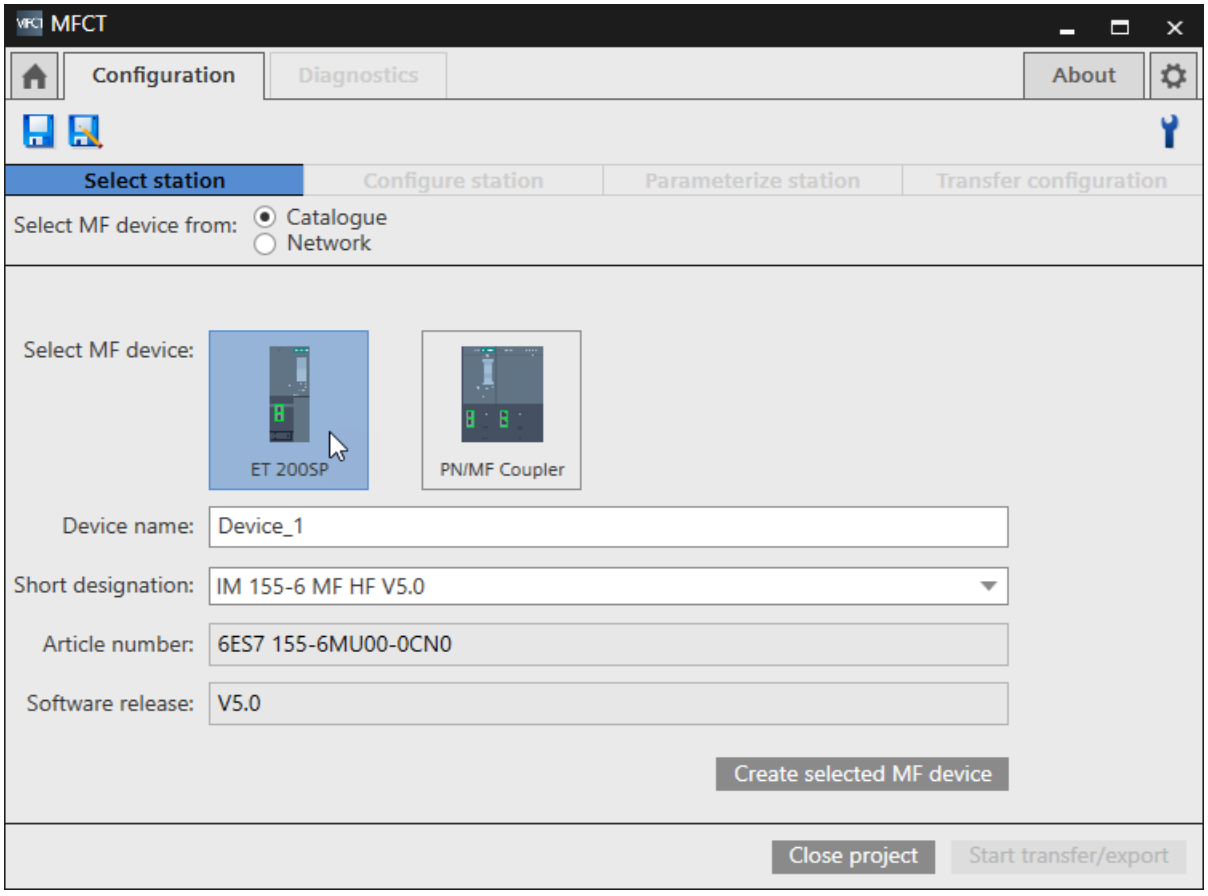
You can create the configuration of the MF device in two ways:

- From the catalog if the real MF station is not available.
- From the network if the MF station is available online.

Selecting MF device from the catalog

1. Select the "Catalogue" option under "Select MF device from".
2. Under "Select MF device", select the desired MF device, e.g. ET 200SP.
3. Assign a name for the MF device under "Device name".
4. Select the desired interface module under "Short designation".
5. Click on the "Create Selected MF Device" button.

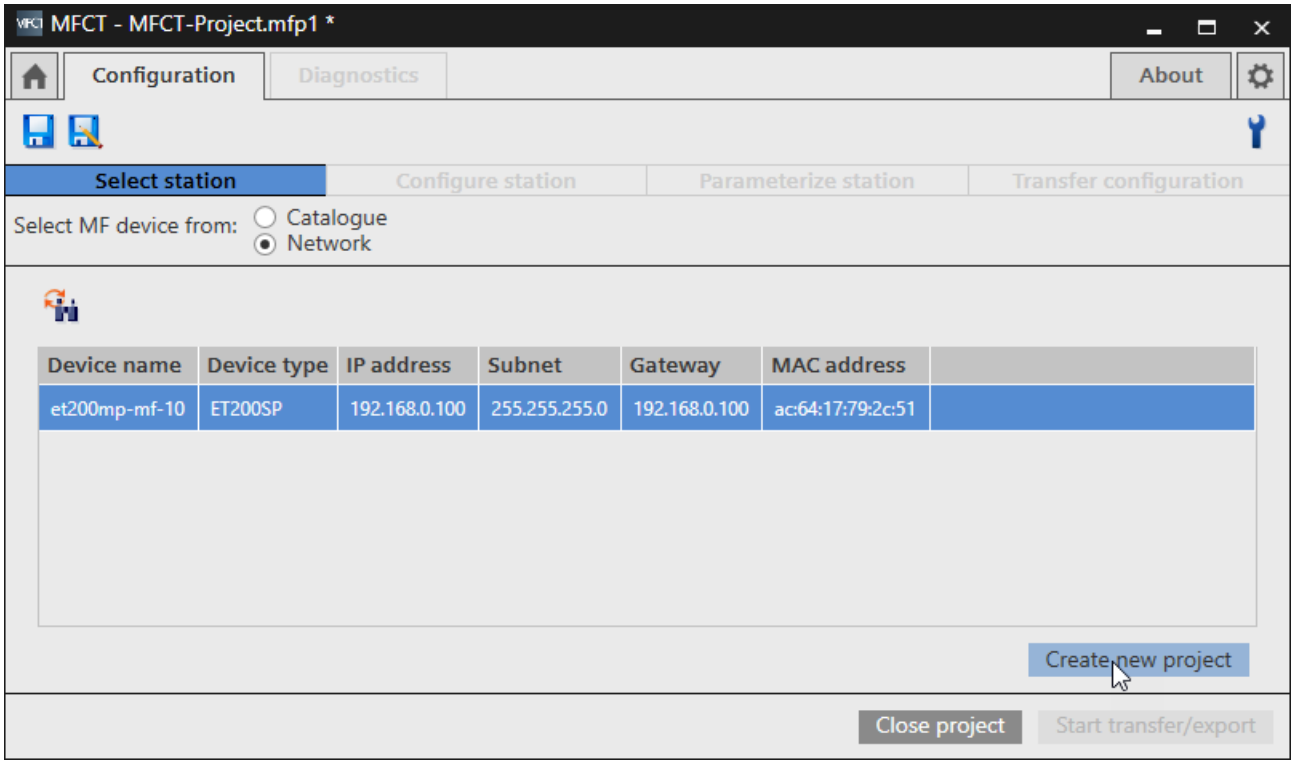
The MFCT automatically goes to the next step, "Configure Station".



Selecting MF device from the network and loading the configuration

1. Ensure that the network interface selected in the "Settings" tab is connected to the desired MF device.
2. Select the "Network" option under "Select MF device from".
3. Click "Start scan".
4. Select the desired MF device from the list. Devices without MultiFieldbus support cannot be selected and are grayed out.
5. Click "Create new project".

The current configuration is read out from the MF device and added to the MultiFieldbus project. MFCT then goes to the next step "Configure Station" for review and editing.



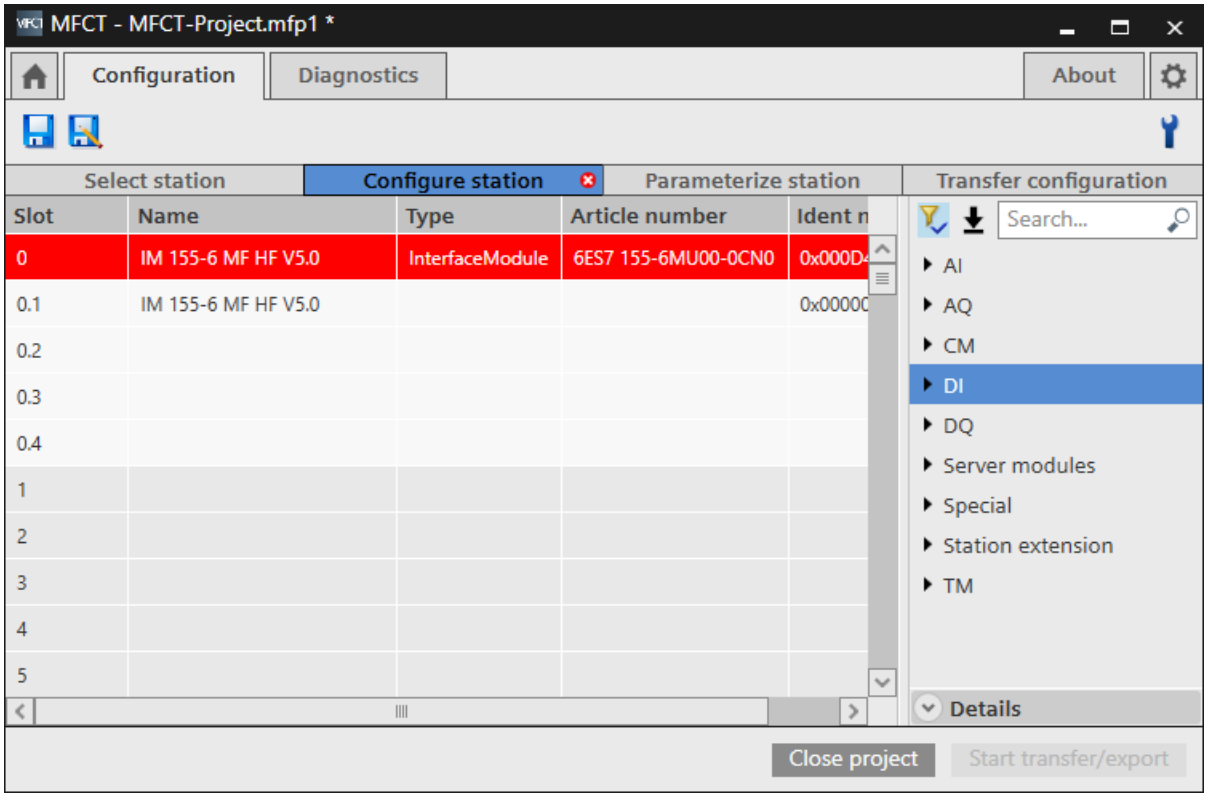
4.2.2.8 Configuring a station

Under "Configure Station", assemble the station with modules and submodules from the hardware catalog based on the GSDML.

The composition of the station is shown as a list on the left, sorted in ascending slot order. The modules and submodules of the hardware catalog based on the installed GSDML are shown on the right.

Additional information on the selected module and potential application at the fieldbuses is shown below the hardware catalog in the "Details" area.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

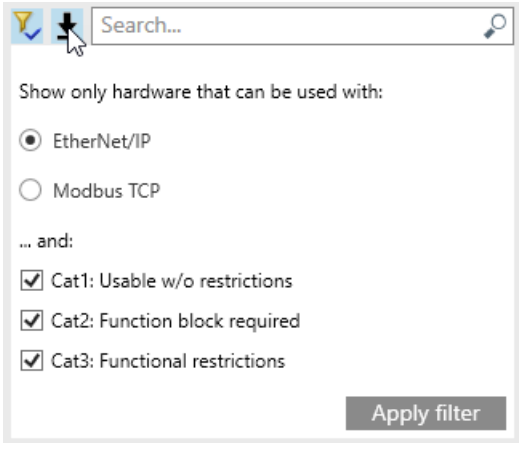


Filter function

You use the filter function to restrict the hardware catalog depending on the fieldbus and the category.

To activate the filter function, follow these steps:

1. Expand the list with the filter criteria.



2. Select the desired fieldbus.

3. Select the desired categories.
4. Activate the filter function using the "Apply filter" button.

To deactivate the filter function, follow these steps:

1. Click the filter icon.



Selecting modules

1. Select the module in the desired version and operating mode from the catalog for each slot and drag it onto the slot.

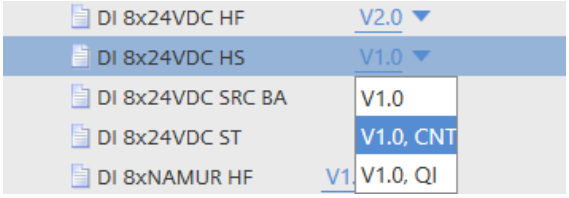
NOTE
The possible slots for the selected module are highlighted in green.

2. Finally, add a server module.

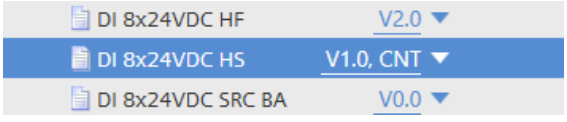
NOTE
The MF device is highlighted in red until you have added the server module.

Selecting submodules

1. Select one of the available submodules from the drop-down list of the module in the hardware catalog.



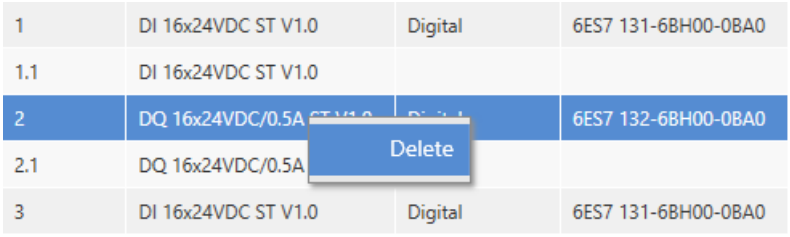
2. Select the submodule and drag it onto a slot.



NOTE
The possible submodule slots are highlighted in green.

Deleting modules/submodules

1. Select the module/submodule to be deleted.
2. Click "Delete" in the shortcut menu.



4.2.2.9 Parameter assignment of the station

Under "Assign Station Parameters", set the parameters of the previously configured station.

The composition of the station is shown as a list on the left, sorted in ascending slot order. The parameters for the MF device and the modules/submodules are shown on the right.

For MF devices that support the "MF Shared Device" function, you can configure various fieldbuses for the MF device and for each module.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

Procedure

1. Select the MF device on slot 0.
2. If the MF device supports the "MF Shared Device" function and you want to configure different fieldbuses for the MF device and the modules, activate the "MF Shared Device" parameter on the right under "Multi fieldbus parameters".



3. Select the desired fieldbus for the MF device under "Multi fieldbus connection".
4. Use the "I/O data alignment" parameter to select "Byte" or "Word" for I/O data mapping (Page 82).
5. Under "MultiFeldbus Modbus TCP", you can set for each Modbus TCP connection separately the hold time for the connection and the time for "Hold time after connection reset" from 1 to 30,000 ms.

   This parameter is not relevant for EtherNet/IP.
6. Assign parameters for the remaining modules and submodules by selecting the slot and setting the parameter values on the right side.
7. When you have activated the "MF Shared Device" parameter, you can select a fieldbus for each module under "MultiFieldbus connection".

Slot	Name	Type	Article number	Fieldbus connection
0	IM 155-6 MF HF V5.2	InterfaceModule	6ES7 155-6MU00-0CN0	PROFINET
0.1	IM 155-6 MF HF V5.2			
0.1				
0.2				
0.3				
1	DI 16x24VDC ST V0.0	Digital	6ES7 131-6BH01-0BA0	EtherNet/IP #0 (0x301, 0x300)
2	DQ 16x24VDC/0.5A BA V0.0	Digital	6ES7 132-6BH00-0AA0	ModbusTCP #0 (0x000, 0x2D0)
3	F-AI 4xU 0..10V HF, XP	FAnalog	6ES7 136-6AB00-0CA1	PROFINET
4	F-DQ 8x24VDC/0.5A PP HF, BP	FDigital	6ES7 136-6DC00-0CA0	PROFINET
5	Server module V1.2 (0 bytes)	ServerModule	6ES7 193-6PA00-0AA0	PROFINET

NOTE

A parameterization error can be displayed during reconfiguration of PROFINET to EtherNet/IP or Modbus TCP in connection with changing the BusAdapter type. You can only remedy the parameterization error with a reset to factory settings (Page 66) and reconfiguration with MFCT.

4.2.2.10 Transfer the configuration

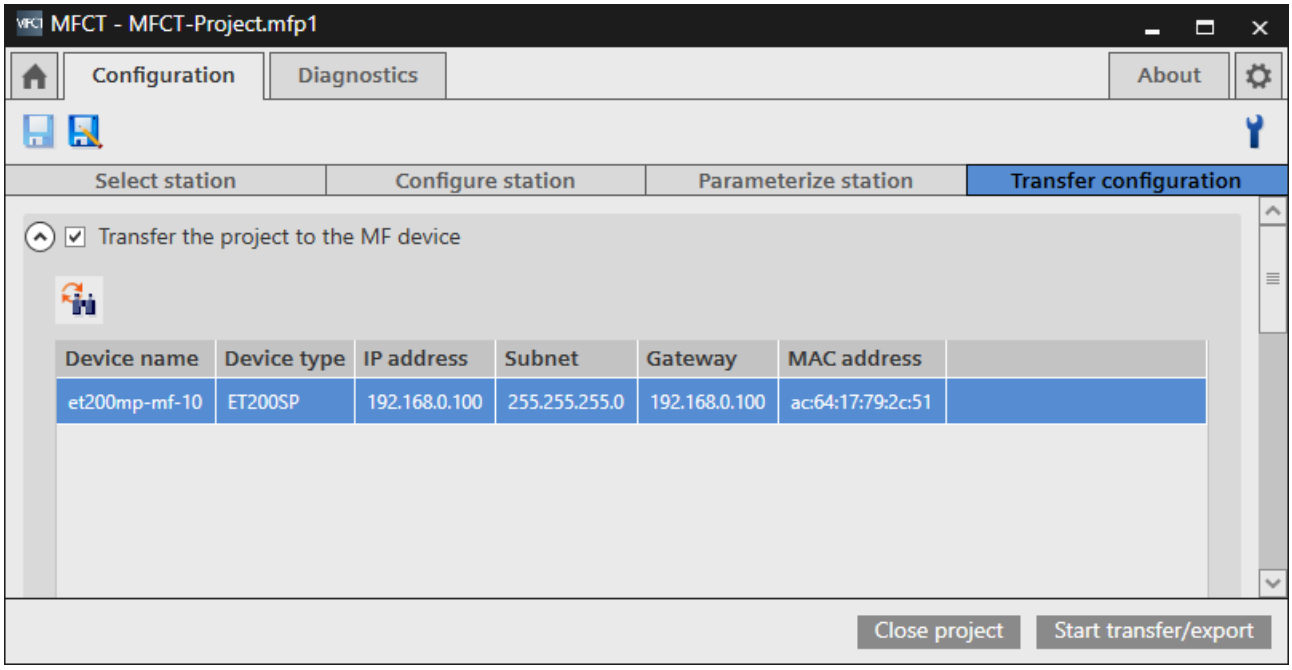
The "Transfer configuration" area offers you the following options:

- Transfer the project to the MF device
- Export the configuration for use in other engineering tools.

Transferring the project to the MF device

To transfer the MF project to the MF device, follow these steps:

1. Select the "Transfer the project to the MF device" check box.
2. Click the "Start scan" button to search via the preset network interface for MF devices for the project download. Devices without MultiFeldbus support cannot be selected and are grayed out.
3. Select an MF device and start the download to the MF device using the "Start transfer/export" button.

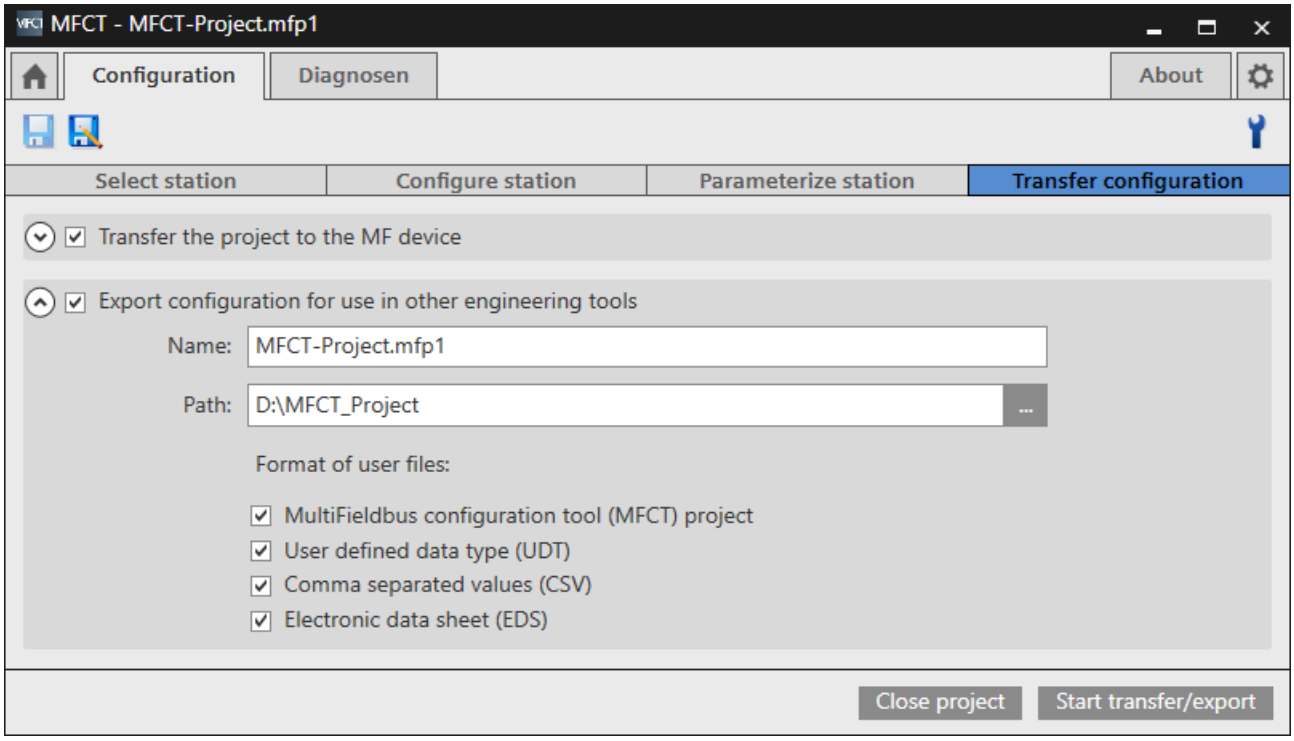


Fault rectification of the timeout on transfer to the MF device

- Check the accessibility of the MF device via the network interface selected in MFCT.
- Disconnect the connection of the MF device to PROFINET IO controllers.
- If you have selected the "Use router for gateway" option in the network parameters, check the network parameters of the device.

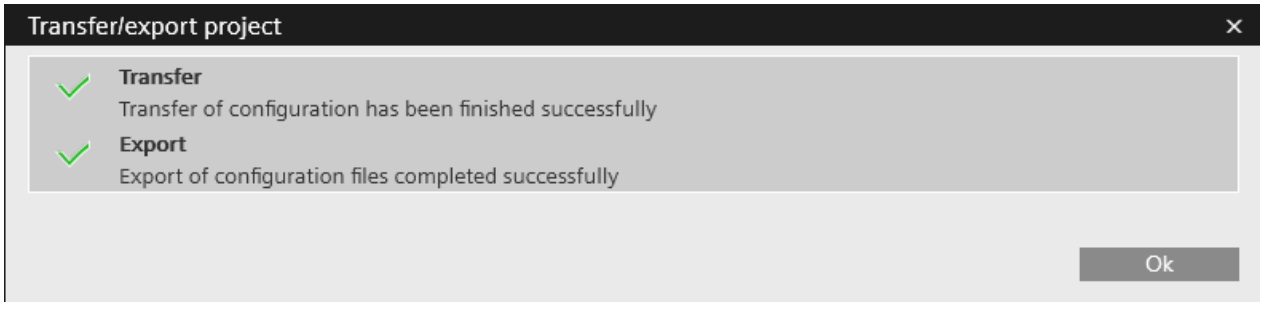
Export of configuration

1. Select the "Export configuration for use in other engineering tools" check box.
2. Assign a name and a path for the export
3. Select the file formats to be exported:
   - MultiFieldbus Configuration Tool (MFCT) project
   - User Defined Data Type (UDT) (as I5x file)
   - Comma Separated Values (CSV)
   - Electronic Data Sheet (EDS)
4. Start the export using the "Start transfer/export" button.



Transfer/export status

The progress and result of the file export and project download are each displayed. The fieldbus activated in the MF device as well as any differences between the configured and real hardware are also displayed.



4.2.2.11 Sending user feedback

You have the option of sending us feedback on MFCT in the "About" tab:

1. Click on the "Send feedback" button.
   MFCT collects diagnostics data and attaches it to the open email.
2. Enter your feedback on MFCT in the email.
3. Send the email.



4.2.3 Configuration in the engineering system

4.2.3.1 Services

The following Modbus TCP services are supported:

- Read Holding Registers (code = 3)
- Write Multiple Registers (code = 16)

4.2.3.2 Register addresses

Overview of the Modbus TCP registers

Consistent access to register:

- Function Code 3:
  Read inputs via 2 parallel connections of a controller: Up to 2 x 125 registers at 16 bits = 2 to 500 bytes
- Function Code 16:
  Write outputs via a controller: 1 to 123 registers at 16 bit = 2 to 246 bytes

Partial writing of the output data or reading of the input data within the configured total length is possible.

The table below shows the overview of the available Modbus TCP registers:

Register area	Address [Hex]	Address [Decimal]	RegLayoutVersion
I/O data of the connection	0x0000 - 0x59FF	0 - 23039	≥ V1.0
Module status	0x6000 - 0x69E3	24576 - 27107	≥ V1.1
Data record	0xD000 - 0xD0FA	53248 - 53498	≥ V1.1
Volatile registers	0xFE00 - 0xFE7C	65024 - 65148	≥ V1.0
Deviceinfo	0xFF00 - 0xFF08	65280 - 65288	≥ V1.0

Input/output data of the connection

The following table shows the valid ranges for register addresses:

Connection ID	Input data (with FC3)		Output data (with FC16)	
	Register addresses [Hex]	Register addresses [Decimal]	Register addresses [Hex]	Register addresses [Decimal]
0	0x0000 - 0x00F9	0 - 249	0x02D0 - 0x034A	720 - 842
1	0x05A0 - 0x0699	1440 - 1689	0x0870 - 0x08EA	2160 - 2282
2	0x0B40 - 0x0C39	2880 - 3129	0x0E10 - 0x0E8A	3600 - 3722
3	0x10E0 - 0x11D9	4320 - 4569	0x13B0 - 0x142A	5040 - 5162
4	0x1680 - 0x1779	5760 - 6009	0x1950 - 0x19CA	6480 - 6602
5	0x1C20 - 0x1D19	7200 - 7449	0x1EF0 - 0x1F6A	7920 - 8042
6	0x21C0 - 0x22B9	8640 - 8889	0x2490 - 0x250A	9360 - 9482
7	0x2760 - 0x2859	10080 - 10329	0x2A30 - 0x2AAA	10800 - 10922
8	0x2D00 - 0x2DF9	11520 - 11769	0x2FD0 - 0x304A	12240 - 12362
9	0x32A0 - 0x3399	12960 - 13209	0x3570 - 0x35EA	13680 - 13802

Bit-by-bit access to cyclic I/O data

The input and output functions work for one connection in the same bit address area.

You can access up to 500 bytes of input data and 246 bytes of output data with 16 connections.

Simultaneous bit-by-bit access with the function codes 1, 2, 5, 15 and register access with the function codes 3, 16 are possible.

Connection		Function codes (FC)	
ID	Bit address	Access to input data	Access to output data
0	0x0000 – 0x0FFF	Max. 500 bytes per connection FC2 (read individual input)	Max. 246 bytes per connection FC1 (read coil) FC5 (write individual coil) FC15 (write multiple coils)
1	0x1000 – 0x1FFF		
2	0x2000 – 0x2FFF		
...	...		
8	0x8000 – 0x8FFF		
9	0x9000 – 0x9FFF		

NOTE

Bit access takes place for input and output data in the same address area within a connection.

Module status area

This area contains detailed information on modules and submodules that were configured for Modbus TCP. The area contains submodule-specific status information for up to 281 submodules.

A summary of the complete configuration is available in the *DeviceStatus* field of the Device-Info area. *RealModuleIdent* and *RealSubmoduleIdent* return 0 if a submodule is not plugged and *SubmoduleState* shows "No submodule".

Table 3-72 Module status area (big-endian, read-only access)

Register	Block	Field	Size	Description
0x6000 (24576)	Block Header	VersionHigh	Unsigned8	0x01 Major revision module status
		VersionLow	Unsigned8	0x00 Minor revision module status
0x6001 (24577)		BlockLength	Unsigned16	Number of subsequent elements for the module status area as Word
0x6002 (24578)	Submod #0	Slot	Unsigned8	Slot number of the module
		Subslot	Unsigned8	Subslot number of the submodule
0x6003 (24579)		ExpectedModuleIdent	Unsigned16	High Word expected ModuleIdentNumber
0x6004 (24580)			Unsigned16	Low Word expected ModuleIdentNumber
0x6005 (24581)		ExpectedSubmod-uleIdent	Unsigned16	High Word expected SubmodIdentNumber
0x6006 (24582)			Unsigned16	Low Word expected SubmodIdentNumber
0x6007 (24583)		RealModuleIdent	Unsigned16	High Word actual ModuleIdentNumber

Register	Block	Field	Size	Description
0x6008 (24584)	Submod #0	RealModuleIdent	Unsigned16	Low Word actual ModuleIdentNumber
0x6009 (24585)		RealSubmoduleIdent	Unsigned16	High Word actual SubmoduleIdentNumber
0x600A (24586)			Unsigned16	Low Word actual SubmoduleIdentNumber
0x600B (24587)		SubmoduleState	Unsigned16	Bits 3..0: Configuration status 0 = OK 1 = Substitute submodule 2 = Wrong submodule 3 = No submodule 4..15 = Reserved Bit 4 = Error diagnostics Bit 5 = Maintenance diagnostics Bits 15..6: Reserved (0)
...	...			
0x69DA (27098) - 0x69E3 (27107)	Submod #280			

Volatile register area

This area provides 123 multi-purpose registers with read/write access for customized use.

The registers can be controlled by any Modbus TCP connection. The content of the volatile registers is stored non-retentively in the RAM of the MF device. The content is set to 0 when the device is switched off and on again.

Table 3-73 Volatile register area (big-endian, read/write access)

Register	Field	Size	Default	Description
0xFE00 (65024)	VersionHigh	Unsigned8	0x01	Major revision of the volatile registers (Read access)
	VersionLow	Unsigned8	0x00	Minor revision of the volatile registers (Read access)
0xFE01 (65025)	BlockLength	Unsigned16	0x007B	Number of volatile registers (Read access)
0xFE02 (65026)	VolatileReg0	Unsigned16	0x0000	
...	...			
0xFE7C (65148)	VolatileReg122	Unsigned16	0x0000	

Device-Info Area

This register area provides read access to revision and status information.
The following table shows the register addresses:

Table 3-74 Device-Info area (big-endian, read-only access)

Register	Field	Size	Default	Description
0xFF00 (65280)	VersionHigh	Unsigned8	0x01	Major revision of the Deviceinfo
	VersionLow	Unsigned8	0x01	Minor revision of the Deviceinfo
0xFF01 (65281)	BlockLength	Unsigned16	0x0008	Number of subsequent elements for the Deviceinfo area in Word
0xFF02 (65282)	RegLayoutVersionHigh	Unsigned8	0x01	Major revision of the layout of the Modbus TCP register
	RegLayoutVersionLow	Unsigned8	0x01	Minor revision of the layout of the Modbus TCP register
0xFF03 (65283)	IOLayoutVersionHigh	Unsigned8	0x01	Major revision of the layout of the I/O data area
	IOLayoutVersionLow	Unsigned8	0x00	Minor revision of the layout of the I/O data area
0xFF04 (65284)	FirmwareVersionMajor	Unsigned8	-	Depending on firmware revision Vx.y.z Major = x*10+y / Minor = z
	FirmwareVersionMinor	Unsigned8	-	
0xFF05 (65285)	ProductCode	Unsigned16	-	You can find the data value in the technical specifications of the MF device under "Device ID according to ODVA (ProductCode)".
0xFF06 (65286)	SerialNumber	Unsigned8	-	Last 4 bytes of the MAC address of the MF device
		Unsigned8	-	
0xFF07 (65287)		Unsigned8	-	
		Unsigned8	-	
0xFF08 (65288)	DeviceStatus	Unsigned16	0x0000	Bits: 0 = Configured (MultiFieldbus project with Modbus TCP modules) 1 = Connected to a Modbus TCP client 2 = Diagnostics error 3 = Maintenance diagnostics 4 = Configuration error (no module or wrong module)
0xFF09 (65289)	RecordAreaVersion-High	Unsigned8	0x01	Revision Major from *Record Register Area*
	RecordAreaVersionLow	Unsigned8	0x00	Revision Minor from *Record Register Area*

4.2.3.3 Behavior of the inputs and outputs

The following section describes how the inputs and outputs of modules behave during the use of Modbus TCP.

- Outputs return substitute values after:
  - POWER ON, if a retentive project download is present
  - Change of the configuration/parameter assignment via MFCT download
  - Interruption of the Ethernet connection longer than the Modbus hold time
  - STOP of the Modbus TCP controller
  - Register access to the output area in a cycle greater than the Modbus hold time
- Outputs return "0":
  - For POWER ON if no project download is present
  - For unwritten output registers after POWER ON or after substitute value output initiated by any write access to the output register area
  - For unwritten I/O registers
- Outputs return the last written values:
  - For output registers other than those addressed in the write access
- Outputs return current values:
  - At a write access to the affected output registers
- Inputs deliver values depending on the module status for configuration, parameter assignment and error modes
  - At a read access to the affected input registers

NOTE
If you have only configured inputs, read these within the configured Modbus hold time to prevent the LED display for timeout.
If you have configured outputs, write these within the configured Modbus hold time to prevent the LED display for timeout and receive the device status = 1 (Connected).

4.2.3.4 I/O data mapping

I/O data mapping

During parameter assignment of the MF Device (Page 73), you can choose between two formats for the I/O data alignment:

- With the "Byte" format, the input or output data of the modules of an I/O connection are lined up by increasing slot address (Slot.Subslot).
- With the "Word" format, the input or output data of the modules of an I/O connection are lined up by increasing slot address (Slot.Subslot). If the submodule has an odd-numbered data length (e.g. data length of 1 for a DI 8 HF module), a padding byte (content 0x00) is inserted after the submodule. This aligns the following data status bytes (IDS, ODS) to word limits. A padding byte (content 0x00) is also inserted after the data status byte (IDS, ODS). Subsequent submodules will then also start at an even byte offset.

The image of the outputs contains only the output data (with padding bytes if necessary), while the input image also supplies additional status bytes together with the input data (with padding bytes if necessary).

An Output Data Status Byte (ODS) is available for each output submodule in the image of the inputs.

There is an Input Data Status Byte (IDS) for each input submodule that follows the respective input data of the submodule in the input image.

Submodules with a data length of 0 for input and output data are treated as input submodules. Only an Input Data Status Byte (IDS) is entered in the input image.

NOTE

You can find the I/O data mapping for your configuration in the exported CSV file (Page 74).

NOTE

For information about data mapping, see the system and equipment manuals.

I/O data status

The following table shows the coding of the status bytes for IDS and ODS:

Field	Bit number	Bit mask	Default	Bit value = '0'	Bit value = '1'
IOValid	7	0x80	0	I/O data invalid	I/O data valid
Problem	6	0x40	0	Initial status	Module problem: • Module not plugged • Incorrect module plugged • Module with incorrect parameter assignment
NoCoupling	5	0x20	0	Initial status	No I/O data from coupling partner (MSO Local)
Reserved	4...2	0x1E	000	-	
ProcessEvent	1	0x02	0	No process event	Process event available
Diagnosis	0	0x01	0	No diagnostics	Diagnostics available

4.2.3.5 Data record interface

Overview

Via this Modbus TCP interface, you can access configured modules in the form of PROFINET data records for reading and writing.

Examples for this are

- Write/read I&M data
- Read diagnostic data
- Write parameter data records
- Read measured value data records

Information on parameter data records, measured value data records and diagnostics can be found in the device manuals of the modules used.

Access to the register areas of the data record interface is exclusively provided via the services Write Multiple Registers (Code=16) and Read Holding Registers (Code=3).

Modbus TCP limits the data that can be consistently transferred to 246 bytes Write (123 registers) and 246 bytes Read (123 registers). Larger data records are provided in an internal intermediate buffer and are read or written via Modbus TCP through multiple record requests. It can be used to transfer PROFINET data records with a maximum length of 4096 bytes.

The data record interface and the protocol are described below.

User interface

Table 3-75 Register area for data records

Connection	Block		Register address	Access
#0	Record Register Area0	0xD000 - 0xD0FA		
		Record request	0xD000 - 0xD006	Read/write
		Record response	0xD040 - 0xD042	Read only
		Record Data	0xD080 - 0xD0FA	Read/write
#1	Record Register Area1	0xD100 - 0xD1FA		
...				
#9	Record Register Area9	0xD900 - 0xD9FA		

Table 3-76 Record request (big-endian, read/write access)

Register Offset	Block	Field	Size	Description
0x0000	Record Header	Slot	Unsigned16	
0x0001		Subslot	Unsigned16	
0x0002		Record Index	Unsigned16	
0x0003		Record Length	Unsigned16	Length of the PROFINET data record in bytes
0x0004	Request Header	Request Offset	Unsigned16	Offset within the PROFINET data record in bytes
0x0005		Request Length	Unsigned16	Number of bytes requested for the *Record Data* register, in the data record starting at *Read Request Offset*. > 246 returns the Modbus TCP error "Illegal Data Value (3)".
0x0006	Request Trigger	Request Control		**0x0000 Execute read:** Fetch new internal data record (record header & request header are evaluated) **0x0001 Resume read:** Returns another data packet of a previously internally requested data record. (Returns the Modbus TCP error "Illegal Data Value (3)", if the content of the *Record Header* has changed since the last execution.) **0x0002 Prepare write:** Fill internal write buffer, but without executing the write request of the data record internally. **0x0003 Execute write:** Fill internal write buffer and execute internal writing of the data record. (Returns the Modbus TCP error "Illegal Data Value (3)", if the content of the *Record Header* has changed since the last execution.) **0x0004 – 0xFFFF:** Reserved (Returns the Modbus TCP error "Illegal Data Value (3)")

Table 3-77 Record response (big-endian, read-only access)

Register Offset	Block	Field	Size	Description
0x0040		Status	Unsigned16	**0x0000:** Done / OK (request was successfully executed.) **0x0001:** Busy (access to the data record interface not allowed.) **0x0002:** Waiting (for **"Execute write"**) **0x0003:** Processing (internal request of the data record is executed) **0x8000-0x80FF:** Error (request failed with the PROFINET data record error response [2])(= 0x8000 + "PROFINET ErrorCode1" column in Param Object/Response-Record-Mapping (Page 58)) **0xFF00:** *Request Length* invalid (> 246 returns the Modbus TCP error "Illegal Data Value (3)") **0xFF01:** *Record Length* invalid (if == 0) **0xFF02:** Request header invalid (if *Request Offset* + *Request Length* > *Record Length*)
0x0041		Processed Length	Unsigned16	Processed length of the PROFINET data record in bytes **Read:** Length of the read PROFINET data record. **Write:** Record length of the executed write job = Record Length (Zero in case of an error)
0x0042		Response Length	Unsigned16	**Read:** Number of valid bytes available in *Record Data*. **Write:** Number of bytes taken from *Record Data*. (Zero in case of an error)

Table 3-78 Record content (big-endian, read/write access)

Register Offset	Block	Field	Size	Description
0x0080-0x00FA	Record	Data [123]	Unsigned16	PROFINET data record content (246 bytes) (Read: Contains the number of valid bytes returned with *Response Length*. Remaining bytes have the value 0.)

Read data record

Proceed as follows to read a PROFINET data record:

1. Write *Record Header* and *Request Header* in the *Record Request* register structure.

   It is important that you first write all information into the *Record Request* register structure before you write the *Request Control* register.
2. Write 0x0000 in *Request Control* to trigger the reading of the PROFINET data record. Write *Request Control* only once until reading is complete.
3. Read the *Record Response* structure and poll *Status* to detect the completion of the internal read request for the PROFINET data record.
4. You can use *Status* == 0x0000 (OK) to read the *Record Data* registers with the contents of the PROFINET data record.
5. If *Processed Length* > *Response Length*, further data of the PROFINET data record are available for reading.

   In this case, continue with step 1. Set *Request Offset* = *Request Offset* + *Response Length* and *Request Control* = 0x0001 to request further data of the PROFINET data record from the internal *PROFINET Record Data Buffer*.

Write data record

Proceed as follows to write a PROFINET data record:

1. Write the first 123 registers (246 bytes) of the PROFINET data record to the *Record Data* registers. If the data record > 246 bytes; otherwise less, depending to the data record.
2. Write *Record Header* and *Request Header* in the *Record Request* register structure.
   It is important that you first write all information into the *Record Request* register structure before you write the *Request Control* register.
3. For a data record >= 246 0x0002, write in *Request Control* to write the first 123 registers (246 bytes) to an internal write buffer. Otherwise, continue with step 6.
4. Wait until writing is complete. To do so, evaluate *Response Length*. When *Response Length* is equal to the number of the first 123 registers (246 bytes), writing is complete.
5. Write the next register of the PROFINET data record to the *Record Data* registers. Write the number of previously written registers (246 bytes) to *Request Offset*.
6. Write 0x0003 in *Request Control* to write the next registers to the internal write buffer and execute the data record task.
   Do not change the address information for previous access.
7. Wait until writing is complete. To do so, evaluate *Response Length*. When *Response Length* is equal to the number of the next written registers, writing is complete.
8. Read the *Record Response* structure and poll *Response Status*.
   - If *Response Status* == 0x0000, the internal write operation for the PROFINET data record has been successfully completed. You can use *Processed Length* and *Response Length* to evaluate the resulting length information.
   - With *Response Status* == 0x0002 the write request of the current data block is completed and *Record Data* was filled into the *PROFINET Record Data Buffer*.

   To write another data block, continue with step 1.

If the PROFINET data record is only up to 123 registers (246 bytes) long, skip steps 3 to 5.

Example: Read I&M0 data

To read I&M0 data from an interface module with Modbus TCP connection #0, proceed as follows:

1. Check the revision of the Modbus TCP data record interface.

Read 0xFF09 (Record Area Version)	=> 0x0100 (1.0)

   Check if you have implemented the correct address scheme (e.g. 0x0100 = V1.0)
2. Prepare request to read the data record.

Write 0xD000 (Slot) = 0x0000	IM slot = 0 in connection #0 of 0xD000
Write 0xD001 (Subslot) = 0x0001	IM subslot = 1
Write 0xD002 (Record Index) = 0xAFF0	I&M0
Write 0xD003 (Record Length) = 0x003C	Read 60 bytes from I&M0 data record
Write 0xD004 (Request Offset) = 0x0000	Request data from offset 0 from I&M0 data record
Write 0xD005 (Request Length) = 0x003C	Request 60 bytes of data from the I&M0 data record

3. Execute the read request.

Write 0xD006 (Request Control) = 0x0000	Starts the internal retrieval of data from the I&M0 record.

4. Wait until the read request is completed.

Read 0xD040 (Status)	Poll status <> 0x0001= Busy or 0x0003 = Processing

5. Evaluate the result of the reading.

When status <> 0x0000 (OK), evaluate the error code.	→ 0x80xx = Normative PROFINET error response code → 0xFFxx = Request parameter error
Read 0xD041 (Processed Length) => 0x003C	60 bytes is the total length of the I&M0 record
Read 0xD042 (Response Length) => 0x003C	60 bytes were returned from the current read request

6. Read the data of the I&M0 record.

Read 0xD080 - 0xD09E (Record Data [0-29])	Read 60 bytes of data of the I&M0 data record

Example: Write I&M1 data

To write I&M1 data to a module with Modbus TCP connection #1, proceed as follows:

1. Check the revision of the Modbus TCP data record interface.

Read 0xFF09 (Record Area Version)	=> 0x0100 (1.0)

Check if you have implemented the correct address scheme (e.g. 0x0100 = V1.0)

2. Fill the data for the PROFINET data record.

Write 0xD180 - 0xD19E (Record Data [0-29])	Write 60 bytes of data of the I&M1 data record

3. Prepare the request to write the record.

Write 0xD100 (Slot) = 0x0002	Slot = 2 in connection #1 of 0xD100
Write 0xD101 (Subslot) = 0x0001	Subslot = 1
Write 0xD102 (Record Index) = 0xAFF1	I&M1
Write 0xD103 (Record Length) = 0x003C	60 bytes total length for the I&M1 data record
Write 0xD104 (Request Offset) = 0x0000	Request to fill the data of offset 0 from the I&M1 data record to
Write 0xD105 (Request Length) = 0x003C	Request to write 60 bytes of data into the I&M1 data record

4. Execute the read request.

Write 0xD106 (Request Control) = 0x0003	Starts the internal retrieval of data from the I&M1 data record.

5. Wait until the write request is completed.

Read 0xD140 (Status)	Poll status <> 0x0001= Busy or 0x0003 = Processing

6. Evaluate the result of the writing.

When status <> 0x0000 (OK), evaluate the error code.	→ 0x80xx = Normative PROFINET error response code → 0xFFxx = Request parameter error
Read 0xD141 (Processed Length) => 0x003C	60 bytes is the total length of the I&M1 record
Read 0xD142 (Response Length) => 0x003C	60 bytes written with the current write request

Example: Read diagnostics (multiple data packets)

To read diagnostic data (0x800C) from a module with Modbus TCP connection #0, proceed as follows:

1. Check the revision of the Modbus TCP data record interface.

Read 0xFF09 (Record Area Version)	=> 0x0100 (1.0)

Check if you have implemented the correct address scheme (e.g. 0x0100 = V1.0).

2. Prepare request to read the first data packet of the diagnostic data record.

Write 0xD000 (Slot) = 0x0002	Slot=2 in connection #0 of 0xD000
Write 0xD001 (Subslot) = 0x0001	Subslot=1
Write 0xD002 (Record Index) = 0x800C	Diagnostics data
Write 0xD003 (Record Length) = 0x1000	Read 4096 bytes data of the diagnostic data record
Write 0xD004 (Request Offset) = 0x0000	Request data from offset 0 of the diagnostic data record
Write 0xD005 (Request Length) = 0x00F6	Request a data packet with the first 246 bytes of the diagnostic data record.
Write 0xD006 (Request Control) = **0x0000**	Starts the internal fetch of the data package from the diagnostic data record.

3. Wait until the read request is completed and evaluate the result.

Read 0xD040 (Status)	Poll status <> 0x0001= Busy or 0x0003 = Processing
When status <> 0x0000 (OK), evaluate the error code.	→ 0x80xx = Normative PROFINET error response code → 0xFFxx = Request parameter error
Read 0xD041 (Processed Length) => 0x0190	For example, 400 bytes is the total length of the diagnostic data record
Read 0xD042 (Response Length) => 0x00F6	246 bytes were returned by the first read request

4. Read first data packet of the diagnostic data record.

Read 0xD080 - 0xD0FA (Record Data [0-122])	Read 246 bytes of data [0-245] of the diagnostic data record

5. Prepare request to read the second data packet of the diagnostic data record.

Write 0xD004 (Request Offset) = 0x00F6	Request data of offset 246 of the diagnostic data record
Write 0xD005 (Request Length) = 0x009A	Request a data packet with the remaining 154 bytes of the diagnostic data record.
Write 0xD006 (Request Control) = **0x0001**	Provides the previously requested data.

6. Wait until the second read request is completed and evaluate the result.

Read 0xD040 (Status)	Poll status <> 0x0001= Busy or 0x0003 = Processing
When status <> 0x0000 (OK), evaluate the error code.	→ 0x80xx = Normative PROFINET error response code → 0xFFxx = Request parameter error
Read 0xD041 (Processed Length) => 0x0190	400 bytes is the total length of the diagnostic data record
Read 0xD042 (Response Length) => 0x009A	154 bytes were returned by the second read request

7. Read second data packet of the diagnostic data record.

Read 0xD080 - 0xD0CA (Record Data [0-76])	Read 154 bytes of data [246-399] of the diagnostic data record

Example: Write parameter data record (multiple data packets)

To write a parameter data record to an AI Energy Meter module with Modbus TCP connection #0, proceed as follows:

1. Check the revision of the Modbus TCP data record interface.

Read 0xFF09 (Record Area Version)	=> 0x0100 (1.0)

Check if you have implemented the correct address scheme (e.g. 0x0100 = V1.0)

2. Fill the first data packet for the parameter data record.

Write 0xD080 - 0xD0FA (Record Data [0-122])	Write 246 bytes of the parameter data record

3. Prepare the request to write the first data packet of the parameter data record.

Write 0xD000 (Slot) = 0x0004	Slot=4 in connection #0 of 0xD100
Write 0xD001 (Subslot) = 0x0001	Subslot=1
Write 0xD002 (Record Index) = 0x0087	Parameter data record
Write 0xD003 (Record Length) = 0x0130	Write 304 bytes data of the parameter data record
Write 0xD004 (Request Offset) = 0x0000	Request to fill the data of offset 0 of the parameter data record
Write 0xD005 (Request Length) = 0x00F6	Request to write the first data packet with 246 bytes of data into the parameter data record.
Write 0xD006 (Request Control) = **0x0002**	Starts the internal writing of the data packet into the diagnostic data record.

4. Wait until the write request is completed and evaluate the result.

Read 0xD040 (Status)	Poll status <> 0x0001= Busy or 0x0003 = Processing
When status <> 0x0000 (OK), evaluate the error code.	→ 0x80xx = Normative PROFINET error response code → 0xFFxx = Request parameter error
Read 0xD041 (Processed Length) => 0x0000	Internal writing of the data packet not yet executed.
Read 0xD042 (Response Length) => 0x00F6	246 bytes were written internally by the first write request.

5. Fill the second data packet for the parameter data record.

Write 0xD080 - 0xD0BA (Record Data [0-28])	Write 58 bytes of the parameter data record [246-303].

6. Prepare request to write the second data packet of the parameter data record.

Write 0xD004 (Request Offset) = 0x00F6	Prepare request to fill the second data packet starting at offset 246 of the parameter data record
Write 0xD005 (Request Length) = 0x003A	Request to write the second data packet with 58 bytes of data into the parameter data record.
Write 0xD006 (Request Control) = **0x0003**	Starts the internal writing of the data packet into the diagnostic data record.

7. Wait until the write request for the second data packet is completed and evaluate the result.

Read 0xD040 (Status)	Poll status <> 0x0001= Busy or 0x0003 = Processing
When status <> 0x0000 (OK), evaluate the error code.	→ 0x80xx = Normative PROFINET error response code → 0xFFxx = Request parameter error
Read 0xD041 (Processed Length) => 0x0130	304 bytes is the total length of the parameter data record.
Read 0xD042 (Response Length) => 0x003A	58 bytes were written internally by the second write request.

4.3 Diagnostics

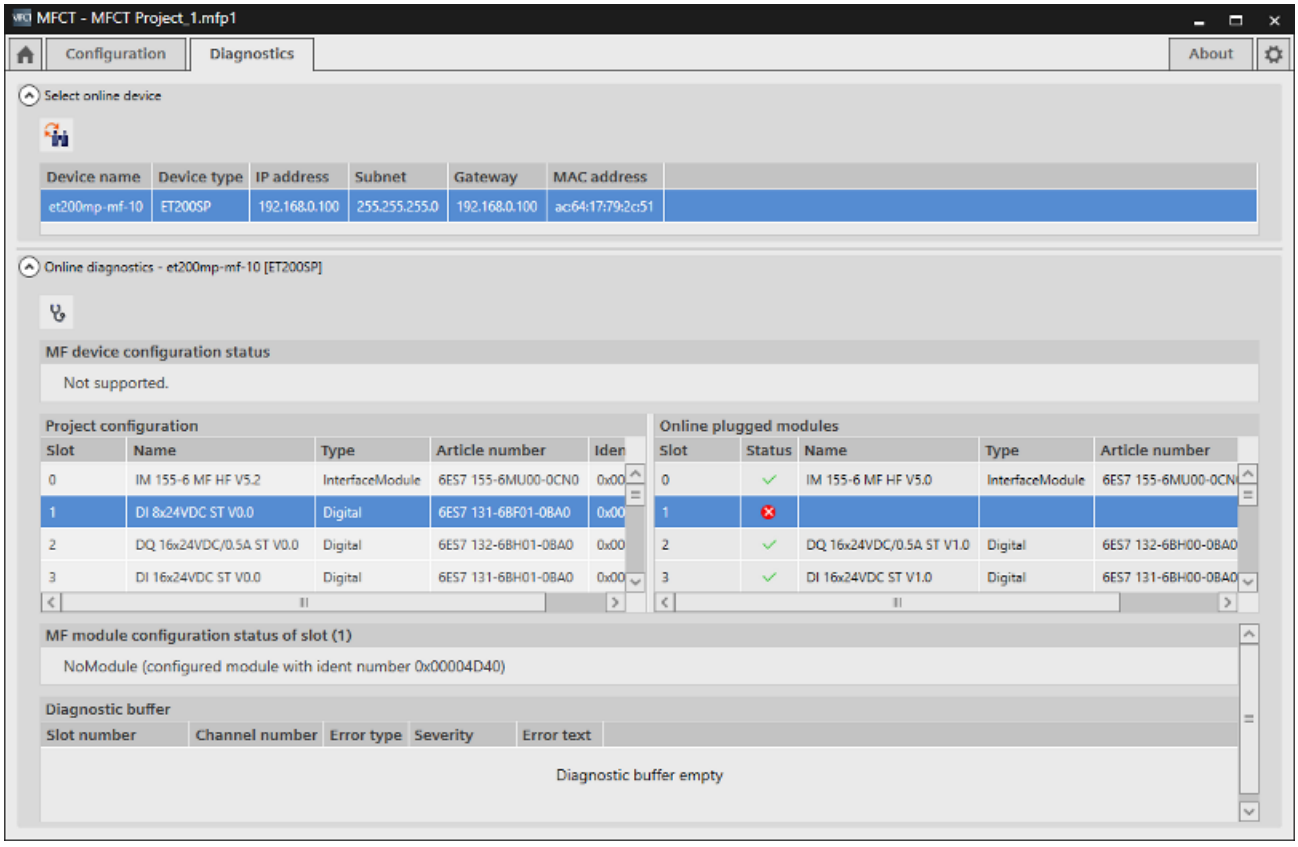
4.3.1 Reading diagnostics with MFCT

In the "Diagnostics" tab, you can read information of selected MF devices:

- The project configuration
- The online plugged modules
- Diagnostics from the diagnostic buffer

Follow these steps:

1. Click the "Start scan" button to find accessible MF devices via the preset network interface.
2. Select an MF device under "Select online device".



You can update the display under "Online plugged modules" with the "Update online status" button.



Project configuration

Under "Project configuration", you will receive information on the configuration of the selected MF device loaded in MFCT.

Online plugged modules

Under "Online plugged modules", you will receive information on the selected MF device, if it is accessible online.

MF module configuration status

Under "MF module configuration status", you can see whether an online plugged module matches the module in the MultiFieldbus project.

Diagnostic buffer

Under "Diagnostic buffer", you can see the content of the diagnostic buffer.

4.3.2 Reading hardware interrupts via event interface

Hardware interrupts are reported on Modbus TCP via the IDS data status and event information. The IDS data status and event information processes the following tasks via acyclic data requests:

- Reading of interrupt information
- Sending of acknowledgements

Notification of hardware interrupts

Field	Bit number	Bit mask	Default	Bit value = '0'	Bit value = '1'
ProcessEvent	1	0x02	0	No process event	Process event available

Reading RALM via the GetAlarmInformation service

A confirmation is made by reading RALM via the GetAlarmInformation service of the event interface. The resulting event data corresponds to the PRAL event information in the table.

Event information (PRAL)			Big Endian	Read access
Byte offset	**Field**	**Size**	**Default**	**Description**
0x0000	VersionHigh	Unsigned8	0x01	Main event of event interface (PRAL)
	VersionLow	Unsigned8	0x00	Sub-event of event interface (PRAL)
0x0002	EventType	Unsigned16	0x0002	PRAL
0x0004	Sequence-Counter	Unsigned16	0x0000	Increases with each event
0x0006	BlockLength	Unsigned16		Number of bytes for the following section
0x0008	USI	Unsigned16		Event structure type
0x000A ... 0x00F5	EventData	Byte [236]		

Data record response for USI 0x0001

The following table explains the data record response structure for USI 0x0001 with a length of 4 bytes.

Bits	Field	Description
16 ... 31	User Structure Identifier (USI)	0x0001
0 ... 1	Event	Event that triggered the hardware interrupt: 0x1: Rising edge 0x2 Falling edge
8 ... 11	Channel	Triggering channel 0x0 ... 0xF

Data record response for USI 0x8320

The following table explains the data record response structure for USI 0x8320 with a length of 14 bytes.

Bits	Field	Description
2 bytes	User Structure Identifier (USI)	0x8320
2 bytes	ChannelNumber	0x8000 (entire submodule)
2 bytes	PRAL_ChannelProperties	Value: 0x0000 Accumulative: 0x00 (individual) Direction: 0x00 (manufacturer-specific)
2 bytes	PRAL_Reason	0x9500 for event code: 0x0000 ... 0x7FFF 0x9501 for event code: 0x8000 ... 0xFFFF
2 bytes	PRAL_ExtReason	0x0001 ... 0x7FFF (event code)
4 bytes	PRAL_ReasonAddValue	0x0000 0000

4.3.3 PULL/PLUG event modbus TCP

The PULL/PLUG event is only supported by the MultiFieldbus IO-Link master.

With a correctly connected and parameterized submodule, the MF IO-Link master makes the configuration and parameterization available to the submodule.

PULL/PLUG event for modbus TCP

The PULL interrupt and PLUG interrupt is communicated to the controller by the data status.

PULL interrupt:
The PULL interrupt is triggered when a parameterized module is pulled. The PULL interrupt is triggered via the problem bit and the diagnostic bit in the data status.

PLUG interrupt:
The PLUG interrupt is triggered if the parameterization in the MF IO-Link master is not identical to the plugged module. The PLUG interrupt is triggered via the problem bit and the diagnostic bit in the data status.

Reset:
If the submodule meets the following properties, the interrupt is reset:

- Correctly connected
- Correctly configured
- Ready for cyclic communication

The following table shows the coding of the status bytes for IDS and ODS:

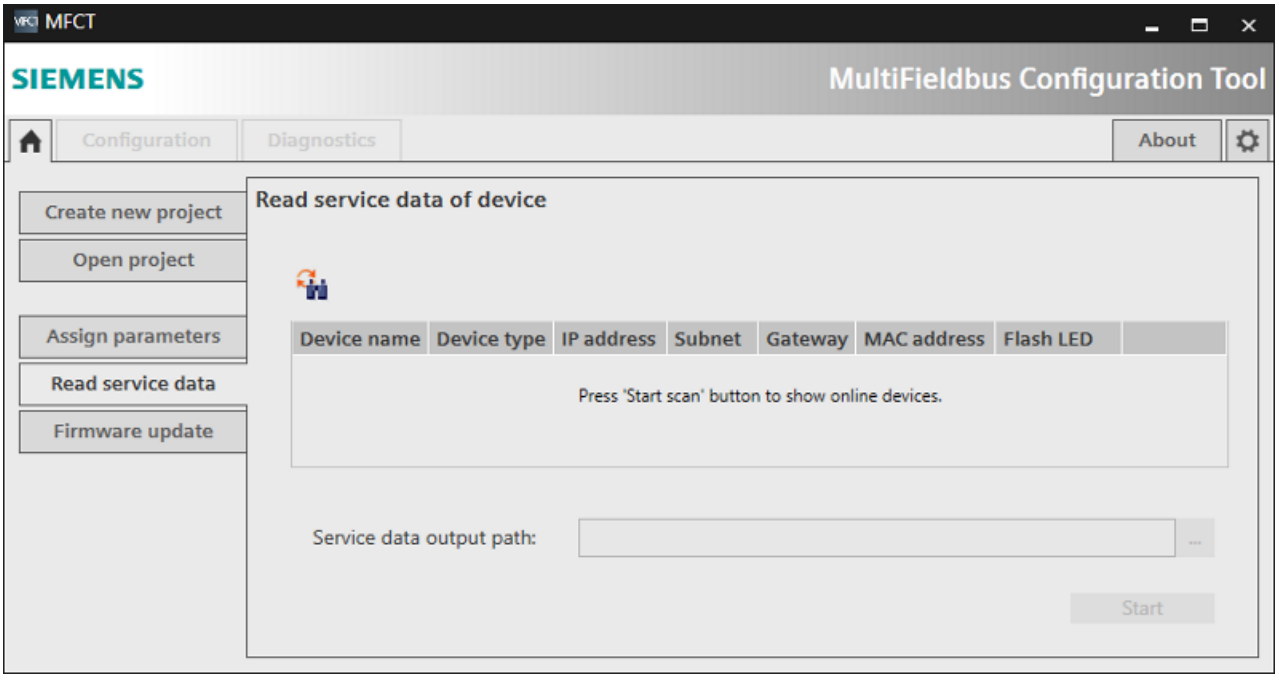
Field	Bit number	Bit mask	Default	Bit value = '0'	Bit value = '1'
Problem	6	0x40	0	Initial status	Module problem: • Module not plugged • Incorrect module plugged • Module with incorrect parameter assignment

4.3.4 Reading service data

In the "Home" tab, you can read out and store the service data provided by an MF device under "Read service data":

1. Click the "Start scan" button to find MF devices via the preset network interface.
2. Select an MF device.
   (You can make the LEDs of the MF device flash for identification with "Flash LED".)
3. Select the path to the location where you want to save the service data under "Service data output path".
4. Click the "Start" button.

The service data is saved under the selected path.



MF Shared Device

5

The "MF Shared Device" function lets you use various fieldbuses in a station. You select the fieldbus you want to use for each module in MFCT.

The System Manual or Equipment Manual of the MF device used describes how many connections and fieldbuses are supported at the same time.

This gives you the option to use, for example, F-modules that communicate via PROFIsafe with an F-CPU in a station. You configure and program the F-modules and the F-CPU in the TIA Portal with STEP 7 Safety.

For information on the maximum amount of I/O data, refer to the Device Manuals of the MF devices that support the MF Shared Device function.

The download size contains the I/O data of all EtherNet/IP and Modbus TCP connections as well as additional bytes for controlling the download.

NOTE

To avoid temporarily exceeding the I/O quantity structure, you must proceed as follows for a reconfiguration that results in changed I/O lengths:

1. Reduce the amount of I/O data in one configuration and download it to the MF device/CPU.
2. Increase the amount of I/O data in another configuration and download it to the MF device/CPU.

Multiple Modbus TCP connections

Several TCP connections (sockets) to the same *register area* for I/O data (e.g. for fieldbus connection ModbusTCP #0) can be established from a Modbus TCP controller to extend the area of the register addresses for input/output addresses.

The *register area* for I/O data of different fieldbus connections (e.g. ModbusTCP #0 and ModbusTCP #1) cannot be accessed within a TCP connection (socket).

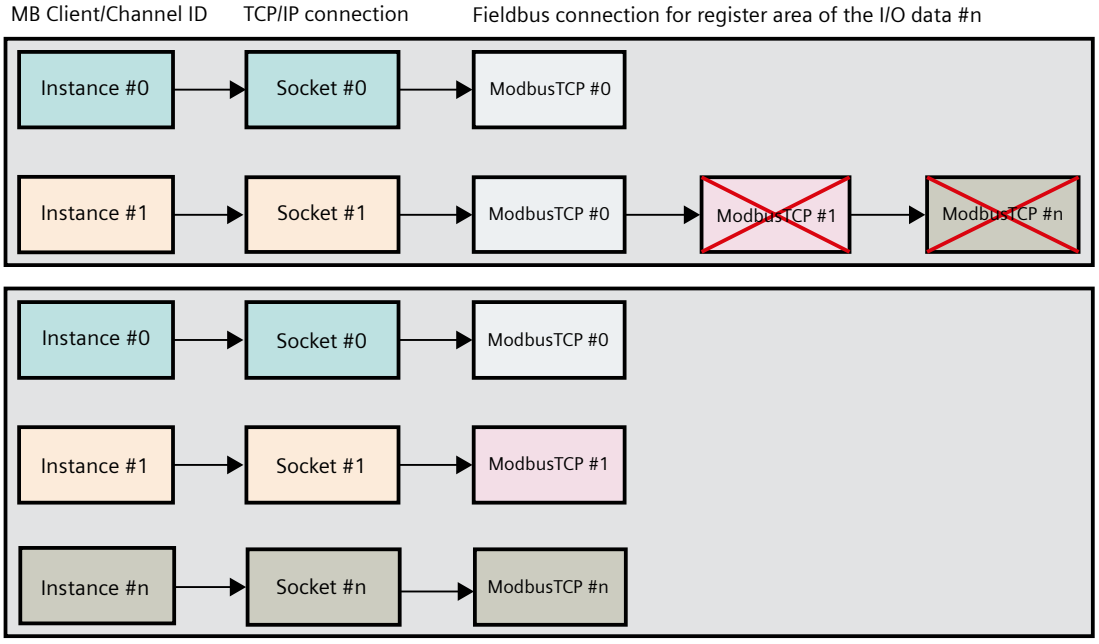


Figure 3-540 Example of multiple Modbus TCP connections

5.1 Configuration

Introduction

You parameterize modules you want to use with EtherNet/IP (Page 23) and Modbus TCP (Page 73) in MFCT.

Modules that are to be operated with PROFINET must be configured separately in the TIA Portal. You can find more information in the TIA Portal help.

Requirements

- MFCT V1.3 and higher
- A MultiFieldbus project is created in MFCT
- When PROFINET is to be used for MF Shared Device mode, a project must be created in the TIA Portal.

Configuring in MFCT

1. Configure the modules in MFCT.
2. In MFCT, enable the "MF Shared Device" function for the MF Device.
   In this way, you can select the fieldbus at each submodule separately.
3. Parameterize modules that you want to use with EtherNet/IP (Page 12) and Modbus TCP (Page 63). Select "PROFINET" for modules that you configure separately in the TIA Portal.
4. Parameterize the desired fieldbus and the controller connection for the modules under "Fieldbus connection".
5. Transfer the MultiFieldbus project to the MF Device.

NOTE

In case of high utilization of the MF Device or too little network bandwidth, the services of the fieldbus selected on the interface module are prioritized. Services of other fieldbuses may be delayed or fail in heavy load scenarios.

Configuring in the TIA Portal

1. Configure the MF Device in the TIA Portal.
2. Configure all modules in the TIA Portal.
3. In the TIA Portal, configure the modules you want to use with PROFINET.
4. In the TIA Portal, configure the modules that use EtherNet/IP or Modbus TCP in the properties of the interface module under "Shared Device" with the IO Controller deselected.
5. Configure the correct potential groups in the TIA Portal.

NOTE

Shared device conflicts between PROFINET and EtherNet/IP or Modbus TCP can be solved by:

- POWER OFF/POWER ON or
- Disconnection of active PROFINET connections to the MF Device, download of the MultiFieldbus project again and re-establishment of PROFINET connections.

NOTE

You can prevent shared device conflicts by first deregistering modules on the old fieldbus and then registering them on the new fieldbus.
Example:

1. Deselect the CPU for the module in TIA Portal.
2. Download the hardware configuration to the CPU,
3. Select EtherNet/IP as the fieldbus for the module in MFCT.
4. Download to the MF Device with MFCT.

5.2 Example

The following example shows you the configuration with one connection each via PROFINET (PROFIsafe), EtherNet/IP and Modbus TCP. The connection via PROFINET (PROFIsafe) is supposed to have the highest priority.

Configuring in MFCT

In this example, the DI module is to be addressed via Modbus TCP and the DQ module via EtherNet/IP. To do so, enable the "MF Shared Device" function in the parameters of the interface module.

Multi fieldbus features

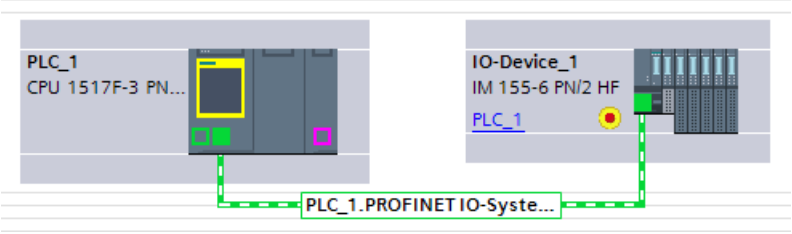
Parameter	Value
MF Shared Device	☑

Next, you can select the fieldbuses and the controller connection in the module parameters.

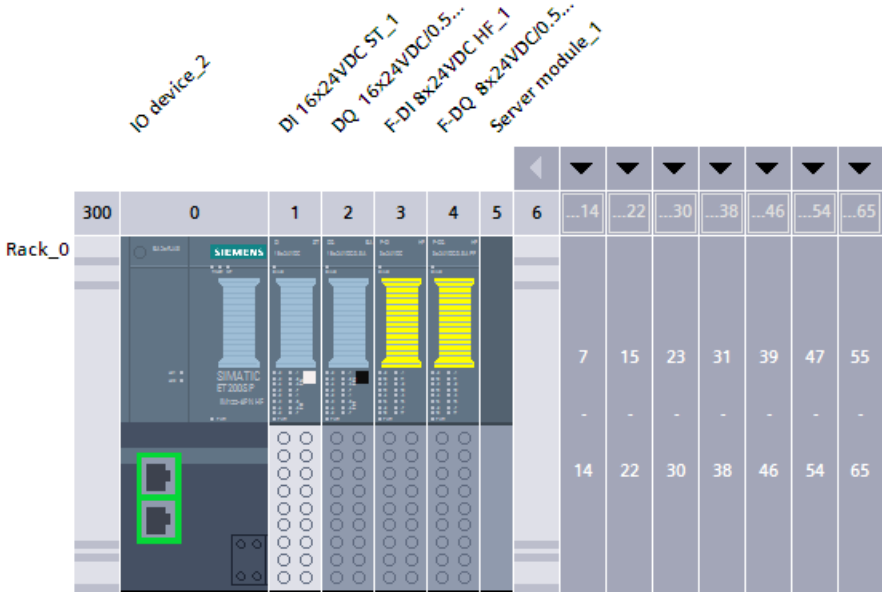
Slot	Name	Type	Article number	Fieldbus connection
0	IM 155-6 MF HF V5.2	InterfaceModule	6ES7 155-6MU00-0CN0	PROFINET
0.1	IM 155-6 MF HF V5.2			
0.2				
0.3				
0.4				
1	DI 16x24VDC ST V0.0	Digital	6ES7 131-6BH01-0BA0	EtherNet/IP #0 (0x301, 0x300)
2	DQ 16x24VDC/0.5A BA V0.0	Digital	6ES7 132-6BH00-0AA0	ModbusTCP #0 (0x000, 0x2D0)
3	F-DI 8x24VDC HF, BP	FDigital	6ES7 136-6BA00-0CA0	PROFINET
4	F-DQ 8x24VDC/0.5A PP HF, BP	FDigital	6ES7 136-6DC00-0CA0	PROFINET
5	Server module V1.2 (0 bytes)	ServerModule	6ES7 193-6PA00-0AA0	PROFINET

Configuring in the TIA Portal

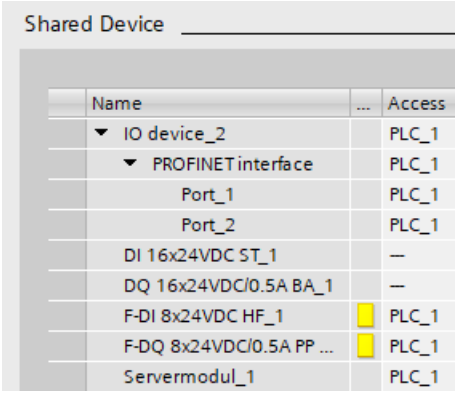
In this example, the two F-modules are to be used by an F-CPU via PROFINET (PROFIsafe).



Configure the interface module IM 155-6 PN HF and the (F) modules in the TIA Portal.



In the settings of the interface module, disable access by the IO controllers to the modules, which you access with EtherNet/IP and Modbus TCP.



Firmware update with MFCT

6

For a firmware update, you can load the new firmware and update the loaded firmware at different times.

This means you can download the firmware during operation to multiple MF devices and modules. The MF devices and modules continue their operation uninterrupted. You can then activate the update of the new firmware with MFCT during a planned maintenance break.

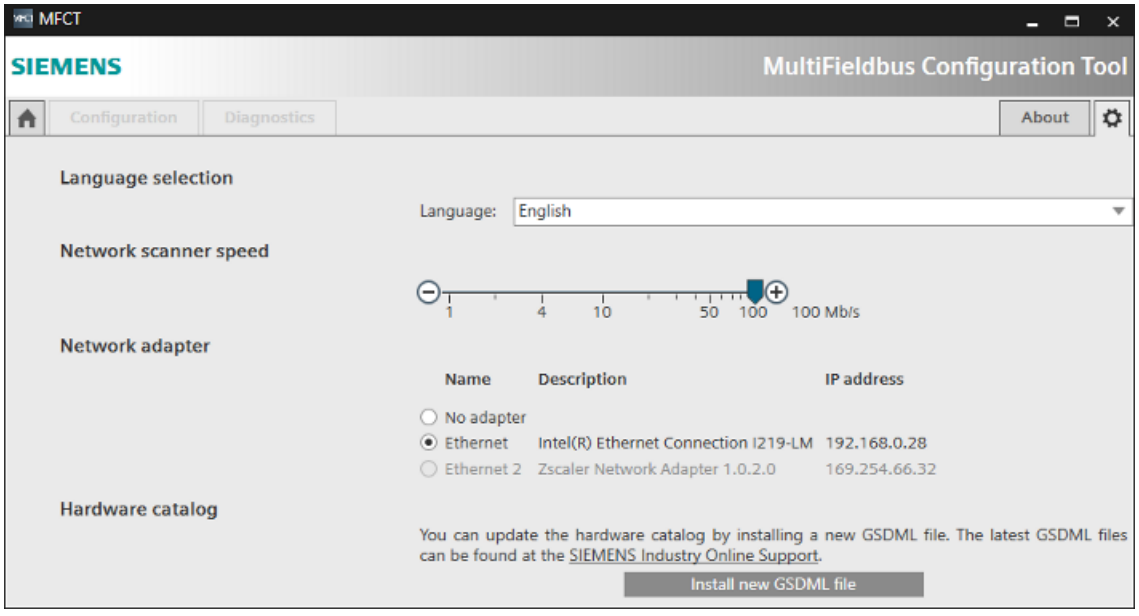
By performing the time-consuming loading during operation, you reduce the downtimes of your plant.

You can also use the option "Automatically activate firmware after download" to select whether you want to update the firmware after the download.

6.1 Settings

You can set the speed of the network scanner in the settings.

The default setting is 100 Mbps.



In the case of networks with high network load we recommend reducing the speed of the network scanner before the firmware update.

A firmware update of more than 20 devices results in a network load of approx. 3 Mbps.

6.2 Updating the firmware

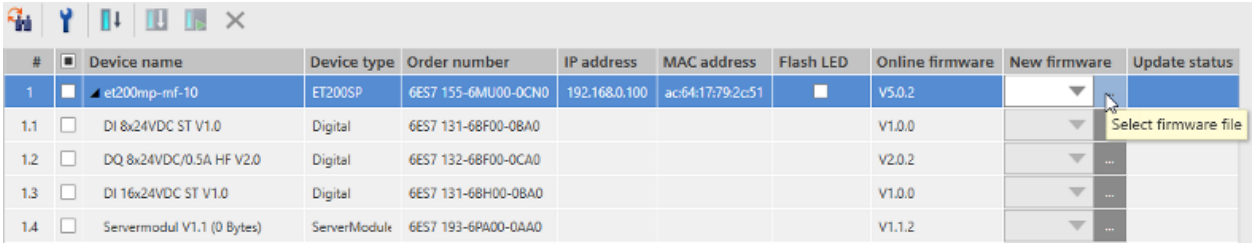
Requirements

NOTE
We recommend that you do not connect directly to the MF device that you want to update. The activation of the new firmware can lead to a loss of the scanned MF devices due to a brief interruption of the network connection at the network adapter.

Procedure

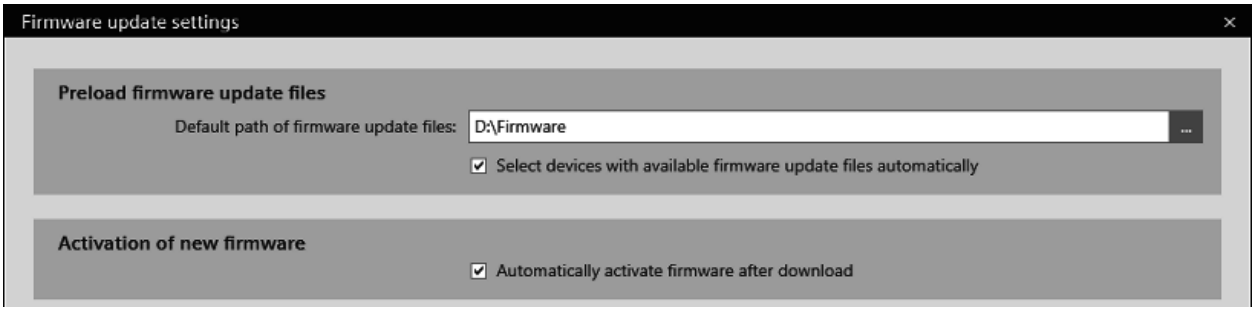
You can update the firmware of MF devices and modules in the "Home" tab under "Firmware update":

1. Click the "Start scan" button to find MF devices via the preset network interface.
   All MF devices and lower-level modules whose firmware you can update are displayed.
2. Select the firmware files (*.upd) for the update:
   – You can select the appropriate firmware file for each MF device with "Select firmware file".



If you are using a STEP 7 FW update file (recommended), select the file header.upd.

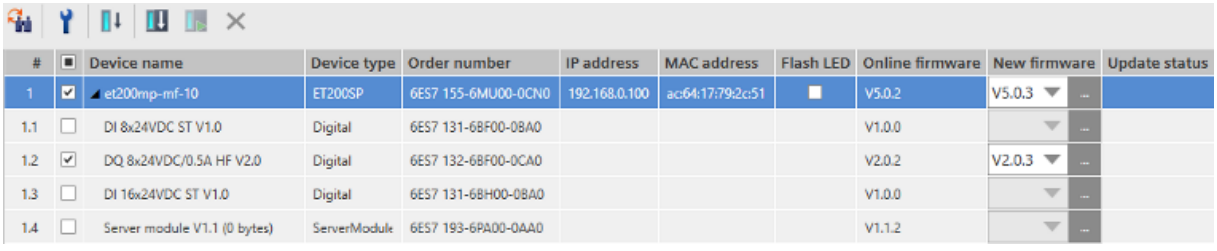
– You can select a directory with "Firmware update settings".



When you activate the option "Automatically activate firmware after download", the firmware is automatically activated after the download.

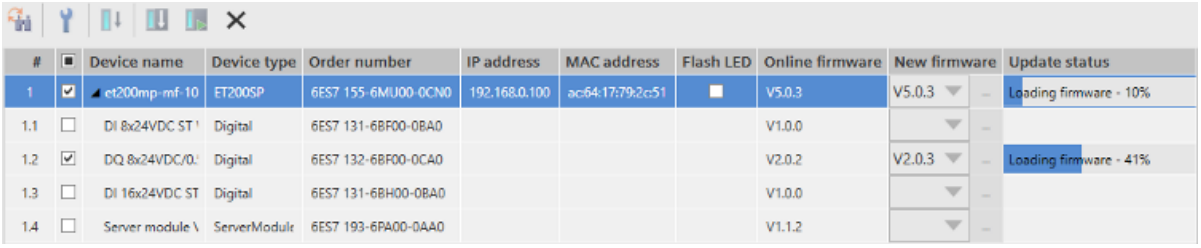
NOTE
Select a directory which contains subdirectories with firmware files.
If large directories, entire hard disks (for example C:\) or directories are selected on network drives, the corresponding access can take very long or MFCT can no longer react.

Then, click "OK".
The latest suitable firmware file is automatically selected for the scanned MF devices.



#	Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware	Update status
1	et200mp-mf-10	ET200SP	6ES7 155-6MU00-0CN0	192.168.0.100	ac:64:17:79:2c:51		V5.0.2	V5.0.3	
1.1	DI 8x24VDC ST V1.0	Digital	6ES7 131-6BF00-0BA0				V1.0.0		
1.2	DQ 8x24VDC/0.5A HF V2.0	Digital	6ES7 132-6BF00-0CA0				V2.0.2	V2.0.3	
1.3	DI 16x24VDC ST V1.0	Digital	6ES7 131-6BH00-0BA0				V1.0.0		
1.4	Server module V1.1 (0 bytes)	ServerModule	6ES7 193-6PA00-0AA0				V1.1.2		

3. Select the MF devices and modules whose firmware is to be downloaded. All MF devices and modules are selected by default.
4. Start the download of the firmware files to the selected MF devices and modules with "Update firmware".



#	Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware	Update status
1	et200mp-mf-10	ET200SP	6ES7 155-6MU00-0CN0	192.168.0.100	ac:64:17:79:2c:51		V5.0.3	V5.0.3	Loading firmware - 10%
1.1	DI 8x24VDC ST	Digital	6ES7 131-6BF00-0BA0				V1.0.0		
1.2	DQ 8x24VDC/0.	Digital	6ES7 132-6BF00-0CA0				V2.0.2	V2.0.3	Loading firmware - 41%
1.3	DI 16x24VDC ST	Digital	6ES7 131-6BH00-0BA0				V1.0.0		
1.4	Server module \	ServerModule	6ES7 193-6PA00-0AA0				V1.1.2		

You can cancel the download at any time with the "Cancel" button.

NOTE
If you cancel the download of the firmware in the "Initialization" or "Waiting" phase, it takes a few minutes until the MF devices are ready again and you can restart the download.

5. Activate the downloaded firmware as described under "Activating the firmware (Page 104)".

NOTE
The number of MF devices and modules that can be loaded simultaneously is not restricted. From experience, a simultaneous download to 60 MF devices with firmware <V3.3.0 takes approximately one hour.

6.3 Updating firmware in multiple subnets

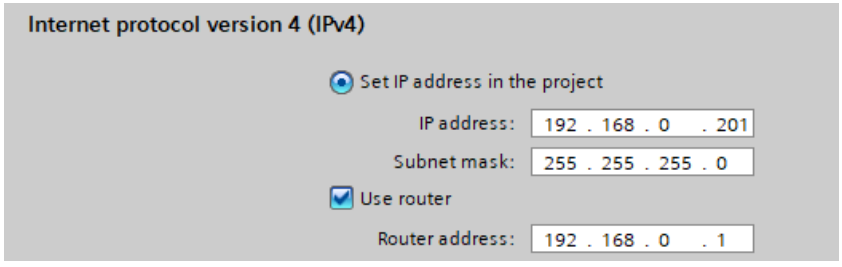
To update the firmware in multiple subnets, follow these steps:

1. Open the settings for the firmware update in the "Home" tab under "Firmware update".
2. Under "Scan options", select "Subnet scan".
3. For each subnet enter the IP address, the subnet mask and the gateway address, and add the subnet to the list with "Add".
4. Exit the dialog with "Ok".
5. Proceed as described under "Updating the firmware (Page 101)".

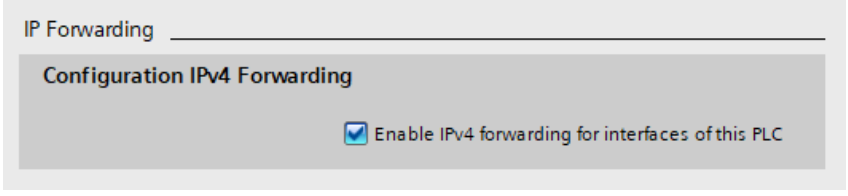
NOTE
Assign a static IP address, the address for the gateway and a device name for each MF Device.

Comments

We recommend activating the "Use router" option for CPUs in the project in the TIA Portal.

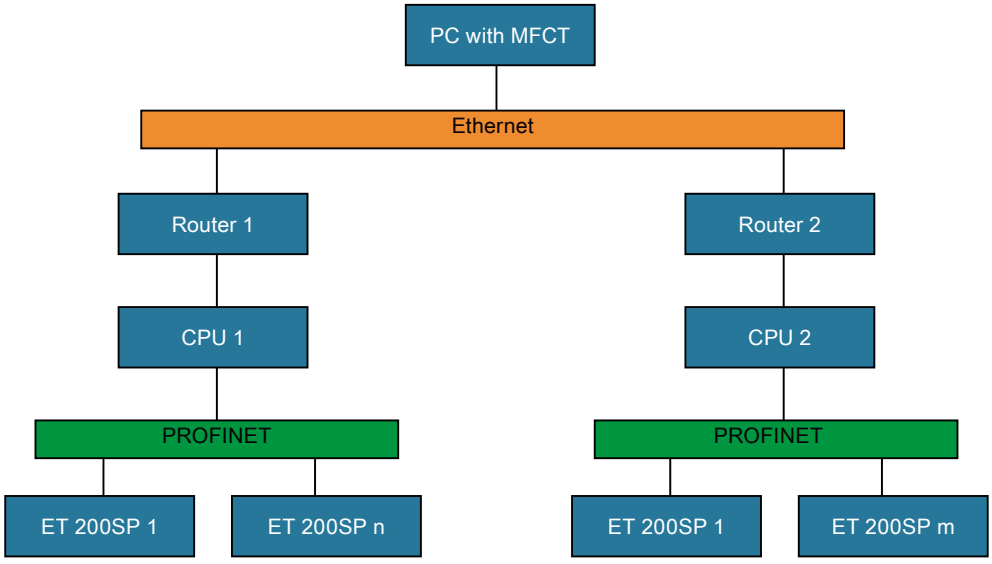


When the router is connected to interface X1 of the CPU and the rest of the topology in which, for example, the ET 200SP is located is connected to interface X2, activate the option "Enable IPv4 forwarding for interfaces of this PLC" for the CPU in the TIA Portal.



Example of multiple subnets

The figure below shows an example of a topology with multiple subnets.



6.4 Activating the firmware

The new firmware is not active yet once the firmware update has been successfully performed. You can activate the firmware later on the MF device or module.

Requirements

We recommend setting the CPU to STOP.

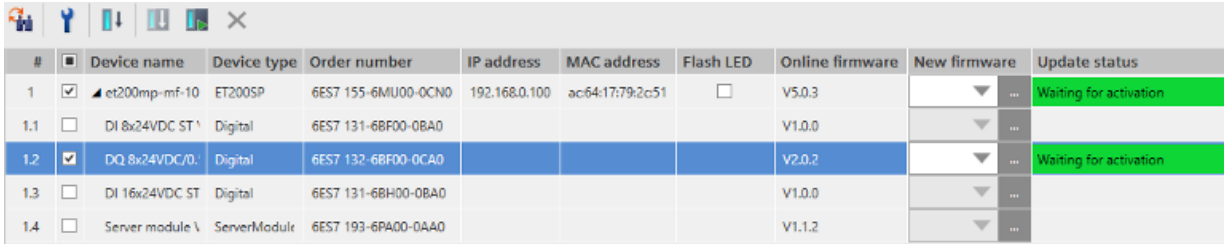
Procedure

You can recognize MF devices and modules with updated firmware that has not been activated yet in the device table by scanning again.

Proceed as follows to activate the firmware:

1. Select the MF devices or modules whose firmware you want to activate.
2. Click the "Activate firmware" button.

The firmware of the selected MF devices or modules is activated one after the other.



#		Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware	Update status
1	☑	et200mp-mf-10	ET200SP	6ES7 155-6MU00-0CN0	192.168.0.100	ac:64:17:79:2c:51	☐	V5.0.3		Waiting for activation
1.1	☐	DI 8x24VDC ST	Digital	6ES7 131-6BF00-0BA0				V1.0.0		
1.2	☑	DQ 8x24VDC/0.5	Digital	6ES7 132-6BF00-0CA0				V2.0.2		Waiting for activation
1.3	☐	DI 16x24VDC ST	Digital	6ES7 131-6BH00-0BA0				V1.0.0		
1.4	☐	Server module V	ServerModule	6ES7 193-6PA00-0AA0				V1.1.2		

If activation fails, scan the network again.

SIEMENS

SIMATIC

MultiFieldbus Configuration Tool (MFCT)

Configuration Manual

Introduction 1

Safety instructions 2

Industrial cybersecurity 3

Description 4

Software installation 5

Functions 6

MultiFieldbus configuration 7

DALI configuration 8

TM FAST 9

SIWAREX 10

PtP Event Trace 11

Maintenance 12

12/2025
A5E53511456-AC

Table of contents

1 Introduction 5

1.1 Reference documents 6

2 Safety instructions 8

2.1 General security instructions 8

3 Industrial cybersecurity 9

3.1 Cybersecurity information 9

3.2 Basic information on industrial cybersecurity 10
3.2.1 Definition of industrial cybersecurity 10
3.2.2 Objectives of industrial cybersecurity 10

3.3 Operational application environment and security measures 10
3.3.1 Intended use 10
3.3.2 Requirements for the operational environment and security measures 11

3.4 Security features of the MFCT 13

3.5 Secure operation of the MFCT 13
3.5.1 Security update notification 14
3.5.2 Hardening measures 14
3.5.3 Access control 14
3.5.4 Notifications about security vulnerabilities (Siemens Security Advisories) 15
3.5.5 Data backup 16
3.5.6 Secure uninstallation 16

4 Description 17

4.1 Area of application of the MFCT 17

4.2 Conditions for operating the MFCT 18

4.3 Operation with multiple subnets 19
4.3.1 Recommended settings for operating the MFCT 20

5 Software installation 21

5.1 System requirements 21
5.1.1 Operating systems 21
5.1.2 Additional software components 22
5.1.3 Security programs 22
5.1.4 Virtualization platforms 23

5.2 Installation 23

5.3 Update the MFCT installation 24

6 Functions 25

6.1 Information on the "About" tab 25
6.1.1 Version information 26
6.1.2 User feedback 26

6.2 Overview of the "Settings" 27
6.2.1 General settings 27
6.2.2 Catalog 29
6.2.3 Plug-ins 30

7 MultiFieldbus configuration 33

7.1 Creating new MultiFieldbus project in MFCT 33

7.2 Open MultiFieldbus project in MFCT 34

7.3 Selecting a station 35

7.4 Configuring a station 39

7.5 Parameterizing the station 42
7.5.1 Parameterizing the I/O data alignment 44

7.6 Transfer the configuration 48

7.7 Exporting the configuration 50

7.8 Reading diagnostics 52

8 DALI configuration 54

8.1 Selecting station with DALI module 54

8.2 Selecting and configuring a DALI module 55

8.3 Making color settings 58

8.4 Device types 60
8.4.1 Control gear 60
8.4.1.1 Device view 60
8.4.1.2 Group view 64
8.4.2 Input devices 66

8.5 Maintenance 67
8.5.1 Event information 68
8.5.2 Running light identification 68
8.5.3 Expert mode 69

8.6 Mass operation 71

8.7 Settings 74

9 TM FAST 76

9.1 Generating UPD and DB files 76

9.2 Download UPD files 77

10 SIWAREX 80
10.1 Scanning for SIWAREX assemblies 80
10.2 Setting up communication in the station view 81
10.3 Working in the station view 82
10.4 Commissioning and monitoring 83

11 PtP Event Trace 86
11.1 Selecting a station with CM PtP module 87
11.2 Analyzing a trace 89

12 Maintenance 90
12.1 "Assign parameters" tab 91
12.1.1 Assigning network parameters 92
12.1.2 Resetting to factory settings 92
12.1.3 Defining scan settings 92
12.2 "Read service data" tab 93
12.3 "Firmware update" tab 93
12.3.1 Settings for firmware update 94
12.3.1.1 Setting scanning options 96
12.3.2 Updating firmware 97
12.3.3 Activating the firmware 100

Introduction

1

Purpose of this documentation

This documentation provides important information on the following topics:

- Description of the MultiFieldbus Configuration Tool (MFCT)
- Configuring and commissioning MultiFieldbus devices on fieldbuses, for example, EtherNet/IP and Modbus TCP.

The configuration manual supplements the description of the system manuals and equipment manuals of the MultiFieldbus devices.

Basic knowledge required

The following knowledge is required to understand the document:

- General knowledge of automation engineering
- Knowledge of the SIMATIC industrial automation system
- Knowledge of the use of Microsoft Windows computers
- Knowledge of PROFINET, EtherNet/IP, Modbus TCP

Scope of this documentation

This documentation is the basic documentation for the MFCT. The product documentation is based on the content of this Configuration Manual.

Conventions

The MultiFieldbus Configuration Tool is referred to in this documentation as MFCT.

This documentation contains illustrations of the MFCT user interface. The illustrations may differ in detail from the current version of the MFCT.

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Open Source Software

Open Source Software is used in the MFCT. The open-source software is provided free of charge. Siemens AG is liable for the product described, including the Open Source Software contained in it, pursuant to the conditions applicable to the product. Any and all liability is excluded:

- For use of the Open Source Software beyond the program sequence intended for the product by Siemens
- For defects caused by changes to the software

For legal reasons, Siemens AG is obliged to publish the original text of the license conditions and copyright notices from the third-party software contained in this product.
You can find the corresponding file with the above-mentioned information in the SiePortal in the section Information on third-party products, license conditions and OSS sources (https://support.industry.siemens.com/cs/ww/en/view/109773881).

1.1 Reference documents

The following list contains additional documentation that supplements this Configuration Manual:

Topic	Link to the documentation
MultiFieldbus topic page	MultiFieldbus - an overview of the most important documents and links (https://support.industry.siemens.com/cs/us/en/view/109779189)
MultiFieldbus Configuration Tool (MFCT) topic page	MultiFieldbus Configuration Tool (MFCT) (https://support.industry.siemens.com/cs/us/en/view/109773881)
SIMATIC MultiFieldbus	SIMATIC MultiFieldbus Function Manual (https://support.industry.siemens.com/cs/us/en/view/109773209)
Communications module DALI	Equipment manual SIMATIC ET 200SP ET 200SP communications module CM 1xDALI (https://support.industry.siemens.com/cs/us/en/view/109769428)
Technology module TM FAST	TM FAST Equipment Manual (https://support.industry.siemens.com/cs/us/en/view/109816087)
SIWAREX WP321	Operating instructions SIWAREX WP321 (https://support.industry.siemens.com/cs/us/en/view/109770838)
CM PtP module	CM PtP - Configurations for point-to-point connections Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59057093)
SIMATIC ET 200SP Distributed I/O System	SIMATIC ET 200SP System Manual (https://support.industry.siemens.com/cs/us/en/view/58649293)
SIMATIC S7-1500/ET 200MP Automation System	SIMATIC S7-1500/ET 200MP System Manual (https://support.industry.siemens.com/cs/us/en/view/59191792)

Topic	Link to the documentation
SIMATIC ET 200AL Distributed I/O System	SIMATIC ET 200AL System Manual (https://support.industry.siemens.com/cs/us/en/view/89254965)
SIMATIC ET 200clean	SIMATIC ET 200clean System Manual (https://support.industry.siemens.com/cs/ww/en/view/109822889)
SIMATIC ET 200eco PN Distributed I/O System	SIMATIC ET 200eco PN System Manual (https://support.industry.siemens.com/cs/us/en/view/109778292)
SIMATIC Bus links PN/MF Coupler	Installation and Operating Manual PN/MF Coupler (https://support.industry.siemens.com/cs/us/en/view/109781406)

Safety instructions

2

2.1 General security instructions

Read the security-related information provided in the corresponding system manual.
You can find cybersecurity-related information in the section Industrial cybersecurity (Page 9).

Industrial cybersecurity 3

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

Refer to the relevant system manual of the devices used for general information and measures regarding industrial cybersecurity.

This section provides an overview of security-related information for the MultiFieldbus Configuration Tool (MFCT).

3.1 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

3.2 Basic information on industrial cybersecurity

3.2.1 Definition of industrial cybersecurity

Industrial cybersecurity is generally understood to mean all measures to protect against the following threats:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability (e.g. due to the destruction of data or denial of service (DoS))

3.2.2 Objectives of industrial cybersecurity

The objectives of industrial cybersecurity are:

- Ensuring trouble-free operation of industrial systems and production processes
- Preventing threats to people and production from cybersecurity attacks
- Protection of industrial plants against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Provision of a practical and cost-effective concept for securing existing systems and devices without their own security functions
- Use of existing, open and proven industrial cybersecurity standards
- Compliance with legal requirements

An optimized and adapted security concept applies to automation and drive technology. The security measures must not impede or endanger production.

3.3 Operational application environment and security measures

3.3.1 Intended use

The MFCT is a PC-based Microsoft Windows software for commissioning and configuring MultiFieldbus devices (MF devices). MFCT uses PROFINET communication for this. You can find information on communication protocols and the port numbers used for Ethernet communication in the Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) function manual.

The software may be used only for the specific task in accordance with the relevant documentation, in particular its warning notices and security information.

Operational reliability and intended use

An MF device supports the following Ethernet-based protocols:

- PROFINET I/O (PN)
- EtherNet/IP (EIP)
- Modbus TCP (MTCP)

Communication between MFCT and an MF device does not cross network boundaries (e.g. to the customer network or the Internet).

Exception: If the IP forwarding option is enabled on devices within the system, data is forwarded to connected subnets or a configured router.

Area of application

You can use the MFCT to configure MF devices, e.g. for the following typical use cases:

- Mechanical engineering
- Tunnel applications
- Energy management

3.3.2 Requirements for the operational environment and security measures

Siemens recommends the following security measures:

- Threat and risk assessment (as part of security management)
- Network security concepts
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
  - Microsoft Windows access and protection mechanisms
- System protection
  - Consideration of security aspects in the selection of systems and components
  - Minimal assignment of rights for user management
- Access control concepts (utilizing access control systems)
  - Physical protection
  - Physical corporate security
  - Physical product security

Threat and risk assessment

Vulnerabilities and risks are identified, and countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) on the Industrial cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) website.

System protection

System protection depends heavily on the endangerment potential of the system operating entity and its infrastructure. The following measures provide extra protection against unauthorized access from external sources and through the network:

- Definition of security-specific guidelines and processes
- Consideration of security aspects in the selection of systems and components. This also relates to external service providers, commissioning and remote maintenance.
- Minimal assignment of rights for user management

Access control concepts

Physical protection
In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security
You can ensure the physical corporate security by taking the following measures:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security
You can ensure physical production security by taking the following measures, including:

- Separate access control for critical areas, such as production zones.
- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.
- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).
- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsecure on systems.

3.4 Security features of the MFCT

The MFCT does not require a setup program for installation. The application is downloaded as a zip file from the Internet and installed on the local drive by simply extracting the zip folder. The installation is now complete.

To check the integrity of the downloaded zip file, compare the checksum of the zip file to the checksum in SiePortal.

The "Standard user" role is sufficient for installing and using the MFCT in Microsoft Windows.

The MultiFieldbus Configuration Tool (MFCT) performs the following security checks itself:

- Checks the data integrity of the MFCT and the plug-ins
- Checks the files added by the user, e.g:
  - GSDML
  - GSDX
  - Project file
- Checks the preset security configuration
- Checks the signatures of the following file types:
  - exe file
  - dll files
  - gsdx containers

More information

You can find information on installing the MFCT in the section Installation (Page 23).

You can read how to compare the checksums in the following Internet article (https://support.industry.siemens.com/cs/ww/en/view/109483101).

3.5 Secure operation of the MFCT

This section describes measures recommended by Siemens to protect the MFCT and the connected devices against manipulation and unauthorized access.

Guidelines for secure operation

The following guidelines apply to the secure operation of the MFCT:

- Only use the original version that you have downloaded from the Internet. You can find the MFCT on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109773881).
  You can find information on installing the MFCT in the section Installation (Page 23).
- Do not mix files from different versions.
- Check regularly whether there are new versions of the MFCT available for download.
- Always use the latest version of the MFCT.
  You can find information on checking for updates in the section Update the MFCT installation (Page 24).

Dependencies on other software components

You can find the requirements for using the MFCT in the section System requirements (Page 21).

3.5.1 Security update notification

Setting up notification of security updates

To receive notifications about security updates, proceed as follows:

1. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home/).
2. Enter the keyword "Security" in the search engine.
3. Choose the "Search in Knowledge base" option.
4. Select your product or product group in the "Product tree" filter menu, e.g. "Automation technology > Automation systems > SIMATIC industrial automation systems > IO systems".
5. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".
6. Select the document with which you want to create notifications.
   If you would like to be informed about changes to the MultiFieldbus Configuration Tool (MFCT), for example, select the entry "MultiFieldbus Configuration Tool (MFCT)".
7. Select "Add to my favorites" using the 3 dots on the right.
8. In the following dialog, select the name and storage location for the favorite. Activate the "Notify me" option for notifications.
   Then click the "+ Add to my favorites" button.

Result: You will be notified by email each time the document is changed.

Under "mySiePortal > Lists & notifications > My notifications", you can display your notifications and delete them if necessary.

3.5.2 Hardening measures

System hardening, also simply referred to as hardening, is the secure configuration of products or systems. The aim is to close security gaps and take various measures to reduce the attack surfaces for cyberattacks.

To minimize the attack surface for a cyber attack, only activate required plug-ins in the MFCT.

3.5.3 Access control

To control access to your system, set up logical protection in addition to physical protection. For example, use the Microsoft Windows access and protection mechanisms.

To be able to install and use MFCT on the PC, the "Standard user" user role is sufficient in Microsoft Windows.

3.5.4 Notifications about security vulnerabilities (Siemens Security Advisories)

A vulnerability is a security vulnerability in information security. It can pose a threat as it provides intruders with the opportunity to access system resources and manipulate or steal data. Many vulnerabilities allow availability to be impaired.

Siemens ProductCERT

If Siemens identifies or fixes security gaps (Vulnerabilities) in the products, this will be published in the Security Advisories.

You can find the documents for SIMATIC on the following Siemens AG Web page: Siemens ProductCERT and Siemens CERT (https://new.siemens.com/global/en/products/services/cert.html?s=SIMATIC#SecurityPublications)

"SIMATIC" is preset in the "Search Security Advisories" search field. You can also enter other product names or other terms in the search field and search for them.

On this page, you can also find all the required information on how to deal with vulnerabilities:

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities
- Notifications are also possible in CSAF format
- Option to subscribe to RSS feeds and newsletters
- List of all current vulnerabilities and detailed information such as:
  - Description
  - Classification according to Common Vulnerability Scoring System (CVSS)
  - Measures
  - Availability
  - Etc.

Set up Security feeds (https://www.siemens.com/cert) to receive notifications about security-related topics.

If you suspect or have discovered a vulnerability in a Siemens product, please inform us immediately. To do this, press the "Contact" button on the CERT Services page (https://www.siemens.com/cert) and follow the instructions.

3.5.5 Data backup

Secure your configuration and parameter settings so that you can quickly restore this data if needed. Do not use the MFCT file folder for data backup. Otherwise, this will delete your backed-up data when you switch to a newer version.

3.5.6 Secure uninstallation

If you want to remove the MFCT from your PC, delete the folder in which the MFCT is stored. Also delete any additional files created in your folders, e.g. configuration and parameter settings.

Since only one zip file was extracted to install the MFCT, no further step is required to uninstall it.

Description

4

4.1 Area of application of the MFCT

The MFCT is a PC-based software for simple commissioning of MultiFieldbus devices on higher-level controllers within fieldbuses.

Main areas of application of the MFCT

The main area of application of the MFCT is in the following functions:

- Configuration of a MultiFieldbus device
- Bulk firmware update of ET 200 devices

Ethernet protocols supported by MultiFieldbus

The MultiFieldbus supports the following Ethernet protocols:

- PROFINET
- EtherNet/IP
- Modbus TCP

Additional plug-ins

You can also supplement the MFCT with the following plug-ins:

- DALI (Page 54)
  You use this plug-in to configure DALI devices.
- TM FAST (Page 76)
  You use this plug-in to create application update files for TM FAST modules or to load an application into a TM FAST module.
- SIWAREX (Page 80)
  You can use this plug-in to configure SIWAREX modules.
- PtP Event Trace (Page 86)
  You use this plug-in to do the following:
  - Read out event traces from a PtP module
  - Analyze serial communication
  - Display the current configuration of a PtP module

You can find more information on the plug-ins in the Plug-ins (Page 30) section.

4.2 Conditions for operating the MFCT

The following conditions should be met for the operation of the MFCT:

- **Commissioning:** The MF device must be connected via an Ethernet connection with 100 Mbps full duplex.
- **Network:** Only one instance of MFCT or PRONETA may be active per network.

NOTE

If PRONETA and MFCT are simultaneously active in the network, you must deactivate cyclic scanning in PRONETA.

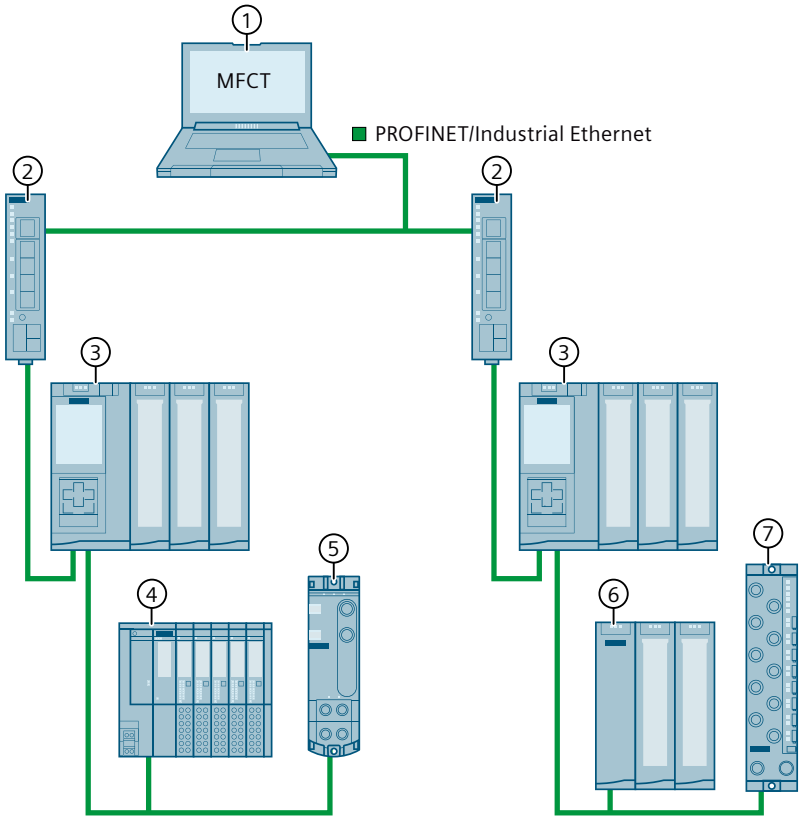
- **Fieldbus:** MFCT can only be operated on the fieldbus, not from the system network via a CPU.

4.3 Operation with multiple subnets

In the general settings of the MFCT, select which devices you would like to scan. You can find information on the individual settings in the section General settings (Page 27).

Depending on the settings selected in the MFCT, the devices must be configured accordingly in the TIA Portal. Otherwise, the MFCT cannot establish a connection to the desired devices.

The figure below shows an example of a topology with multiple subnets. The PC with installed MFCT is in a different subnet than the MF devices.



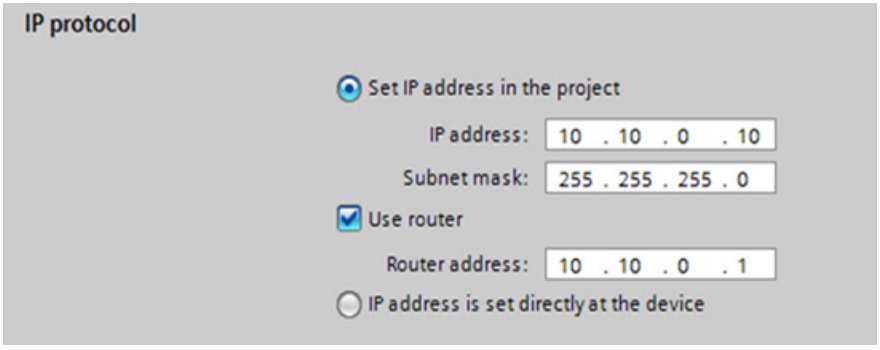
① PC with MFCT installed
② Router, e.g. SCALANCE S615
③ CPU, e.g. CPU1515-2 PN
④ MF device ET 200SP IM 155-6 MF HF
⑤ MF device ET 200AL IM 157-1 MF
⑥ MF device ET 200MP IM 155-5 MF HF
⑦ MF device ET 200eco PN

4.3.1 Recommended settings for operating the MFCT

Settings when using routers

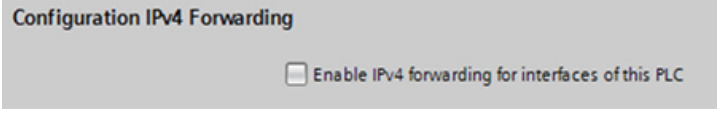
Routers have the task of connecting IP subnets. If the MFCT is to search for MF devices in other subnets, the MFCT is first forwarded to the router. To be able to reach the devices in the other subnet, you need to enter the address of the router for each desired device.

The IP address of a device in the subnet and the IP address of the router may only be different in the places where the subnet mask contains "0".



Settings for the IPv4 forwarding configuration

If the router is connected to interface X1 of the CPU and the rest of the topology is connected to interface X2, select the "Enable IPv4 forwarding for interfaces of this PLC" check box in the TIA Portal for the CPU.



More information

You can more find information on the setting options in the TIA Portal online help, for example.

Software installation

5

In the following sections, you can find all the software information required for trouble-free operation of the MFCT.

More information

You can find more information on MFCT and the current system requirements on the Internet (https://support.industry.siemens.com/cs/us/en/view/109773881).

5.1 System requirements

5.1.1 Operating systems

To operate the MFCT, you need Microsoft Windows. Install one of the following operating systems to operate the MFCT. The installation of Microsoft .NET Framework 4.8 must be supported.

NOTE

The ability of MFCT to run on all other operating systems is not ensured. The use of any other operating system is at your own risk.

- Microsoft Windows 10 (32/64-bit)
  - Microsoft Windows 10 Home
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 (IoT) Enterprise 2016 LTSB
  - Microsoft Windows 10 (IoT) Enterprise 2019 LTSC (for IPC/PG)
  - Microsoft Windows 10 Enterprise 2021 LTSC
- Microsoft Windows 11 (32/64-bit)
  - Microsoft Windows 11 Home
  - Microsoft Windows 11 Pro
  - Microsoft Windows 11 Enterprise
- Microsoft Windows Server (32/64-bit)
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022

NOTE

Security patches from Microsoft

To ensure secure operation, make sure that the security patches from Microsoft are installed promptly.

5.1.2 Additional software components

To use the MFCT, also install the following software:

- Microsoft .NET Framework 4.8
  Use the Offline installer (https://support.microsoft.com/de-de/topic/microsoft-net-framework-4-8-offline-installer-f%C3%BCr-windows-9d23f658-3b97-68ab-d013-aa3c3e7495e0) to install it.
- The npcap-x.xx-oem.exe file from the folder "MFCT_xx.xx.xx.xx_xx.xx > Npcap > Misc"
  You can find the "Misc" folder in the unzipped folder of the MFCT.

Optional software installations:

- PG/PC Interface from the "Misc" folder
- Microsoft Visual C++ Redistributable Package (x86)

5.1.3 Security programs

To protect the software from unwanted manipulation, use the following security programs.

NOTE
Promptly perform updates available security programs.

Overview of virus scanners

The following virus scanners have been tested for compatibility with the systems:

- Trend Micro OfficeScan V12.0.6040 Service Pack 1
- Avira Security V1.1.86.3
- Trend Micro Apex One V14.0.12902

You can run these antivirus programs in the default setting.

Encryption software: BitLocker

BitLocker is a Windows security feature that protects your data by encrypting your drives. This encryption ensures that anyone attempting to access a data storage medium offline cannot read any of its contents.

5.1.4 Virtualization platforms

You have the option of operating the MFCT in a virtual machine (VM)

Use the following virtualization software:

- VMware vSphere Hypervisor ESXi ≥ 6.5
- VMware Workstation ≥ 15.5.0
- VMware Workstation Player ≥ 15.5.0
- Microsoft Hyper-V Server ≥ 2016

NOTE

Hardware certified by the manufacturer is recommended for the use of the following virtualization software:

- VMware vSphere Hypervisor ESXi
- Microsoft Hyper-V Server

Guest operating systems for virtualization software

Use the following guest operating systems within the selected virtualization software:

- Microsoft Windows 10 Pro (32/64-bit)
- Microsoft Windows 11 Pro (32/64-bit)

There could be restrictions with the online functions.

NOTE

The plant operator must ensure that sufficient system resources are provided for the guest operating systems.

5.2 Installation

The MFCT is provided as a portable application. To install the MFCT, proceed as follows:

1. Download (https://support.industry.siemens.com/cs/us/en/view/109773881) the MFCT as a zip file from the Internet.
2. To check the integrity of the downloaded zip file, compare the checksum of the zip file to the checksum in SiePortal.

   You can find instructions for comparing the checksums in the following FAQ on the online support page (https://support.industry.siemens.com/cs/ww/en/view/109483101).
3. If both checksums match, extract the downloaded zip file to a local drive on your PC.

Result: You have completed the installation. The MFCT is installed on your PC. Start the MFCT by double-clicking the "MFCT.exe" file in the extracted folder.

5.3 Update the MFCT installation

Always use the latest version of the MFCT.

To check whether a new version is available, proceed as follows:

1. Open the MFCT.
2. Open the "About" tab.
   You can find information about the installed version in the "Version information" area.
3. Click the "Check for updates" button.
   The MFCT checks whether a new version is available in SiePortal.

Result: You are notified if a new version is available. Otherwise, the MFCT indicates below the release date that your installation is up-to-date.

Optionally, you can select the "Check on startup" check box to have the MCFT automatically check for updates on each startup of the application.



More information

You can find more information on the "About" tab in the section Information on the "About" tab (Page 25).

Functions

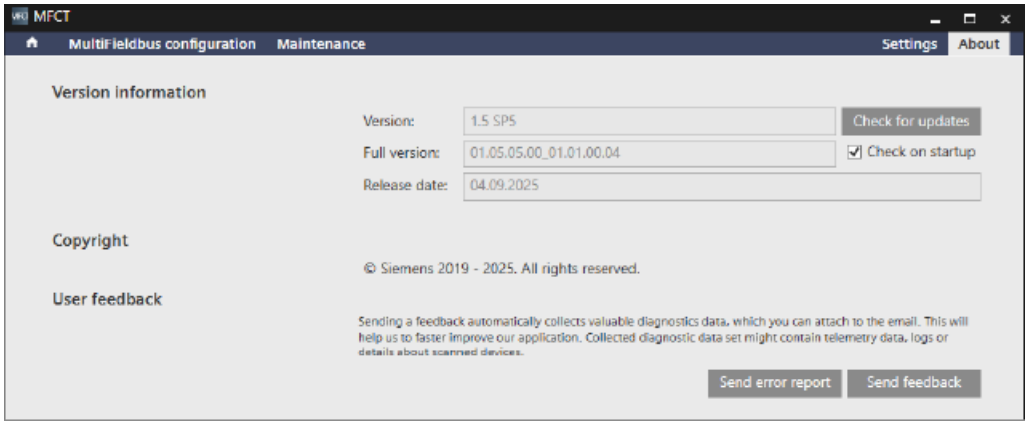
6

6.1 Information on the "About" tab

After opening the MFCT, you can find the "About" tab on the right. You can find the following information there:

- Version information
- Copyright
- User feedback

The figure below shows the contents of the "About" tab.



More information

You can learn more about version information and updates in section Update the MFCT installation (Page 24).

6.1.1 Version information

To obtain information about your installed version of the MFCT, click the "About" tab. The "Version information" area shows the following

- Version
- Full version
- Release date
- Check for updates
  You can find information on checking for updates in the section Update the MFCT installation (Page 24).

NOTE

Version of the MFCT required for operation

To ensure problem-free operation of the MFCT with an MF device, the MFCT requires at least the version required by the MF device. You can find this version in the equipment manual of the MF device used.

6.1.2 User feedback

To send error reports and feedback, click the "About" tab. The "User feedback" area offers the following options:

- Send error report:
  You can send information on collected diagnostic data.
- Send feedback:
  You can make suggestions and proposals for using the tool.

Sending an error report

To send an error report with information on collected diagnostic data, proceed as follows:

1. Select the "About" tab.
2. Click the "Send error report" button in the "User feedback" area.
   The MFCT collects diagnostic data and stores it in the MFCT installation folder under "Logs".
   The MFCT also opens a new email. The corresponding recipient is already specified in this email and the collected diagnostic data is attached as a zip file.
3. Enter additional information on the error description in the email.
4. Send the email.

Sending feedback

To make suggestions and proposals for handling the tool, proceed as follows:

1. Select the "About" tab.
2. Click the "Send feedback" button in the "User feedback" area.
   The MFCT opens a new email. The corresponding recipient is already specified in this email.
3. Enter your suggestions and proposals in the email.
4. Send the email.

6.2 Overview of the "Settings"

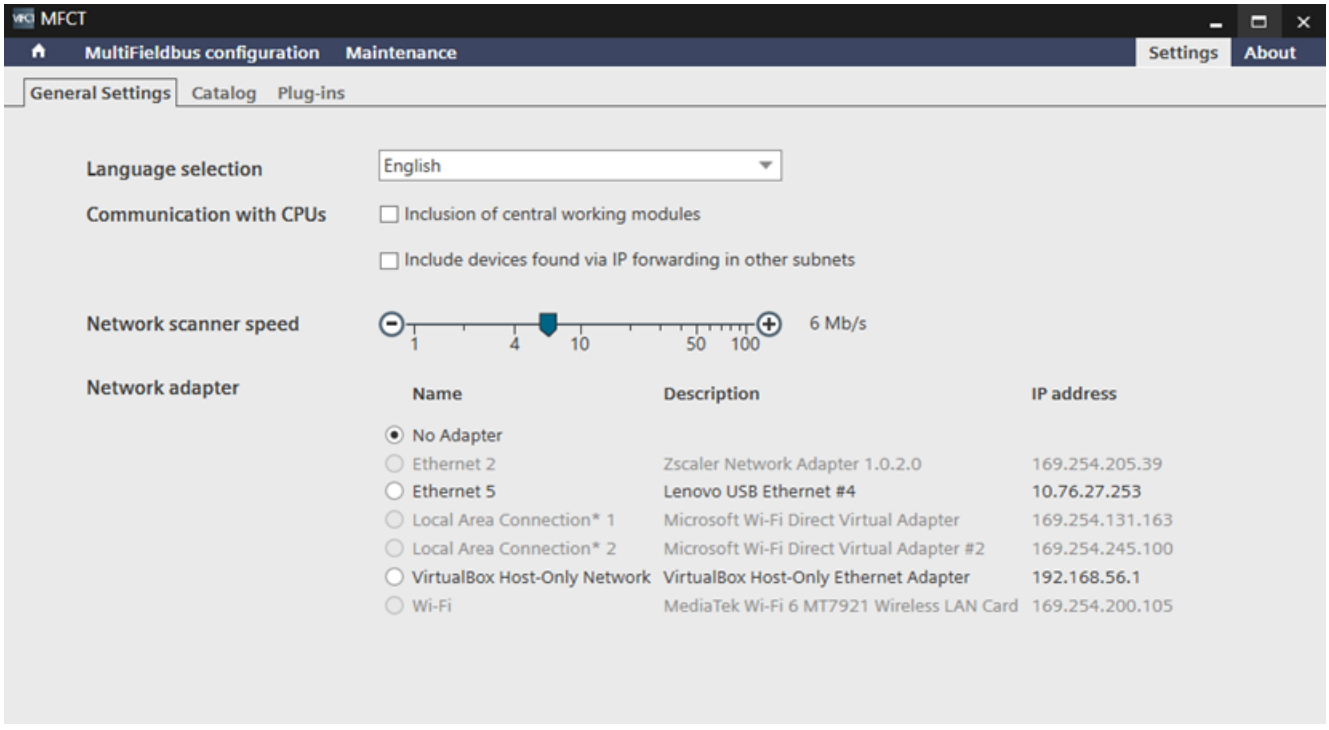
After opening the MFCT, you can find the "Settings" on the start page as an application. In an opened MFCT application, you can find the "Settings" on the right as a separate tab next to the "About" tab.

In the "Settings" tab, you have the option of configuring the basic settings of the MFCT in the following areas:

- General settings (Page 27)
- Catalog (Page 29)
- Plug-ins (Page 30)

6.2.1 General settings

The following figure shows the configuration options in the "General settings" tab:



Language selection

In the "Language selection" area, select the desired language for the user interface from the selection list. The currently supported languages are German and English.

Communication with CPUs

In the "Communication with CPUs" area, select the range in which the network scan should detect modules.

- "Inclusion of centrally working modules" check box:
  The network scan detects centrally plugged modules on a CPU.
- "Include devices found via IP forwarding in other subnets" check box:
  The network scan also detects devices in other subnets.

Network scanner speed

In the "Network scanner speed" area, select the speed at which the network is scanned.

The default setting is 6 Mbps. The highest speed that can be set is 100 Mbps.

In networks with high network load, reduce the speed of the network scanner, for example, before a firmware update. A firmware update of more than 20 devices results in a network load of approx. 3 Mbps.

Network adapter

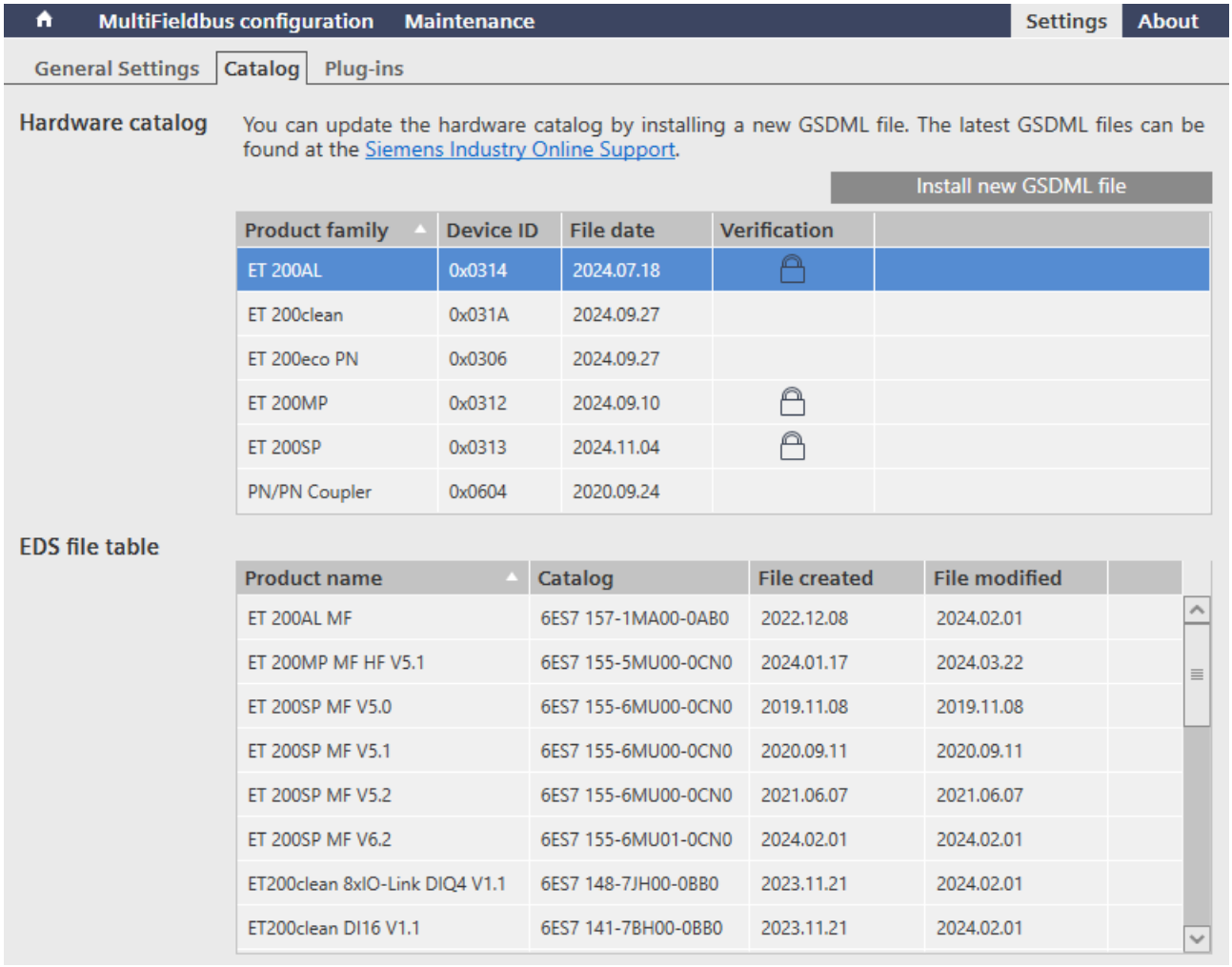
In the "Network adapter" area, you can see all available network adapters on your PC with the configured settings.

- The activated network adapters of your PC are black and can be selected.
- The deactivated network adapters of your PC are displayed grayed out.

The MFCT can only establish a connection to the devices if a network adapter is selected.

6.2.2 Catalog

The following figure shows an example of the contents of the "Catalog" tab:



Hardware catalog

You can find the currently installed GSDML files in the "Hardware catalog" area.

If the "Verification" column displays a padlock symbol, then this device originates from a GSDX-container for which the signature has been successfully verified.

To install additional GSDML files or update the GSDML files used, click the "Install new GSDML file" button.

You can find the GSDML/GSDX files used and additionally installed in the folder "MFCT_xx.xx.xx.xx_xx.xx > GSD"

EDS file table

In the "EDS file table" area, you can find the EDS files used in the MFCT.

An EDS file (Electronic Data Sheet) is an ASCII text file that contains all the relevant information of a user application. The files are used by configuration tools and controllers, for example, to integrate and configure sensors or field bus components in networks.

You can only create and configure EDS files with the MFCT (generic EDS file).

You can find the used and additionally generated EDS files in the folder "<MFCT_xx.xx.xx.xx_xx.xx > EDS".

To transfer your configuration from the MFCT project to your MF device, you need to extract the EDS file. You can find information on extracting the EDS file in the section Transfer the configuration (Page 48).

NOTE

For integration in EtherNet/IP configuration systems, use a generic EDS file according to CIP specification Vol. 1.

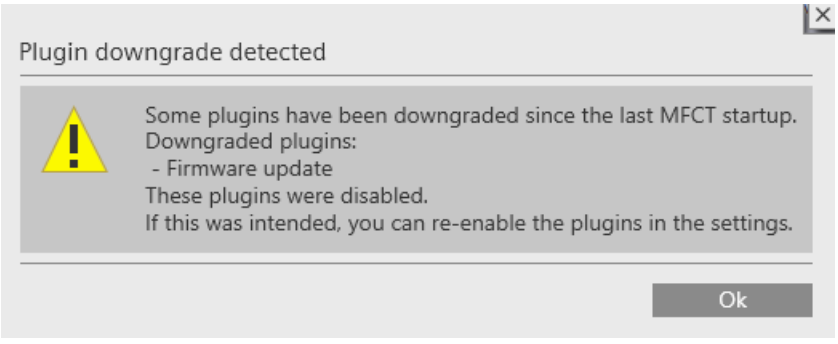
More information

You can find an overview of the most important documents and links to MultiFieldbus in the following Internet article (https://support.industry.siemens.com/cs/ww/en/view/109779189).

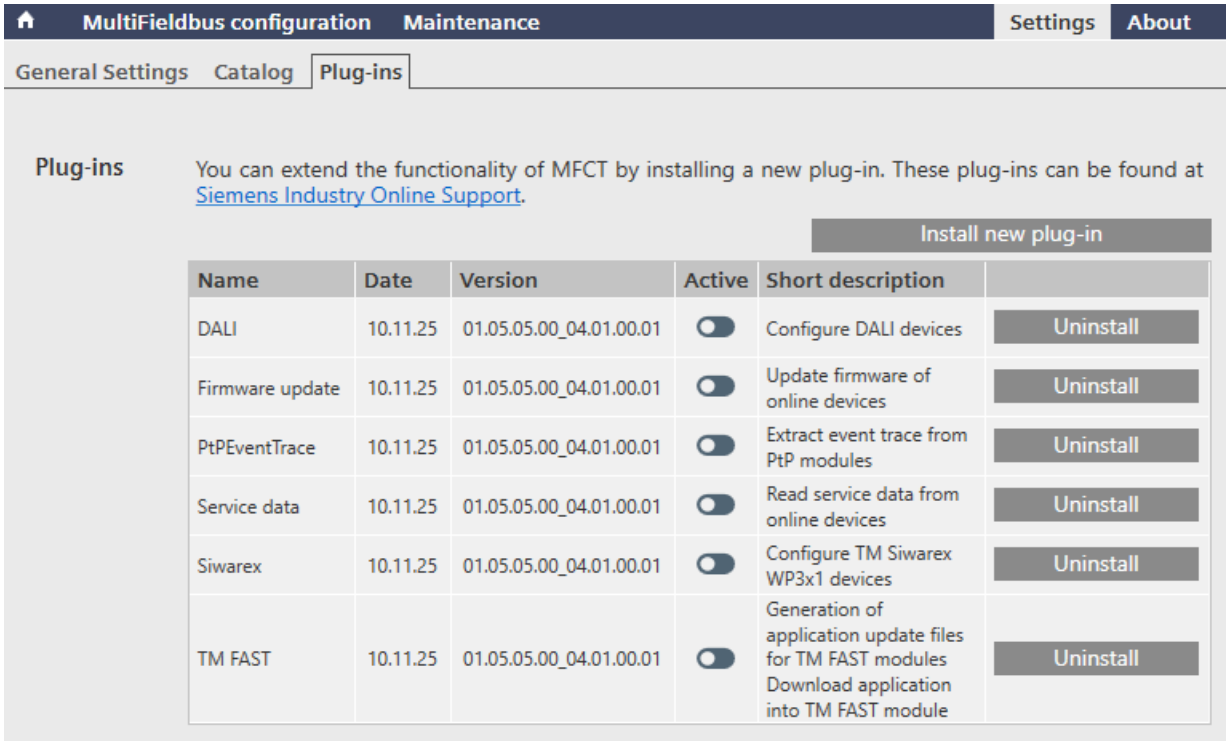
6.2.3 Plug-ins

Plug-ins supplement the MFCT with additional functions not originally supported in the main application.

On startup, the MFCT checks whether all activated plug-ins match the installed MFCT version. If a plug-in from a previous MFCT version is found, it is disabled by the MFCT.
If you want to continue working with a previous version of a plug-in, you can re-enable the plug-in on the "Plug-ins" tab. The warning is no longer displayed on the next start-up.
The MFCT displays the following warning on the start page:



In the "Plug-ins" tab, you can install, activate/deactivate and uninstall the plug-ins. The figure below shows the contents of the "Plug-ins" tab.



Installing

To install a new plug-in, click the "Install new plug-in" button.

"Active" column

You have the following options in the "Active" column:

- Activate available plug-ins: To activate the plug-in for the desired function, drag the slider to the right.
- Deactivate available plug-ins: The default setting is generally deactivated. To deactivate an activated plug-in, drag the slider to the left. The deactivation only takes effect when you restart the MFCT.

Uninstalling

To uninstall a plug-in, click the "Uninstall" button.

NOTE

Uninstalled plug-ins

If you uninstall a plug-in, the plug-in is completely removed and is no longer available to the MFCT.

If you need the uninstalled plug-in again, download the plug-in from the Siemens Industry Online Support page and reinstall the plug-in using the "Install new plug-in" button.

MultiFieldbus configuration 7

You have the following options in the "MultiFieldbus configuration" application:

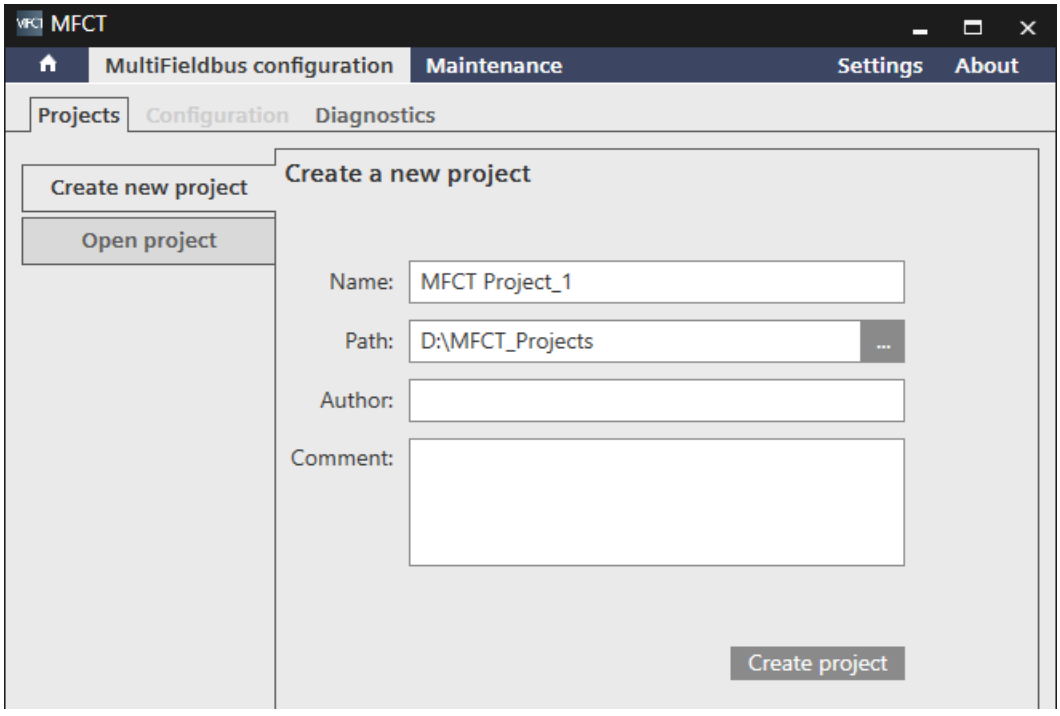
- Configure the basic settings for your MFCT project.
- Configure and assign parameters to the required MF devices for your MFCT project.
- Perform diagnostics on MF devices that can be accessed online.

After opening the MFCT, you can find the "MultiFieldbus configuration" as an application on the start page. In an application of the MFCT that is already open, you can find the MultiFieldbus configuration as a tab in the area of the button for the start screen.

7.1 Creating new MultiFieldbus project in MFCT

To create a new project in the MFCT, proceed as follows:

1. Select the "MultiFieldbus configuration" application.
2. Select the "Projects" tab.
3. Click "Create new project".
4. Assign a name for your project, e.g. MFCT Project_1.
5. Select the storage location for your MFCT project next to "Path".
6. Optionally, you can describe the project with author and comments.
7. Click "Create project".

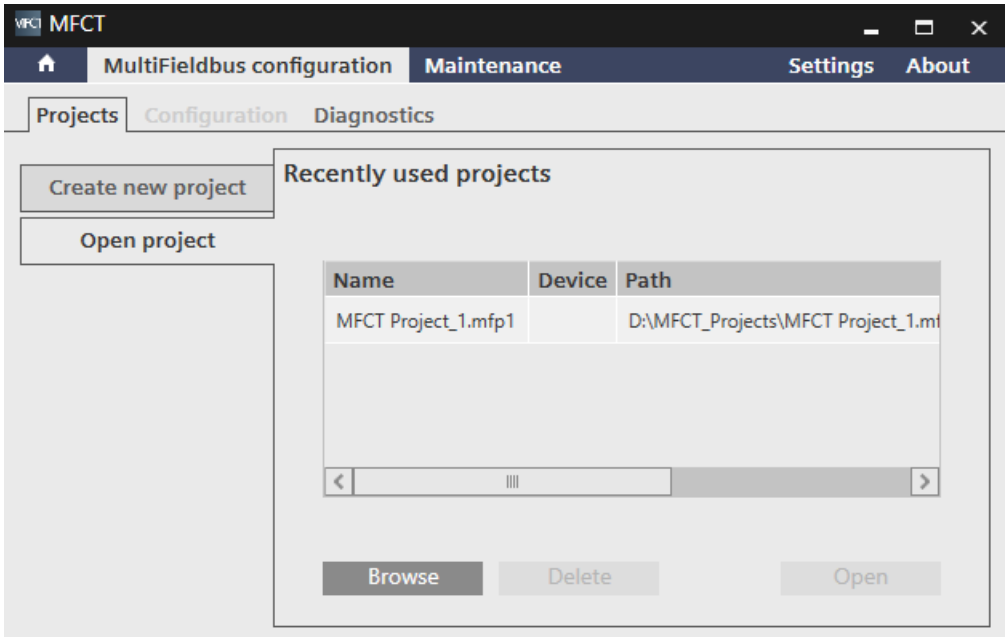


Result: MFCT creates the project under the selected path and switches to the "Configuration" (Page 35) tab for the next processing step.

7.2 Open MultiFieldbus project in MFCT

To open an existing MFCT project, proceed as follows:

1. Select the "MultiFieldbus configuration" application.
2. Select the "Projects" tab.
3. Click the "Open project" button.
   The "Recently used projects" area shows a list of the most recently used MFCT projects.
4. Select one of the following options:
   – If the list contains the desired project, click the desired project.
   To open the project, click the "Open" button or double-click the project.
   – If the list does not show the desired project, click the "Browse" button.
   Navigate to the desired project in the file explorer and select the file MFP1file.
   To open the project, click the "Open" button.



Result: MFCT opens the selected project and switches to the "Configuration" (Page 35) tab for the next processing step.

NOTE

You can use the "Delete" button to delete selected entries from the "Recently Used Projects" list. The project file itself is not deleted by this action.

7.3 Selecting a station

In the "MultiFieldbus configuration" application, you configure the devices for your project in the "Configuration" tab. To add devices to your project, you have the following options in the "Select station" area:

- Catalog:
  If the real MF device is not available or you want to configure an MF device offline.
- Network:
  If the real MF device is available online and you want to load this configuration into the MFCT project.
- Project:
  If you want to transfer MF devices from another project to this project.

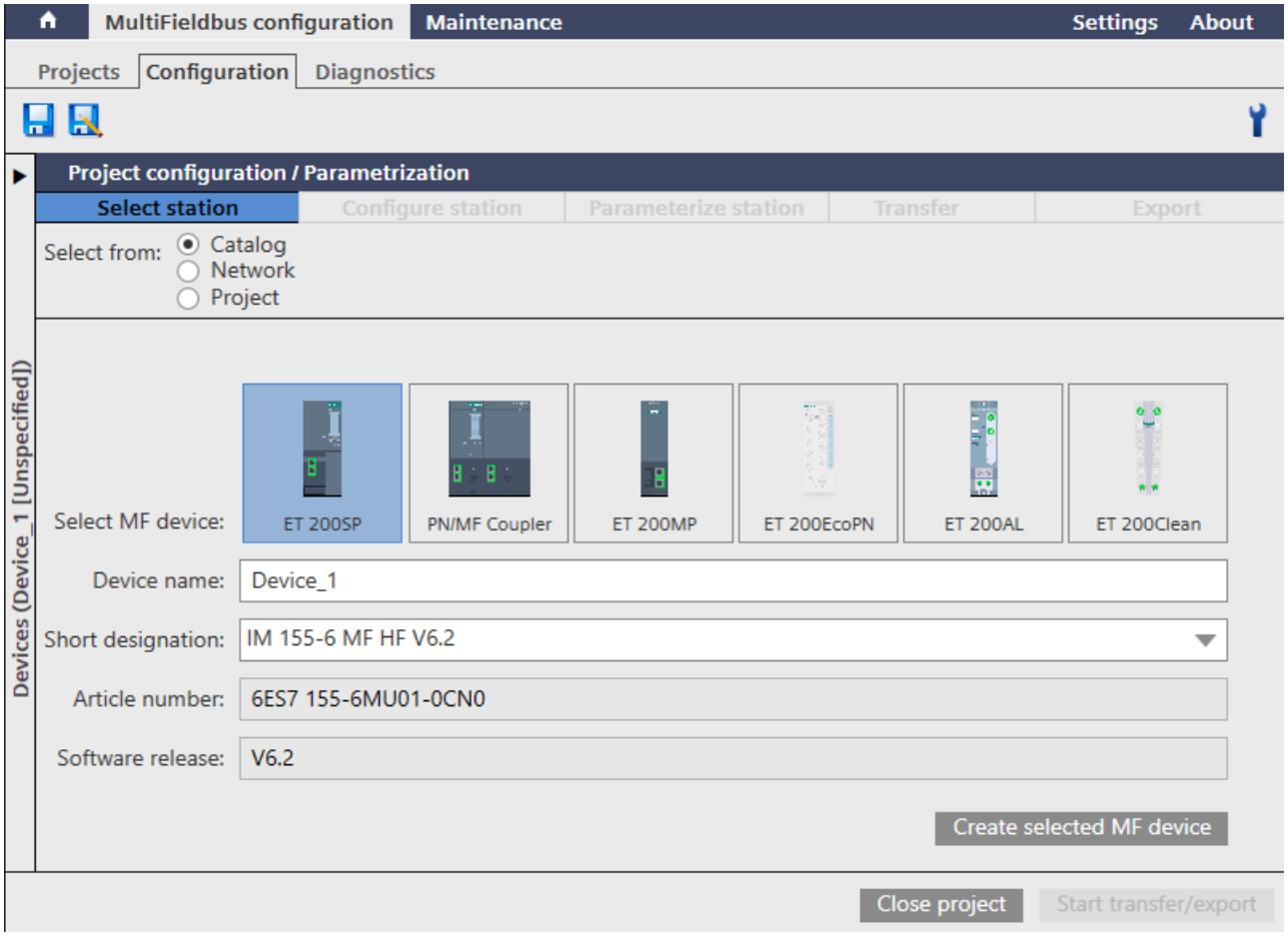
In the following sections, you can read the respective procedure for adding MF devices to your project.

Add an MF device from the catalog

To add an MF device from the catalog to your project, proceed as follows:

1. In the "Devices" area, select the "Add new device" entry.
   The MFCT creates a new device. The "Project configuration / Parameterization" area shows the other options for station selection under "Select station".
2. Select the "Catalog" option.
3. Select the product family, e.g. ET 200SP.
4. Assign a name for the MF device, e.g. Device_1.
5. Select the desired MF device from the "Short designation" selection menu.
   The "Article number" and "Software version" fields show the corresponding data.

6. Click the "Create selected MF device" button.



Result: MFCT adds the device to the project and automatically switches to the next step "Configure station" (Page 39).

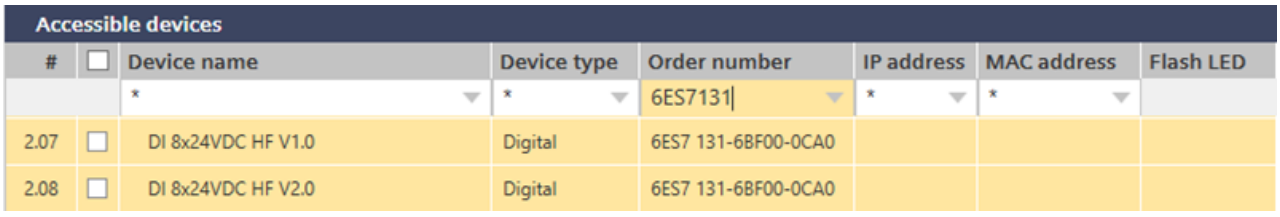
Add an MF device from the network

Requirement: The selected network adapter can access the desired MF device.

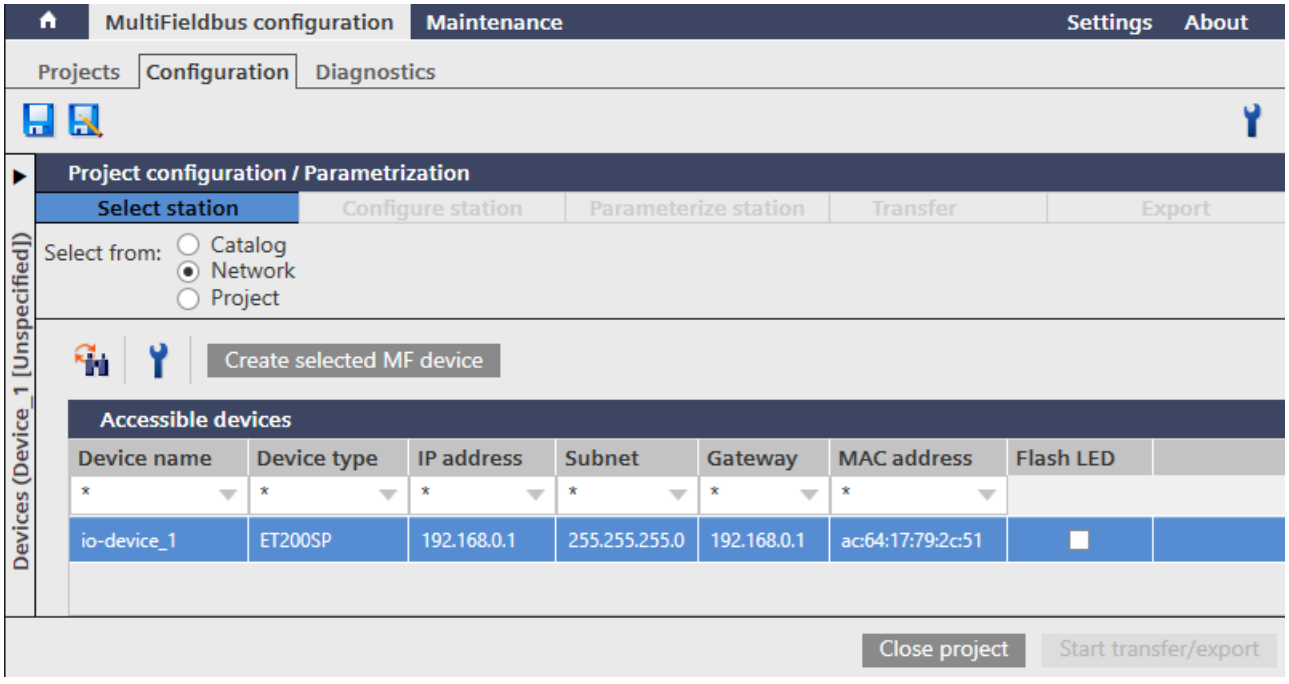
To add an MF device that can be accessed online to your project, proceed as follows:

1. In the "Devices" area, select the "Add new device" entry.
   The MFCT creates a new device. The "Project configuration / Parameterization" area shows the other options for station selection under "Select station".
2. Select the "Network" option.
3. Click the "Start scan" button.
   The MFCT searches for devices that are accessible online and displays the results in the "Accessible devices" table. Devices without MultiFieldbus support are grayed out and cannot be selected.
4. If the "Accessible devices" table does not show any results, click the "Scan settings" button .
   MFCT opens the "Scan settings (Page 92)" window to configure the settings.

5. Optional: Use the incremental search function to locate the desired MF devices. The search starts immediately after you enter the first character. The search query is refined with each additional character. The results are dynamically adapted according to your entry.



6. Select the desired MF device in the "Accessible devices" table.
7. Click "Create selected MF device".



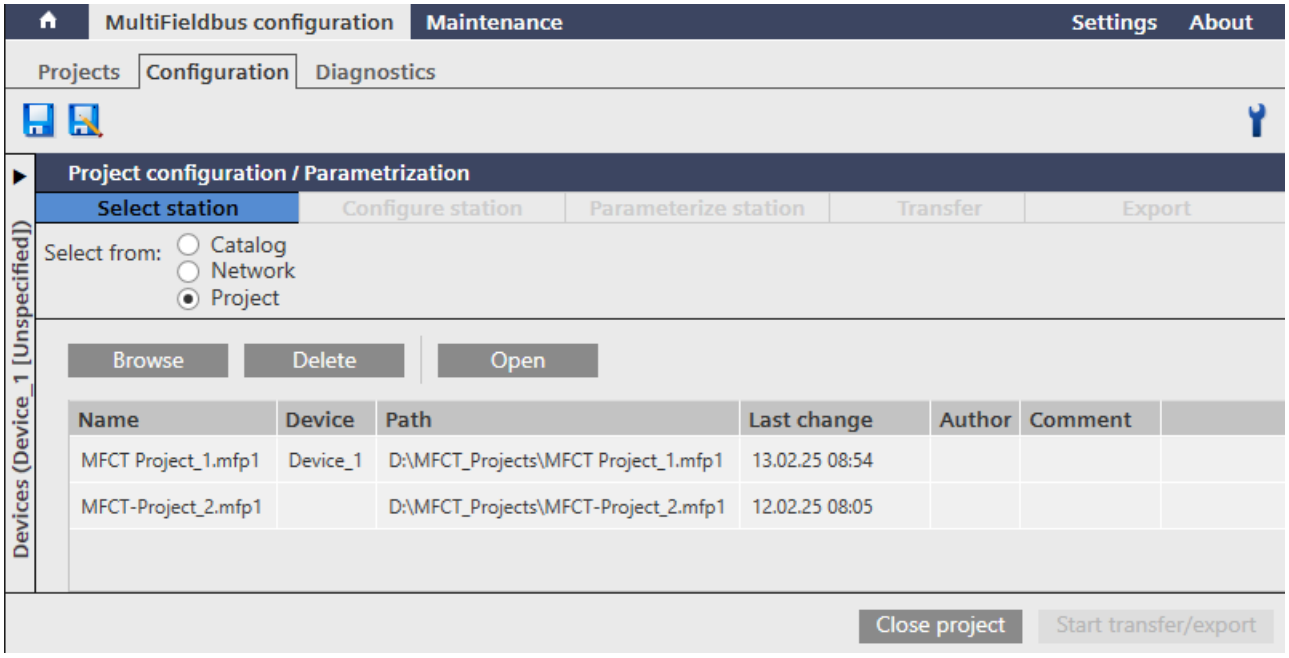
Result: MFCT reads the configuration from the MF device, transfers the configuration to the MF device added in your project and automatically switches to the next step "Configure station (Page 39)".

Add an MF device from a project

To add an MF device from another project to your project, proceed as follows:

1. In the "Devices" area, select the "Add new device" entry.
   The MFCT creates a new device. The "Project configuration / Parameterization" area shows the other options for station selection under "Select station".
2. Select the "Project" option.
   The MFCT displays a list of the most recently used MFCT projects.

3. Select one of the following options:
   - If the list contains the desired project, click the desired project.
     To open the project, click the "Open" button or double-click the project.
   - If the list does not show the desired project, click the "Browse" button.
     Navigate to the desired project in the file explorer and select the file MFP1file.
     To open the project, click the "Open" button.



Result: MFCT loads all MF devices from the selected project into your project and automatically switches to the next step "Configure station" (Page 39).

NOTE

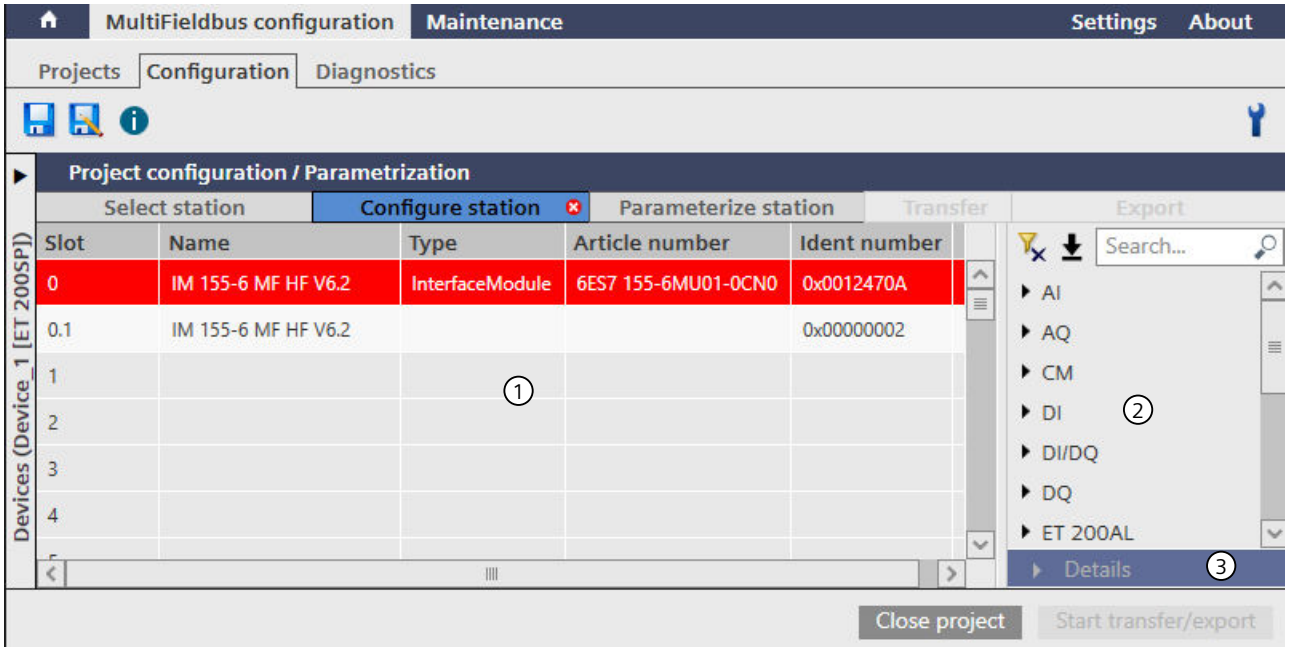
You can use the "Delete" button to delete selected entries from the "Recently Used Projects" list. The project file itself is not deleted by this action.

7.4 Configuring a station

After you have selected your required MF devices in the "Select station" area, configure your MF devices with all the required modules in the "Configure station" area.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

The following figure shows the "Configure station" area in the "Configuration" tab:



① Station setup

This area shows the structure of the MF device as a list, sorted by slots in ascending order. Incorrect configurations are displayed in red. In this example, a server module has not yet been added for the IM 155-6 MF HF interface module.

② Hardware catalog

The hardware catalog shows the modules that, based on the installed GSDML files, you can use for your MF device.

③ Details

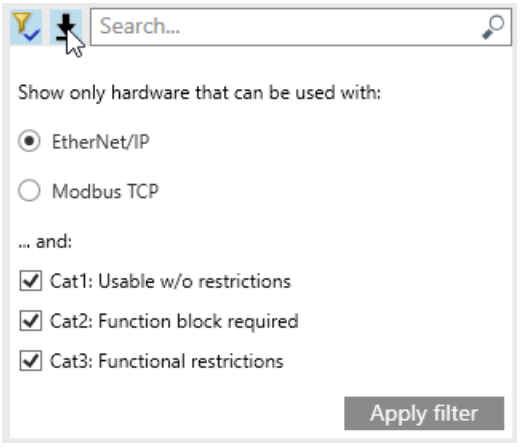
If you select a module in the hardware catalog, you can display information on the selected module and its use on fieldbuses in the "Details" area. To open the detailed view for a module from the hardware catalog, double-click the "Details" entry.

Filter function via modules of the hardware catalog

You can use the filter function to restrict the hardware catalog depending on the fieldbus and the category.

To activate the filter function, proceed as follows:

1. Open the list with the filter criteria.



2. Select the desired fieldbus.
3. Select the desired categories.
4. Activate the filter function using the "Apply filter" button.

Result: The hardware catalog only shows modules that match the filter criteria.

To disable the filter function, click the filter symbol.



Add modules

To add modules from the hardware catalog to your MF device, proceed as follows:

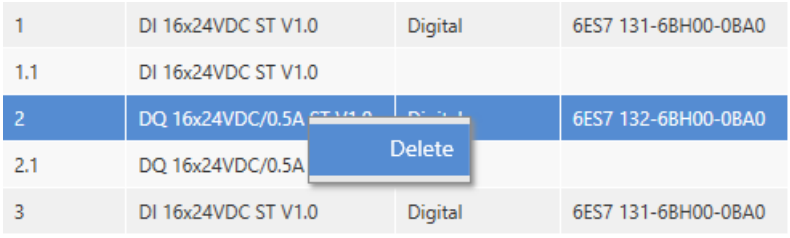
1. Navigate to the required module in the hardware catalog.
2. Select the required module version, e.g. V1.0.
3. Drag-and-drop the module to the desired slot in the station setup.
   The possible slots for the selected module are highlighted in green on the MFCT.
4. Repeat steps 1 and 2 to add further modules from the hardware catalog to your MF device.

Result: You have added the desired modules to your MF device. The corresponding submodules are automatically added for each module.

Delete modules

To delete modules on the MF device, proceed as follows:

1. Select the module to be deleted in the list view.
2. Right-click the module to be deleted.
3. Select "Delete" in the context menu.



Result: You have deleted the module.

Example configuration for a PN/MF-Coupler

The following figure shows an example of the configuration of the network page X1 of a PN/MF coupler.

1	OUT 64 Byte	Output		0x04400000
1.1	OUT 64 Byte			0x00000001
2	IN 128 Byte+DS	Input		0x00000480
2.1	IN 128 Byte+DS			0x00000001

In this example 64 bytes are written to the network page X2 and 128 bytes are read from the network page X2.

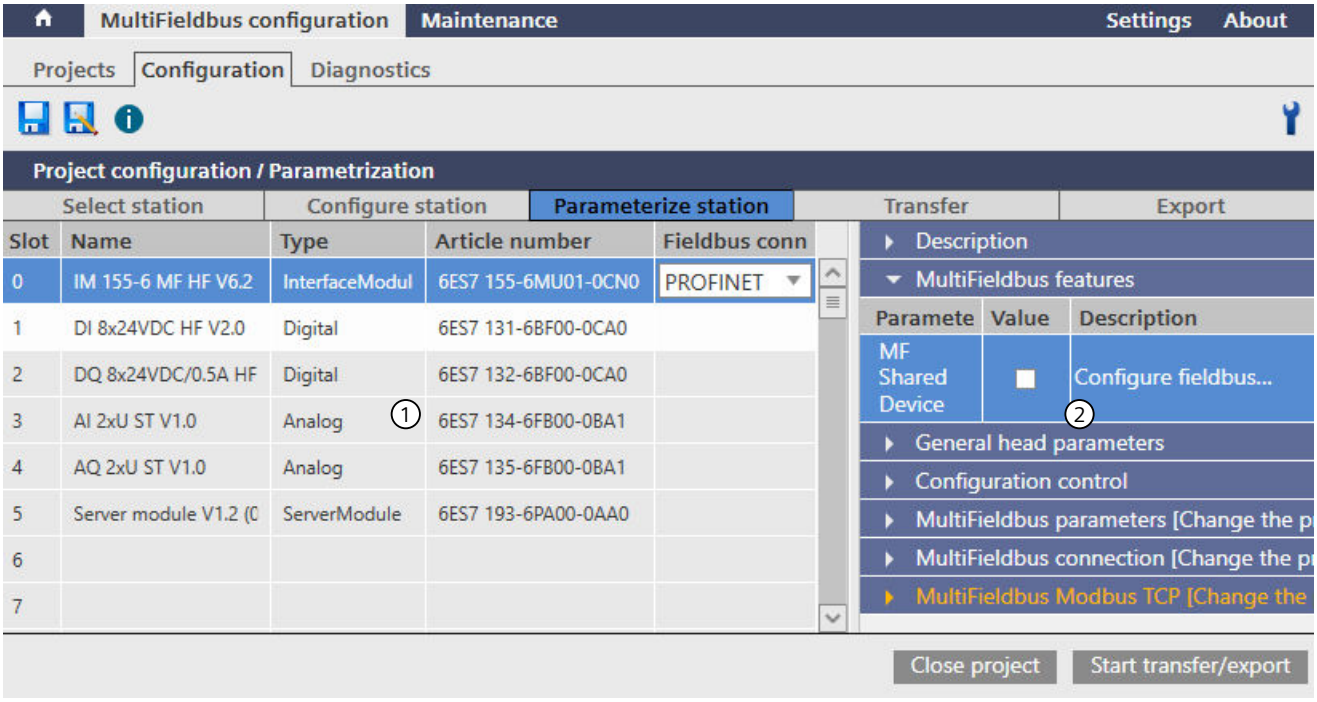
You can find information on how to use the network page X2 with STEP 7 (TIA Portal) with GSD file in the "PN/MF Coupler (https://support.industry.siemens.com/cs/ww/en/view/109781406)" installation and operating manual.

7.5 Parameterizing the station

After you have configured your MF devices with all the required modules in the "Configure station" area, configure the modules of the station in the "Parameterize station" area.

A tooltip above the MF device displays the amount of I/O data available and the amount currently used.

The following figure shows the "Parameterize station" area in the "Configuration" tab:



① Station setup

This area shows the structure of the MF device as a list, sorted by slots in ascending order. In this example, the IM 155-6 MF HF interface module was configured with digital and analog modules.

② Configure the parameters of the modules

This area shows the configurable parameters for the selected module in the list view ①.

You can find information on the MultiFieldbus properties in the respective equipment manual for the module. You can find an overview in the section Reference documents (Page 6).

Procedure - Configure different fieldbuses

If an MF device supports the "MF Shared Device" function, you can configure different fieldbuses for all modules. To configure different fieldbuses for the modules of the MF device, proceed as follows:

1. In the list, select the interface module in slot 0.
   The MFCT shows the configurable parameters for the selected module.
2. Open the "MultiFieldbus properties" selection menu.
3. Activate the "MF Shared Device" option.
   The MFCT displays a selection menu next to each module in the "Fieldbus connection" column. The configured fieldbus connection of the interface module is adopted in the basic settings, e.g. PROFINET.
4. Select the fieldbus connections for the modules in the selection menus.

Project configuration / Parametrization

Select station		Configure station		Parameterize station
Slot	**Name**	**Type**	**Article number**	**Fieldbus connection**
0	IM 155-6 MF HF V6.2	InterfaceModule	6ES7 155-6MU01-0CN0	PROFINET
1	DI 8x24VDC HF V2.0	Digital	6ES7 131-6BF00-0CA0	ModbusTCP #0 (0x000, 0x2D0)
2	DQ 8x24VDC/0.5A HF V2.0	Digital	6ES7 132-6BF00-0CA0	EtherNet/IP #0 (0x301, 0x300)
3	AI 2xU ST V1.0	Analog	6ES7 134-6FB00-0BA1	PROFINET
4	AQ 2xU ST V1.0	Analog	6ES7 135-6FB00-0BA1	PROFINET
5	Server module V1.2 (0 bytes)	ServerModule	6ES7 193-6PA00-0AA0	PROFINET
6				

Result: You have configured different fieldbuses for the modules.

Procedure - Configure the Modbus TCP fieldbus connections

Optionally, you can configure the hold times for all Modbus TCP field bus connections as follows:

1. In the list, select the interface module in slot 0.
   The MFCT shows the configurable parameters for the selected module.
2. Edit the following values for the desired Modbus TCP fieldbus connections in the "MultiFieldbus Modbus TCP" selection menu:
   - Connection hold time:
     The default setting is 5 000 ms. You can edit the value in a range from 1 to 30 000 ms.
   - Reset hold connection:
     The default setting is 0 ms. You can edit the value in a range from 1 to 30 000 ms.

Result: You have configured the hold times for the desired Modbus TCP field bus connections.

More information

If you change the configuration from PROFINET to EtherNet/IP or Modbus TCP, a parameterization error may occur in connection with the change of BusAdapter type. You can only remedy the parameterization error with a reset to factory settings (Page 92) and reconfiguration with MFCT.

You can find information on restrictions in the equipment manuals of the MF devices used.

7.5.1 Parameterizing the I/O data alignment

In MFCT you generate and export the I/O data alignment for modules with a fieldbus connection over EtherNet/IP. The MFCT exports the generated data as a user-defined data type (User Defined Type, UDT) in an I5x file. In addition, the MFCT generates a CSV file in which byte addresses are assigned to the slots and modules.

For further processing, the user must find the required values in the UDT and insert them into a tag in the user program. Only in this way can the values be arranged in the required order. The larger the UDT is, the greater the effort will be to find the required values in the UDT.

As of MFCT version V1.5 SP5, you can configure flexible I/O data alignment for EtherNet/IP. You can configure the order of the required I/O data already in the MFCT. The MFCT generates the UDT according to your configuration. This enables you to find the required values in the UDT more quickly and avoid having to make extensive modifications in the user program of the higher-level IO controller.

The next sections provide information on the configuration options.

Selecting flexible I/O data alignment for EtherNet/IP

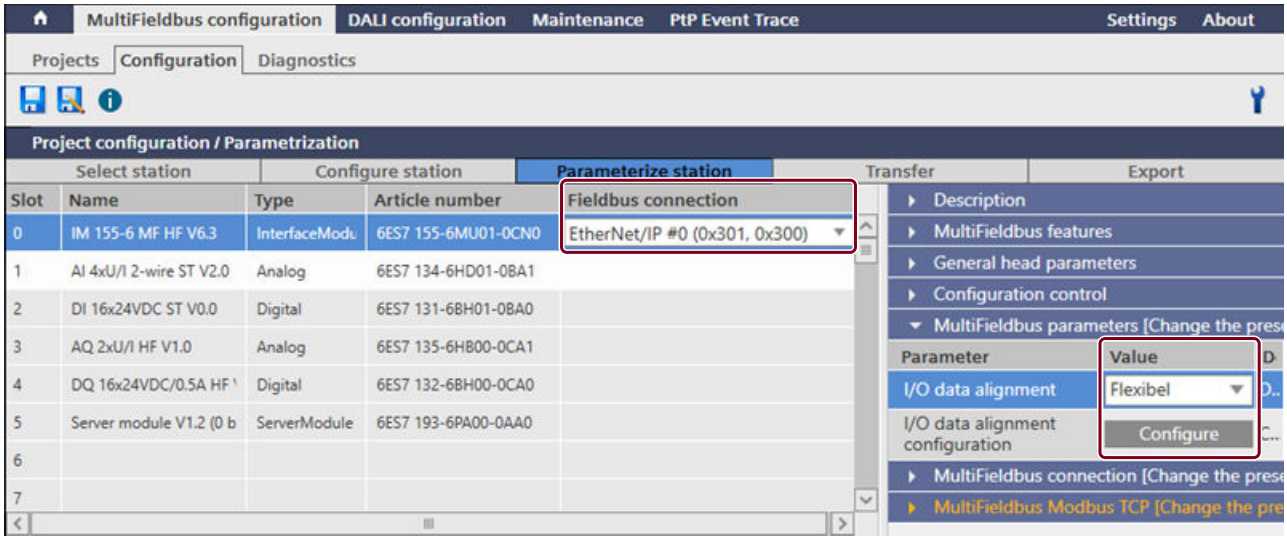
You can find the configuration options for the I/O data alignment in the module parameters of the interface module under "Parameterize station > MultiFieldbus parameters > I/O data alignment". You can choose between the following standard values in the "I/O data alignment" selection menu:

- Byte (default)
- Word

To select the flexible I/O data alignment for EtherNet/IP, proceed as follows:

1. Select the desired interface module in the "Parameterize station" area.
2. Select a fieldbus connection over EtherNet/IP.
3. Navigate in the right window to the "MultiFieldbus parameters > I/O data alignment" area.

4. Select "Flexibel" in the drop-down menu next to "I/O data alignment".
   An additional line "I/O data alignment configuration" appears below the drop-down menu.



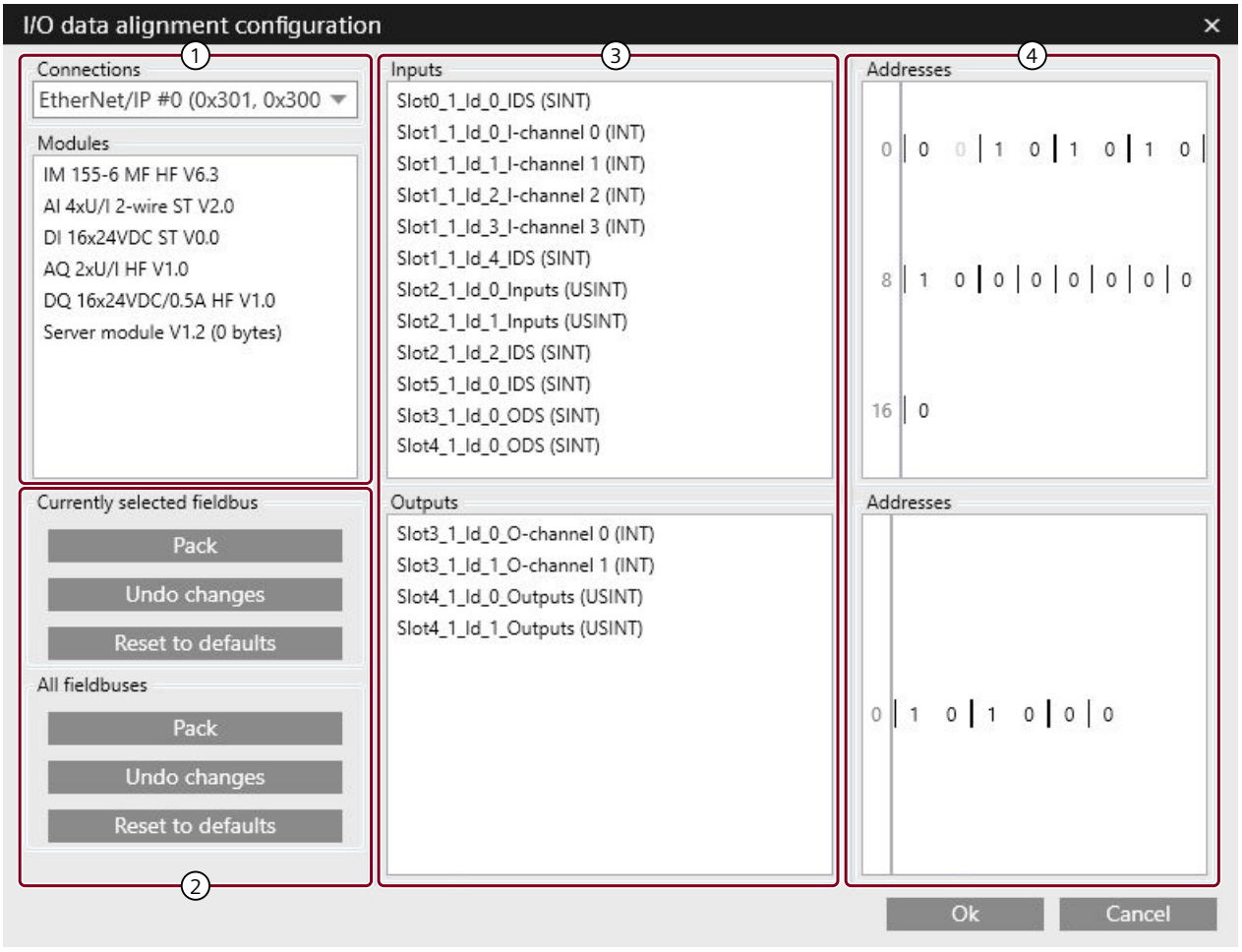
Result: You have selected a fieldbus connection over EtherNet/IP and the flexible I/O data alignment.

If you click the "Configure" button, the MFCT opens the editor for configuring the I/O data alignment.

Editor for configuring the I/O data alignment

In the "I/O data alignment configuration" editor, you configure the order of the inputs and outputs for the UDT. The next sections provide information on the various areas.

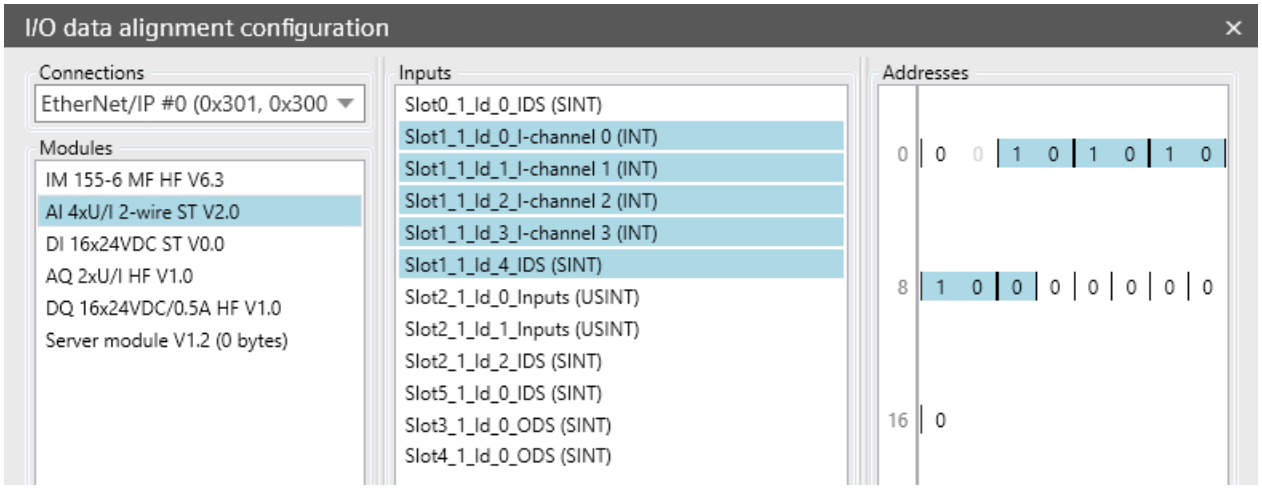
The figure below shows the "I/O data alignment configuration" editor.



① Connections and Modules

In the drop-down menu in the "Connections" area, you select the connection for which you want to configure the order of the input and output data.

In the "Modules" area, you see the modules for which the selected connection has been configured. If you select an input module, for example, then the associated data is highlighted in color in the "Inputs" and "Addresses" areas, as shown in the following figure.



② Buttons for configuration and reset

The following buttons provide configuration options that you can apply to the selected fieldbus or all fieldbuses:

- Pack:
  Arranges the data by size, starting with the largest elements. This removes padding bytes and reduces the size of the UDT.
- Undo changes:
  Resets changes.
- Reset to defaults:
  Resets the configuration to the default configuration.

③ Inputs and outputs

The "Inputs" and "Outputs" areas show all available input and output data of the selected connection.

If you select an entry in the "Inputs" or "Outputs" area, other entries belonging to the module are shown in gray.
The "Modules" and "Addresses" areas behave as follows:

- Modules:
  The module to which the selected entry belongs is highlighted in color.
- Addresses:
  The addresses belonging to the selected entry are highlighted in color. Other addresses that belong to the module are shown in gray.

④ Addresses of inputs and outputs

The "Addresses" areas show the respective address ranges of the selected input and output data. If you select an address range, this address range is highlighted in color. Other address ranges that belong to the module are shown in gray.

If you select an address range of input data, for example, then the "Modules" and "Inputs" areas behave as follows:

- Modules:
  The module to which the selected address range belongs is highlighted in color.
- Inputs:
  The entry to which the selected address range belongs is highlighted in color. Other entries that belong to the module are shown in gray.

Changing the order of input and output data

You configure the order of the input and output data for the UDT in the "Inputs" and "Outputs" areas.

To change the order of the entries, proceed as follows:

1. Left-click on the desired entry in the "Inputs" or "Outputs" area and hold down the left mouse button.
2. Drag the entry to the desired position.
   You can only move input data within the "Inputs" area. You can only move output data within the "Outputs" area.
3. Release the left mouse button.
4. Repeat steps 1 through 3 for other entries that you want to move.

Result: You have configured the order of the input and output data. The "Addresses" areas next to the "Inputs" and "Outputs" areas are automatically adjusted to reflect the changed order.

Click the "OK" button to apply the changes. The MFCT closes the "I/O data alignment configuration" editor.

7.6 Transfer the configuration

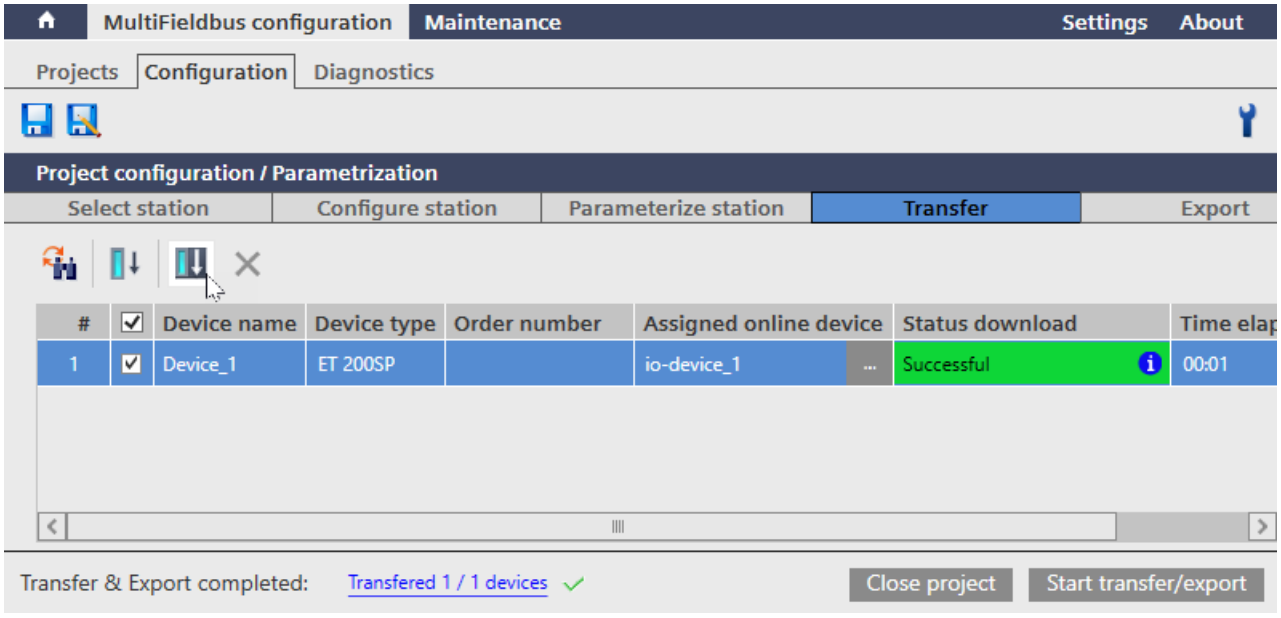
Once you have configured your station with the modules in the "Parameterize station" area, the following options are available to you:

- Transfer configuration:
  You load the configuration into the MF device that can be accessed online.
- Export configuration:
  You export the configuration for use in other engineering tools. You can learn how to export the configuration in the section Exporting the configuration (Page 50).

Transfer the configuration to the MF device

To transfer the configured and parameterized station to the MF device, proceed as follows:

1. Select the "Transfer" function in the "Configuration" tab.
   The MFCT displays the configured devices as a list.
2. In the list, select the device that you want to transfer to the MF device that is accessible online.
3. In the "Assign device online" column, click the button next to the "<Select device>" entry.
   The MFCT opens another "Accessible devices" window.
4. In the "Accessible devices" window, click the"Start scan" button .
   The MFCT shows the accessible devices for the download as a list. Devices without MultiFieldbus support cannot be selected and are shown grayed out.
5. Select an MF device from the list.
6. Click the "Assign device" button.
   The MFCT closes the "Accessible devices" window. You can see the selected device in the "Assign device online" column.
7. Click the "Start transfer of configuration" button.
   The MFCT loads the configuration into the selected MF device. You can see the progress and status in the "Download status" column.



Result: You have transferred your configuration to the MF device.

NOTE

Transferring and exporting configuration

If you click the "Start transfer of configuration" button, the configuration is transferred to the MF device.

If you click the "Start transfer/export" button, the configuration is transferred to the MF device and also exported.

Troubleshooting - Timeout during transfer to the MF device

If the transfer of the configuration to the MF device exceeds a defined time window, the MFCT shows the error as a timeout under "Download status". To correct the error, you have the following options, for example:

- Check the network accessibility of the MF device via the network adapter selected in MFCT.
- Disconnect the connection of the MF device to PROFINET I/O controllers.
- If you have selected the option "Use router for gateway" in the network parameters, check the network parameters of the device.

7.7 Exporting the configuration

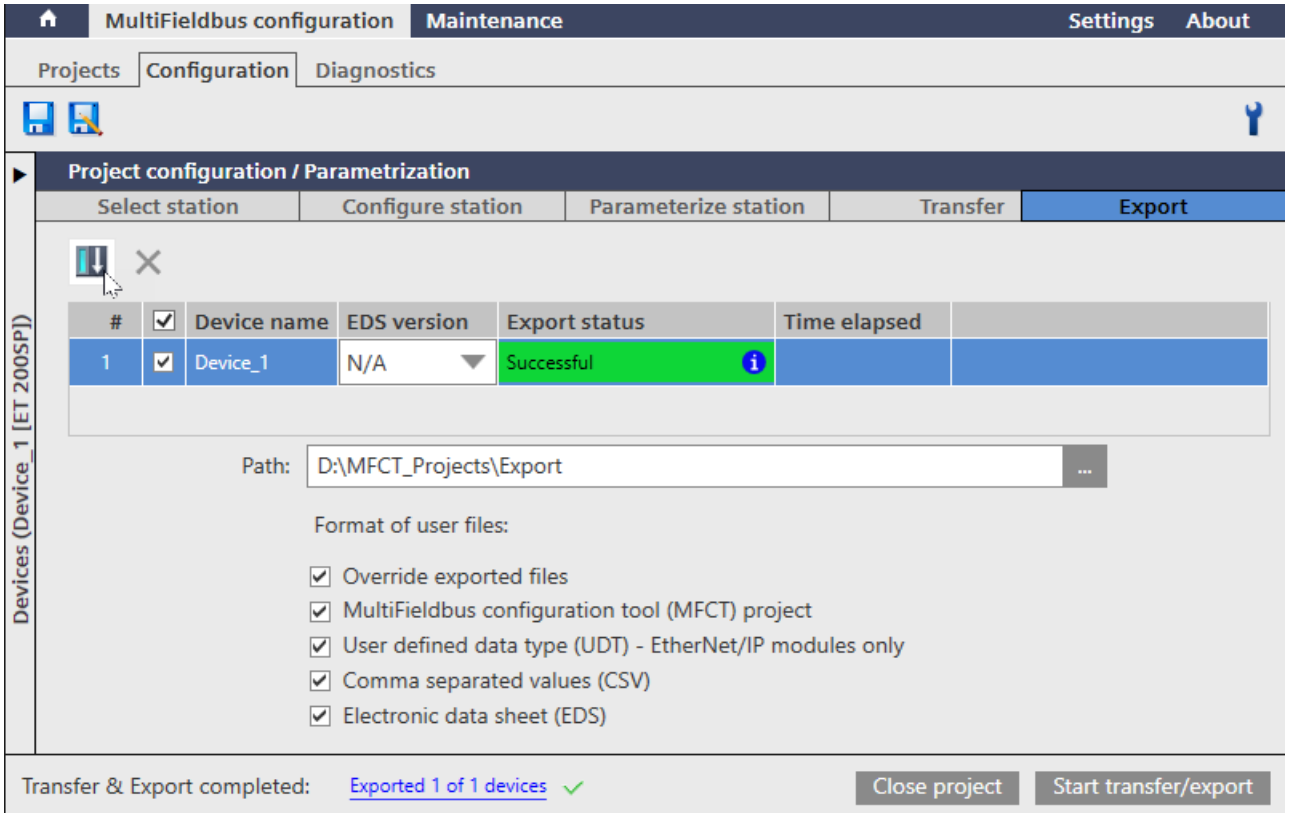
Once you have configured your station with the modules in the "Parameterize station" area, the following options are available to you:

- Export configuration:
  You export the configuration for use in other engineering tools.
- Transfer configuration:
  You load the configuration into the MF device that can be accessed online. You can learn how to export the configuration in the section Transfer the configuration (Page 48).

Exporting the configuration

To export the configured and parameterized station, proceed as follows:

1. Select the "Export" function in the "Configuration" tab.
   The MFCT displays the configured devices as a list.
2. Select the device you want to export from the list.
3. Next to "Path", select the storage location for the data to be exported.
4. Select the files to be exported in the "Format of user file" area.
5. Click the "Start configuration export" button.
   The MFCT exports the configuration to the selected storage location.



Result: You have exported your configuration to the selected storage location.

NOTE

Transferring and exporting configuration

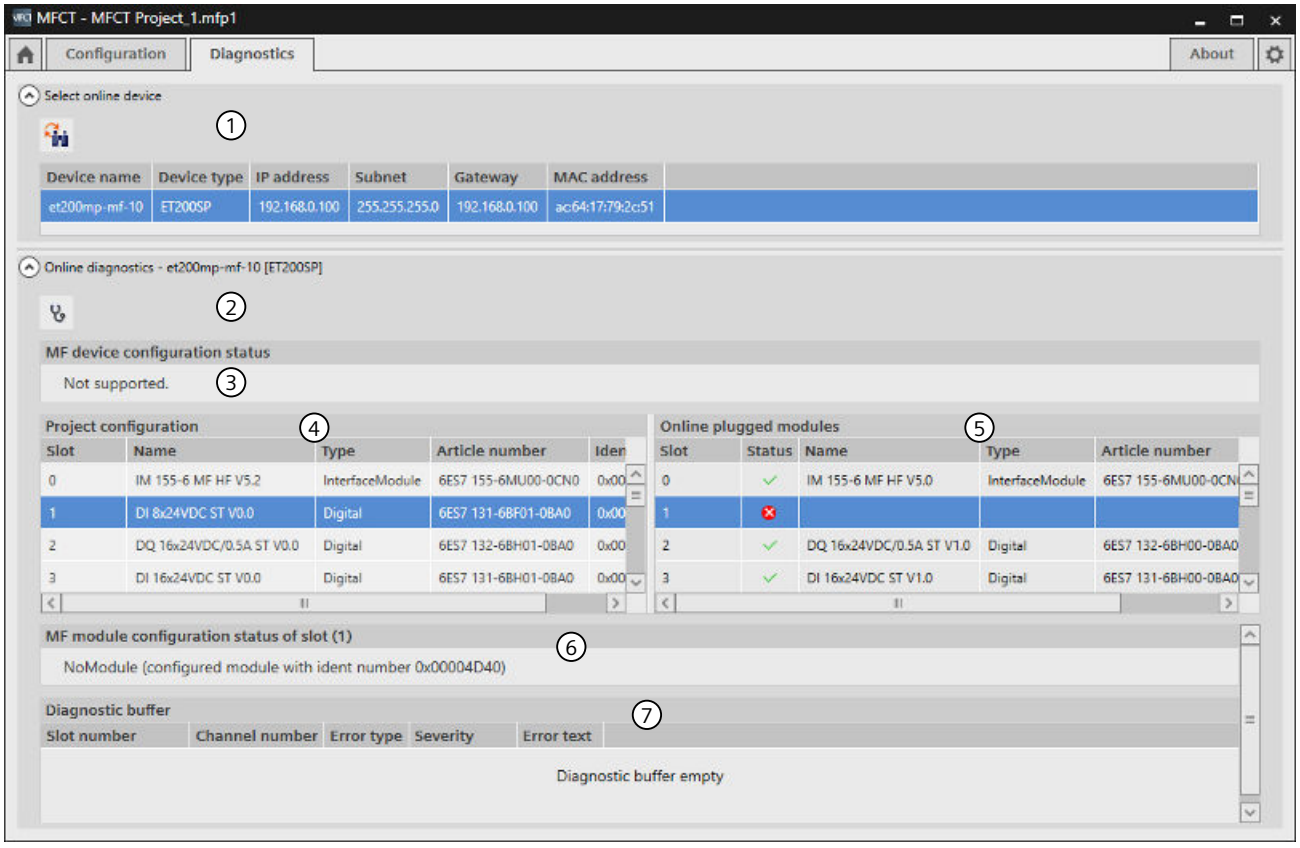
If you click the "Start configuration export" button, the configuration is exported to the selected storage location.

If you click the "Start transfer/export" button, the configuration is transferred to the MF device and also exported.

7.8 Reading diagnostics

In the "MultiFieldbus configuration" application, you can perform diagnostics on the MF devices that can be accessed online in the "Diagnostics" tab.

The following figure shows the contents of the "Diagnostics" tab:



① Selecting an online device

Use the "Start scan" button to search for the MF devices that are accessible via the preset network interface.

The MFCT shows the devices that are accessible online, from which you can select an MF device.

② Online diagnostics

Use the "Update online status" button to update the display under "Online plugged modules" ⑤.

③ MF module configuration status

The status of the configuration is displayed in the "MF module configuration status" area.

④ Project configuration

In the "Project configuration" area, you can find information on the loaded configuration of the selected MF device.

⑤ Online plugged modules

You can find information on the selected MF device in the "Online plugged modules" area. This requires that the
MF device is accessible online.

⑥ MF module configuration status of slot (x)

The "MF module configuration status of slot (x)" area shows you whether a module plugged in online matches the module in the MF project.

⑦ Diagnostic buffer

Under "Diagnostic buffer", you can see the content of the diagnostic buffer.

DALI configuration

8

The "DALI configuration" application is available as a plug-in in the MFCT. To use the "DALI configuration" application, activate the plug-in.

Once you have activated the plug-in, you can find the DALI configuration on the start page as an application. In an opened application, you can find the DALI configuration as a tab in the area of the button for the start screen.

You search the connected network for devices with DALI modules in the "DALI configuration" application. You can address, parameterize and control devices connected to the DALI modules.

As of MFCT version V1.5 SP4, you can also use expert mode without an online connection to MF devices and create or save frames.

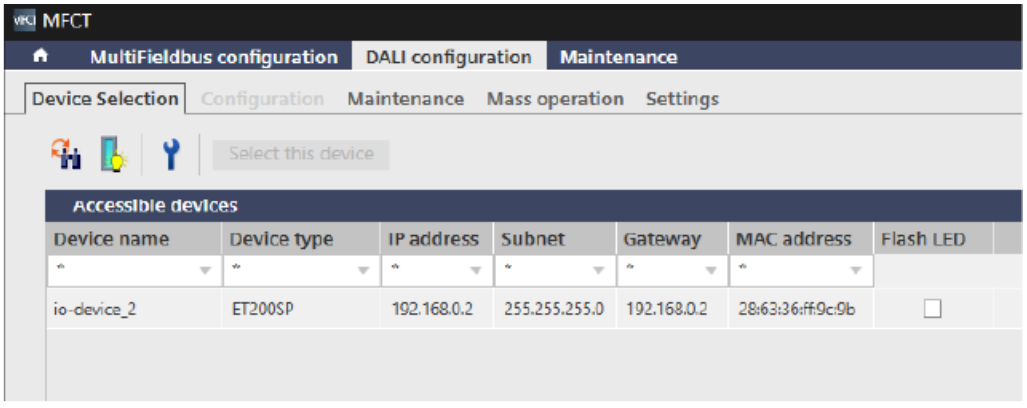
More information

You can learn how to activate a plug-in in section Plug-ins (Page 30).

You can learn how to configure frames in expert mode in section Expert mode (Page 69).

8.1 Selecting station with DALI module

You scan for ET 200 stations in which DALI modules are integrated on the "Device selection" tab.



Procedure

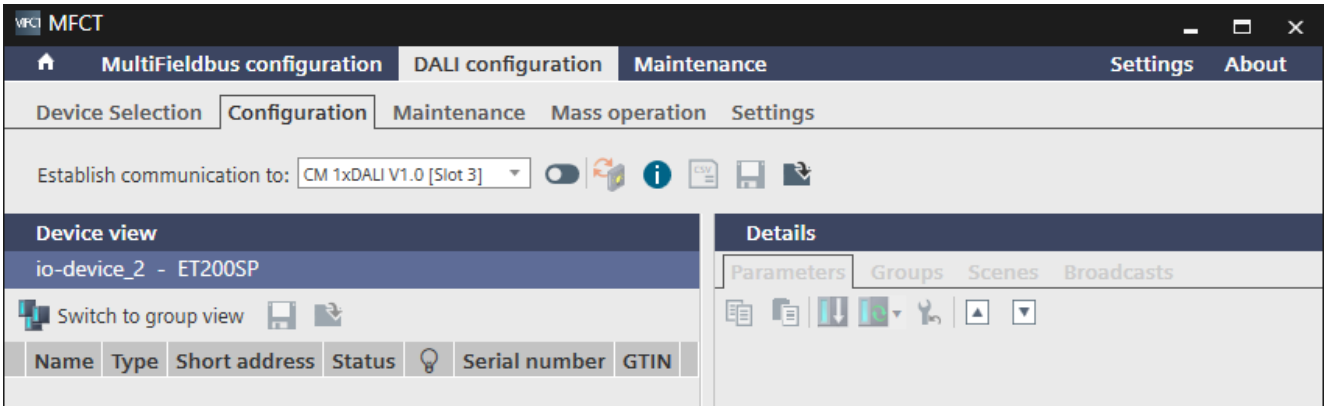
To select an accessible device, proceed as follows:

1. Click the "Start scan" button to search for accessible CPUs and ET 200SP interface modules.
2. Click the button to filter by CPUs and interface modules with an inserted DALI module.
3. Select the desired station from the list.
4. Select the station for the configuration by clicking the button Select this device or double-clicking the station.

Result: MFCT selects the desired station and opens the "Configuration" tab.

8.2 Selecting and configuring a DALI module

You select the DALI modules present in the ET 200 station and configure the connected DALI devices on the "Configuration" tab.



Procedure

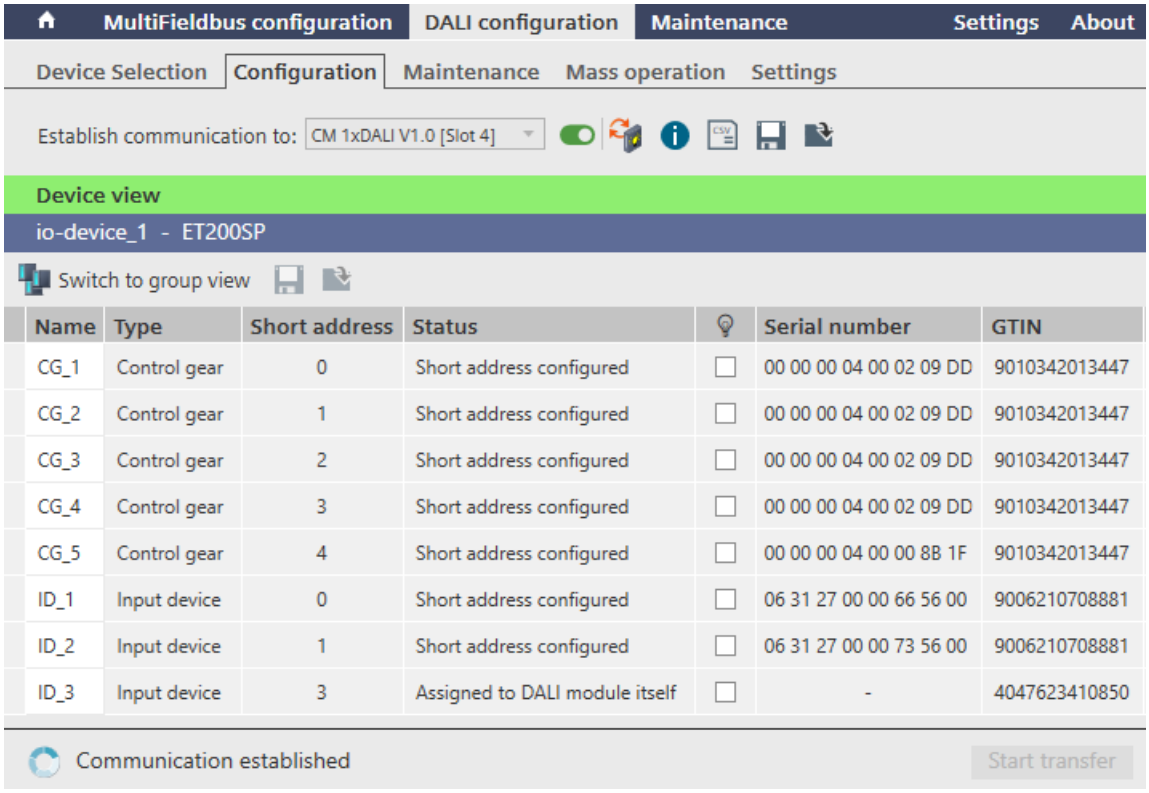
To select and configure your DALI module, proceed as follows:

1. Select the DALI module you want to connect to in the drop-down menu CM 1xDALI V1.0 [Steckplat.
2. Click the toggle switch "Establish communication" to establish the connection to the DALI module.
3. Beforehand, select only the required parameters in the settings (Page 74), e.g. assign short addresses automatically. The more parameters you select, the longer the scanning process will take.

   NOTE
   If you have selected the "Assign short addresses automatically" parameter, the unaddressed DALI devices are automatically assigned short addresses during scanning.

4. The button calls the communication status, i.e. whether you are connected to the module. When the connection is set up, start the search for the DALI devices connected to the module.

5. Click the "Start scan" button . Depending on the number of bus nodes, the process can take several minutes.



Result: You have read out the serial numbers and the GTIN code (Global Trade Item Number) of the connected DALI devices. For the detected DALI devices, you have the following options:

- Identify individual DALI devices using the column with the light bulb icon .
  To do so, select the check box in the row of the desired DALI device. As a result, an identification command is set on the DALI bus. Information on how a DALI device responds to this identification command can be found in the DALI device's manual.
- Change short addresses or device parameters
- Assign the DALI devices to groups

The following options are available:

- Optionally, you can export the currently displayed configuration of the devices as a *.csv file. To do this, click the "CSV" button . This allows you to document the existing configuration.
- You save and open projects with the "Save" and "Open" buttons . You can only open a saved project when there is an active connection to the CM DALI module.
- The "Status" column in the device view displays information about the bus nodes.

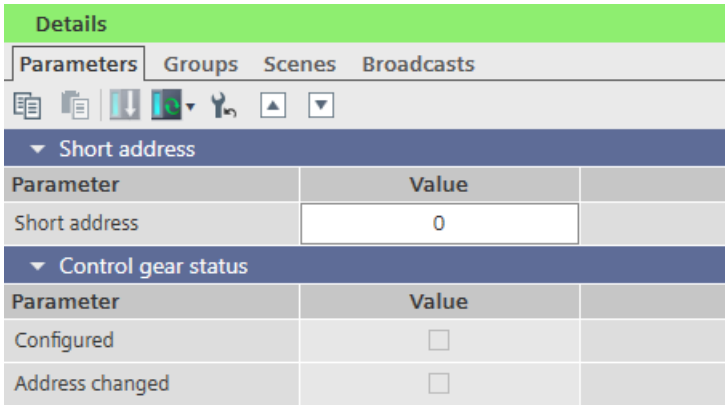
Information about the short addresses

DALI input devices and control gear have separate address ranges for short addresses. If a short address is assigned more than once within an address range, there is an address conflict. In this case, the "Status" column displays the corresponding text message.

For each DALI module, you may only assign each short address once to a DALI device or control gear connected to it. If a short address has been assigned more than once, you must reset the DALI devices involved. The next subsection explains how to reset DALI devices.

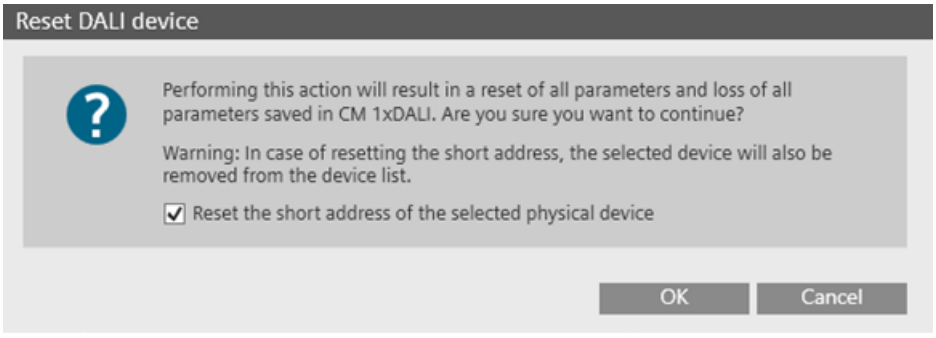
Details view

In the "Details > Parameters tab" area, you have additional options for configuring your devices.



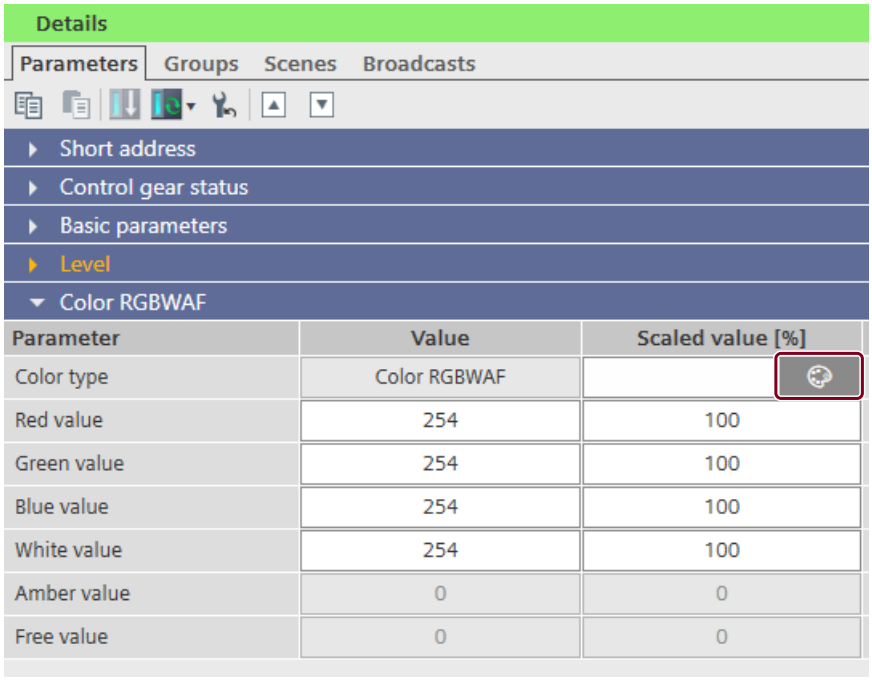
- To copy the configuration of one device and insert it into another device, use the button .
- To apply the modified parameters to the DALI device, click the button .
- In the "Details > Parameters tab" area, you can use the button to refresh the parameters of an individual device. The remaining bus nodes are not scanned again.
- To reset and/or delete a device, click the button .

  To reset only the short address of the selected device, select the "Reset the short address of the selected physical device" check box.



8.3 Making color settings

In the "Details > Parameters tab" area, click the button  to open the color picker. Select the desired color or color temperature there. The parameter fields show the appropriate values for the selected color and color temperature based on the selection.

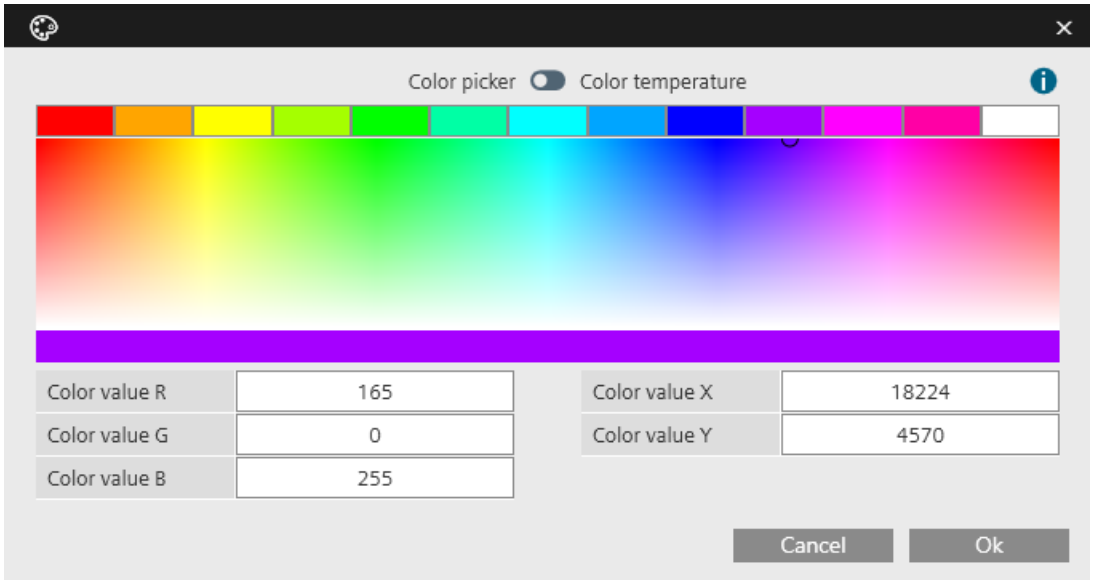


Setting the color

Depending on the control gear used, different colors are supported. The MFCT supports you in selecting a suitable color in various ways:

- Button: Select a suitable color by clicking on or in the color areas.
- Direct input:
  - Color value X/Y: X and Y coordinates for all colors
  - Color value RGBWAF: 6 values for up to 6 color components: Red, green, blue, white, amber and one free color

The following picture shows an example of a possible color selection:

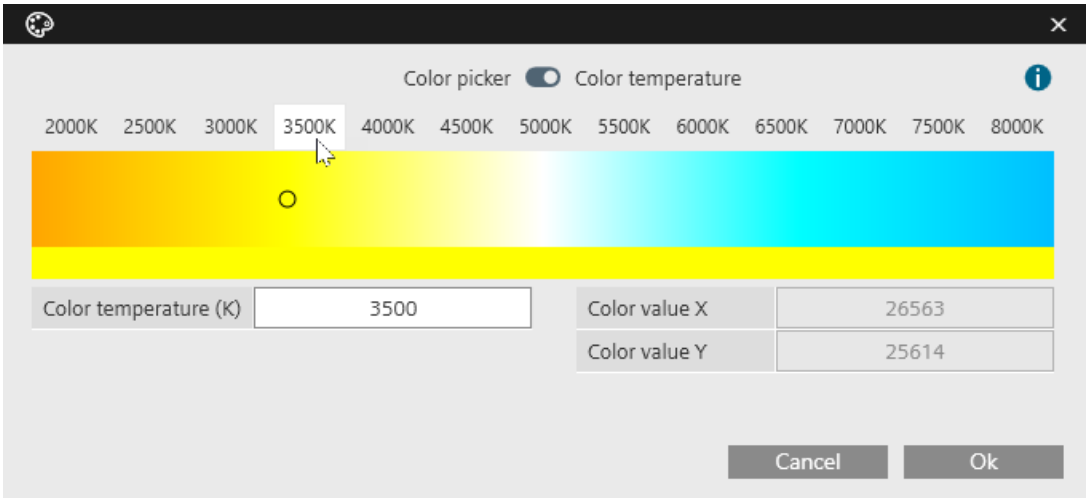


Setting the color temperature

The MFCT supports you in selecting a suitable color temperature in various ways:

- Buttons: Select a suitable value, e.g. "3500K", by clicking on the buttons.
- Direct input: Assign a value between 2000 K for warm white and 8000 K for cool white in the field next to "Color temperature (K)".

The color temperature is specified in Kelvin (K). The following figure shows an example of a color temperature of 3 500 K:



8.4 Device types

The DALI devices can be subdivided into two device types: control gear and input devices. There are different setting options for the two device types.

You can find more information in the SIMATIC ET 200SP Communication Module CM 1xDALI ST equipment manual (https://support.industry.siemens.com/cs/us/en/view/109769428).

8.4.1 Control gear

8.4.1.1 Device view

You have the following options for the control gear in the device view in the "Details" area:

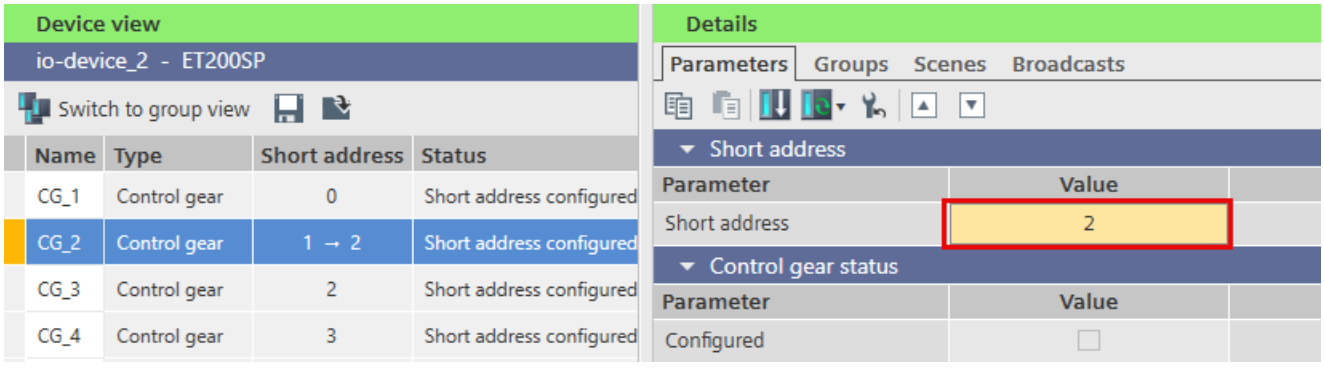
- Read out and transfer parameters
- Manage groups
- Edit scenes
- Send broadcasts

Parameters that have been changed but not yet transferred are highlighted in yellow.

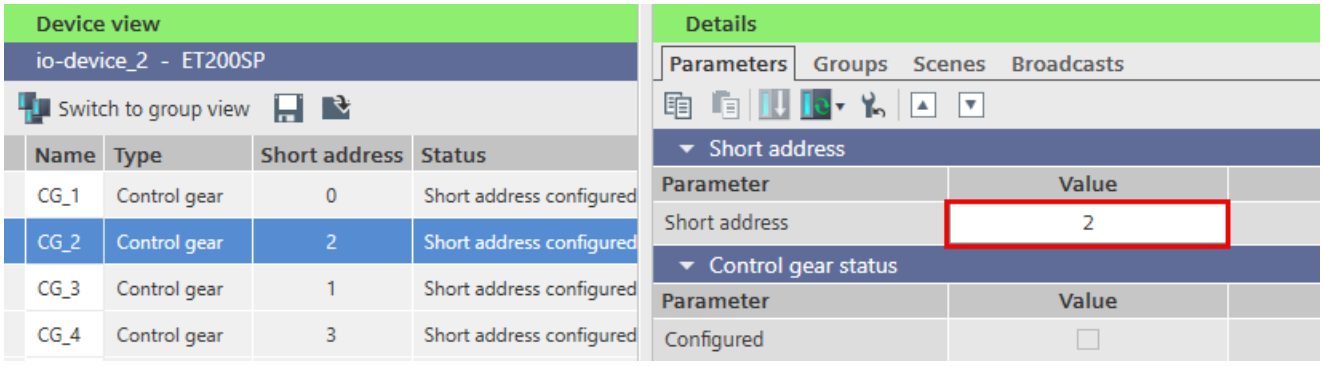
Read out and transfer parameters

You can display, change or transfer the parameters of a DALI device on the "Parameters" tab. For example, to change the short address of a DALI device, proceed as follows:

1. Select a device in the device view.
2. Change the value of the short address in the "Details > Parameters tab" area. The field with the changed value is highlighted in yellow.
3. Click the button Start transfer to transfer the changed parameters.



Result: The parameters have been successfully transferred and the result is displayed accordingly.



NOTE

Replacing existing addresses

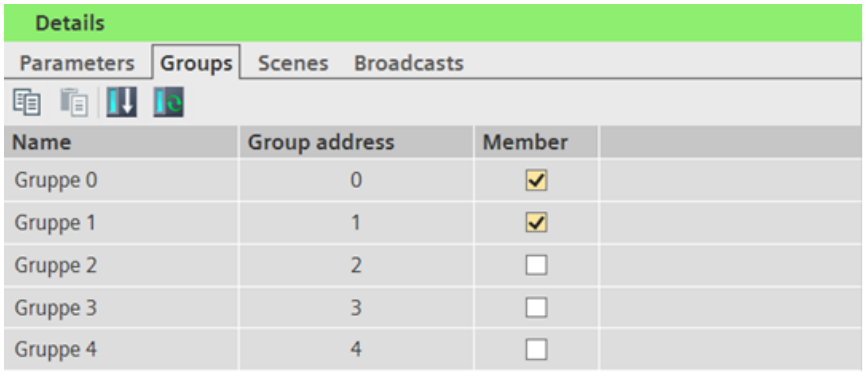
f the newly assigned address already exists within the address range, the addresses are replaced as follows:

The DALI device that is currently assigned this address receives the address of the device to which the new address was assigned.

Manage groups

Multiple devices can be configured and addressed simultaneously with the help of groups. To assign the devices to different groups, proceed as follows:

1. Select a device in the device view.
2. Switch to the "Details > Groups tab" area.
3. In the "Member" column, select the groups to which you want to add the selected device. In the figure below, the selected device was added as a member of groups 0 and 1.



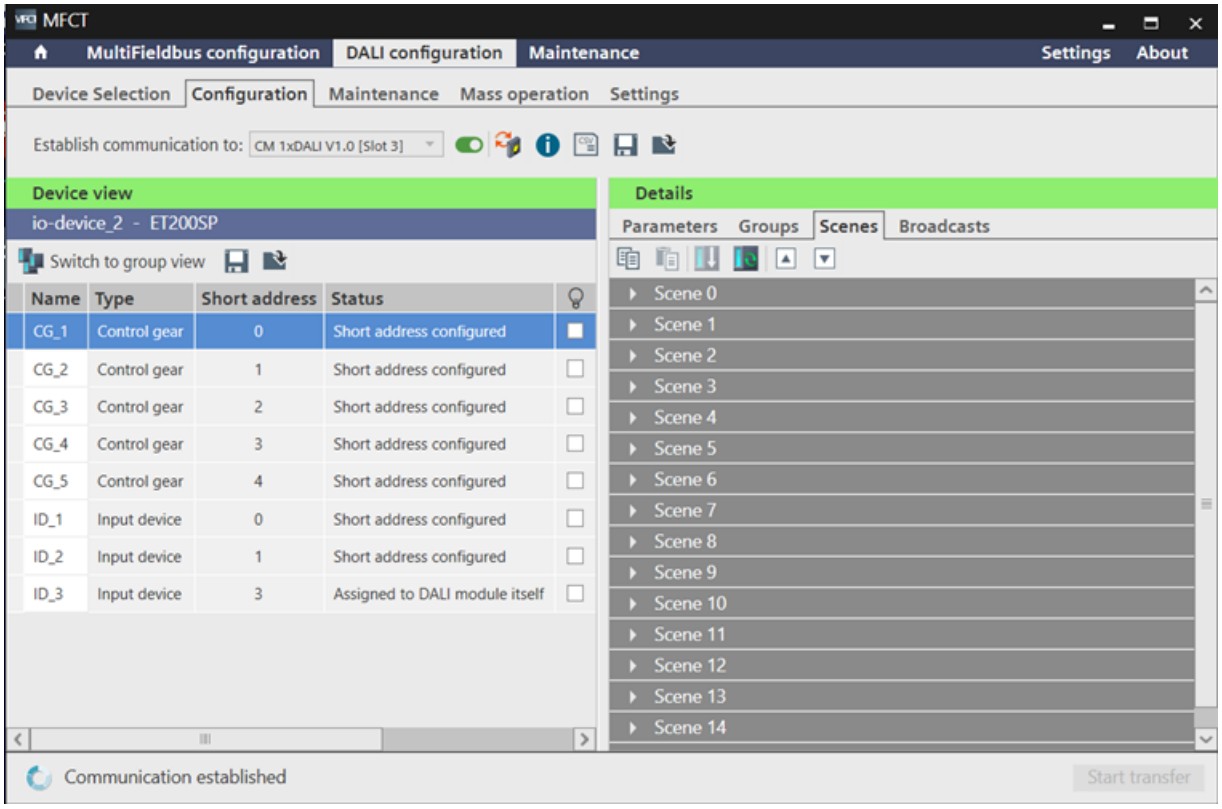
4. Click the button Start transfer to transfer the selected changes.

Edit scenes

Scenes are predefined value settings stored in the device and can be activated via a control command.

To edit the scene of a device, proceed as follows:

1. Select a device in the device view.
2. Switch to the "Details > Scenes tab" area.
3. To open the context menu, right-click in the "Scenes" area.
4. Select "Add scene".

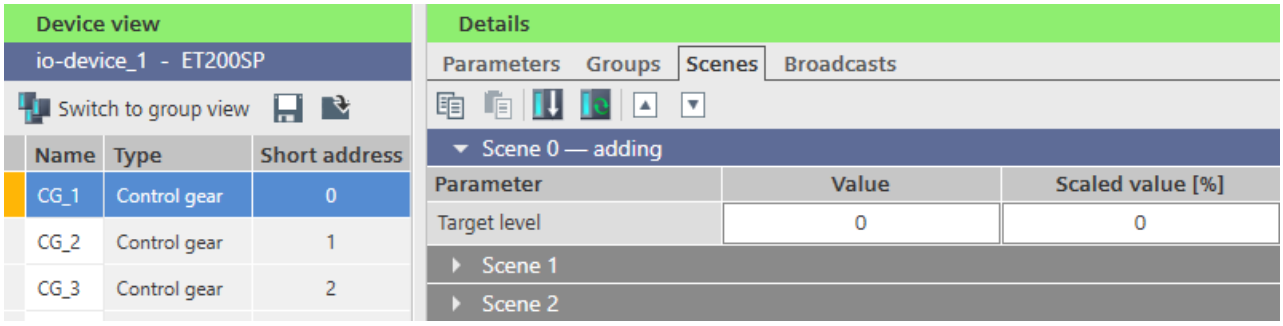


The context menu offers the following additional options

- Rename scenes
- Add all scenes
- Remove all scenes

5. For a scene stored in the device, you have the following options:
   - Activate scene
   - Remove scene

6. Optionally, you can specify the target value of the scene for the selected device.
   To do this, enter a value between 0 and 255 in the "Value" field. Depending on the type of DALI device used, you can also specify a color value for the scene.



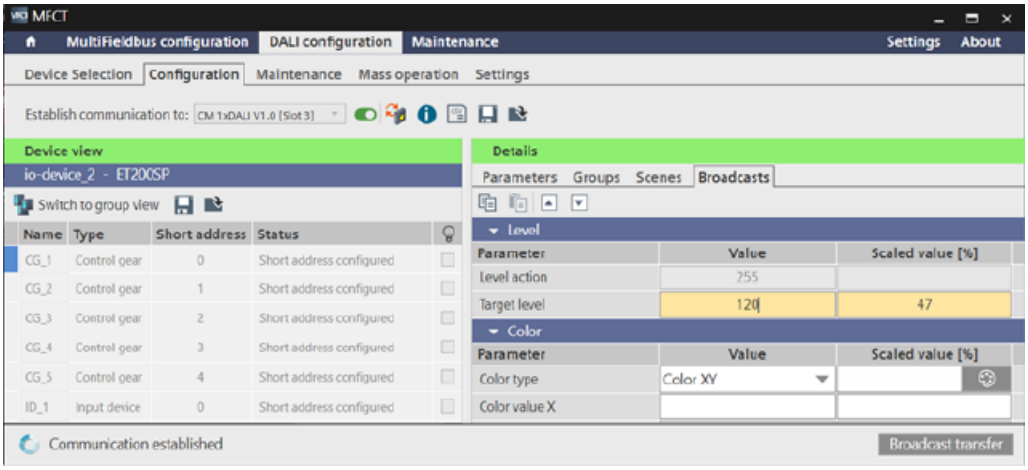
7. Click the button Start transfer to transfer the changed parameters.

Result: The parameters have been successfully transferred and the result is displayed accordingly.

Send broadcasts

To broadcast to all DALI devices, proceed as follows:

1. Select a device in the device view.
2. Switch to the area "Details > Broadcasts tab".
3. For example, change the target level in the "Value" area.
   The figure below shows an example of setting the brightness of all DALI devices on the bus to 47%:



4. Click the button "Broadcast transfer" to transfer the changed parameters.

Result: The parameters have been successfully transferred and the result is displayed accordingly.

8.4.1.2 Group view

To switch to the group view, click the "Switch to group view" button .
You have the following options for the control gear in the group view in the "Details" area:

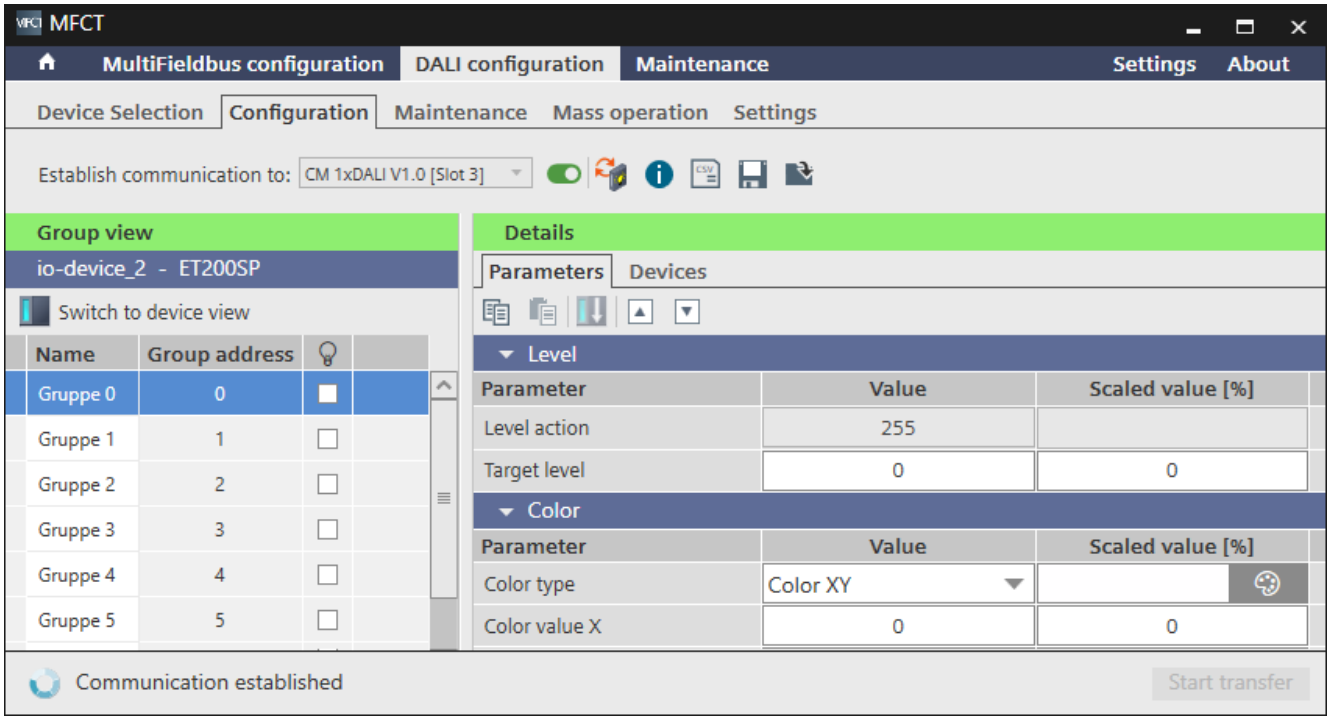
- Transfer parameters to groups
- Manage group members

Parameters that have been changed but not yet transferred are highlighted in yellow.

Transfer parameters

You can send commands to all members of a group in the "Details > Parameters tab" area.

1. Select a group in the group view.
2. Enter the required values in the "Parameters" tab.
3. Click the button Start transfer to transfer the selected changes.



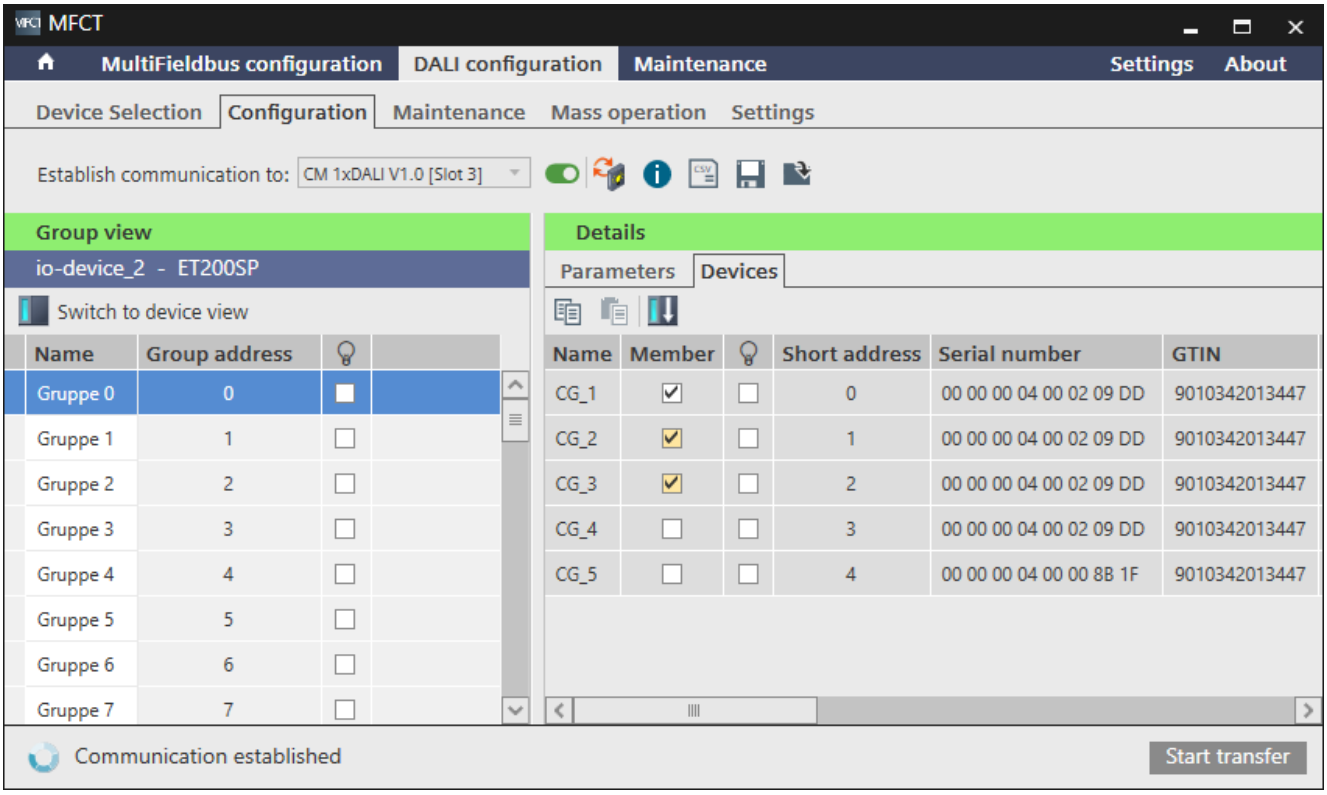
Manage group members

You have the following options in the "Details > Devices tab" area:

- Identify the individual group members. To do this, select the check box in column with the light bulb icon .
- Display, add and delete group members

For example, to add devices to a group. proceed as follows:

1. Click the desired group in the group view.
2. In the "Member" column on the "Devices" tab, select the check boxes of the devices you want to add to the group.
3. Click the button Start transfer to transfer the changed parameters.



Result: The parameters have been successfully transferred and the result is displayed accordingly.

If you want to check the result, select the check box of the corresponding group under the light bulb icon in the "Group view" section. This identifies all group members at once.

8.4.2 Input devices

DALI input devices can contain multiple instances under a single short address. The "Details" area shows a separate set of parameters for each instance. You can read out and transfer parameters.

Parameters that have been changed but not yet transferred are highlighted in yellow.

Read out and transfer parameters

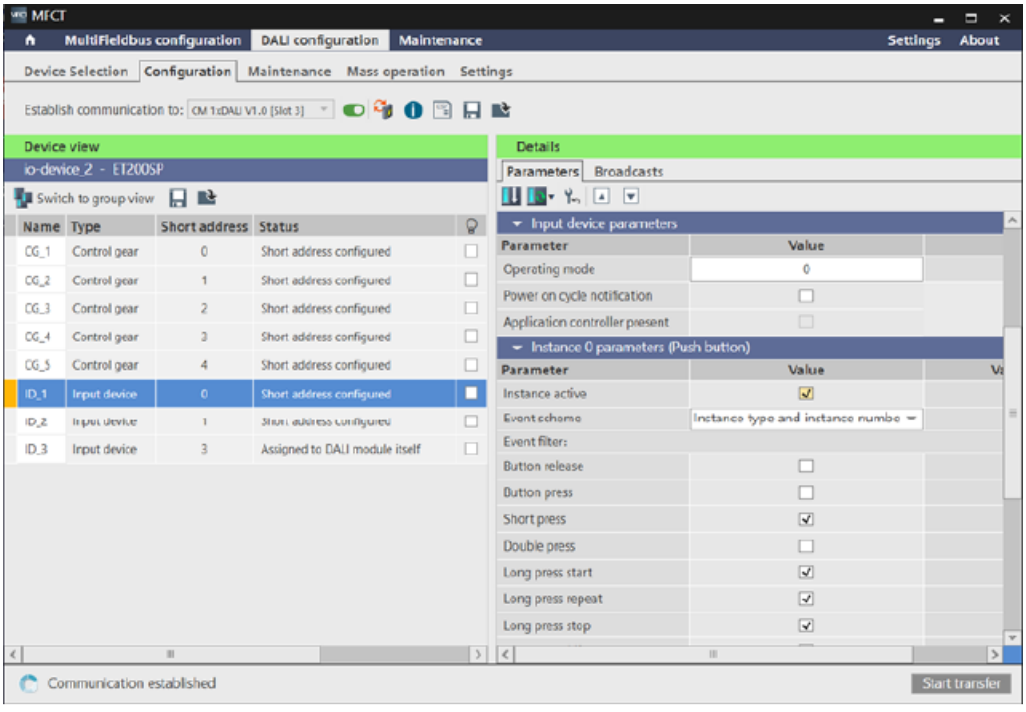
The parameters available depend on the instance type. The image below shows an example of the parameters of the "Push button" instance type.

You have the following options for the sensor instances in the "Parameters" tab:

- Activate
- Display
- Change
- Transfer

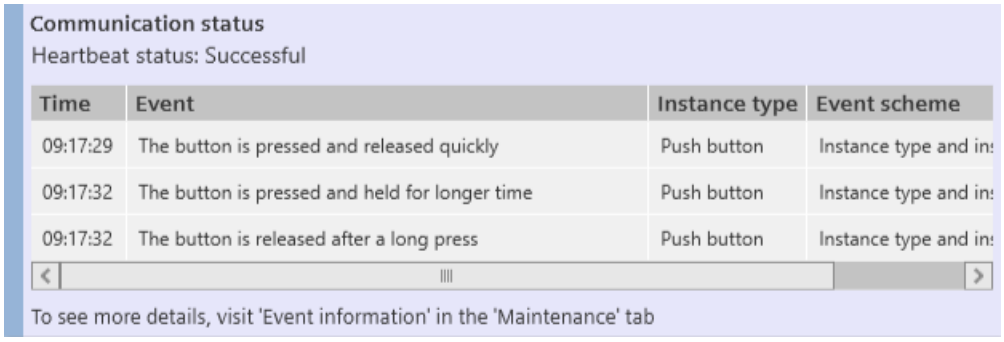
For example, to activate an instance, proceed as follows:

1. Select a device in the device view.
2. In the "Details > Parameters tab" section, open the desired instance, e.g., "Instance 0 Parameters (push button)".
3. Select the "Instance active" check box. The field with the changed value is highlighted in yellow.
4. Click the button Start transfer to transfer the changes.



Result: The changed parameters have been transferred to the selected input device.

If you want to verify the messages of the input devices, click the "Communication status" button . You then see the frames received from the CM 1xDALI module. This enables pushbutton events, for example, to be verified.



NOTE

Avoid simultaneous access attempts

An active DALI CTRL block accesses a DALI module in the user program of a CPU. At the same time, you want to access a DALI module with the MFCT. If the CPU is already communicating with the DALI module, the event is not displayed by the MFCT. The reason for this is that only the communication partner that first communicates with the DALI module after the message occurs receives the data. Either the CPU or the MFCT.

8.5 Maintenance

You can implement and process various commands with the DALI module on the "Maintenance" tab.

The sections below provide information on the following:

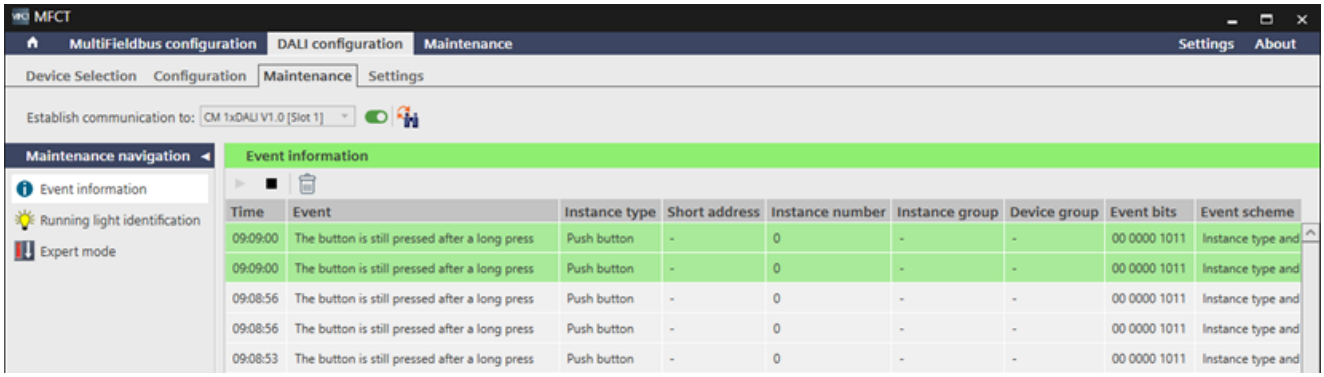
- Event information (Page 68)
- Running light identification (Page 68)
- Expert mode (Page 69)

8.5.1 Event information

Input devices compliant with the DALI-2 standard can actively report events on the DALI bus. These events are received by the CM 1xDALI and can be recorded by the control unit or the MFCT.

You control the function with the Start/Stop commands ▶ ■. You clear the window by clicking the button 🗑.

The following figure shows an example of received events on the DALI bus.



NOTE

Avoid simultaneous access attempts

An active DALI CTRL block accesses a DALI module in the user program of a CPU. At the same time, you want to access a DALI module with the MFCT. If the CPU is already communicating with the DALI module, the event is not displayed by the MFCT. The reason for this is that only the communication partner that first communicates with the DALI module after the message occurs receives the data. Either the CPU or the MFCT.

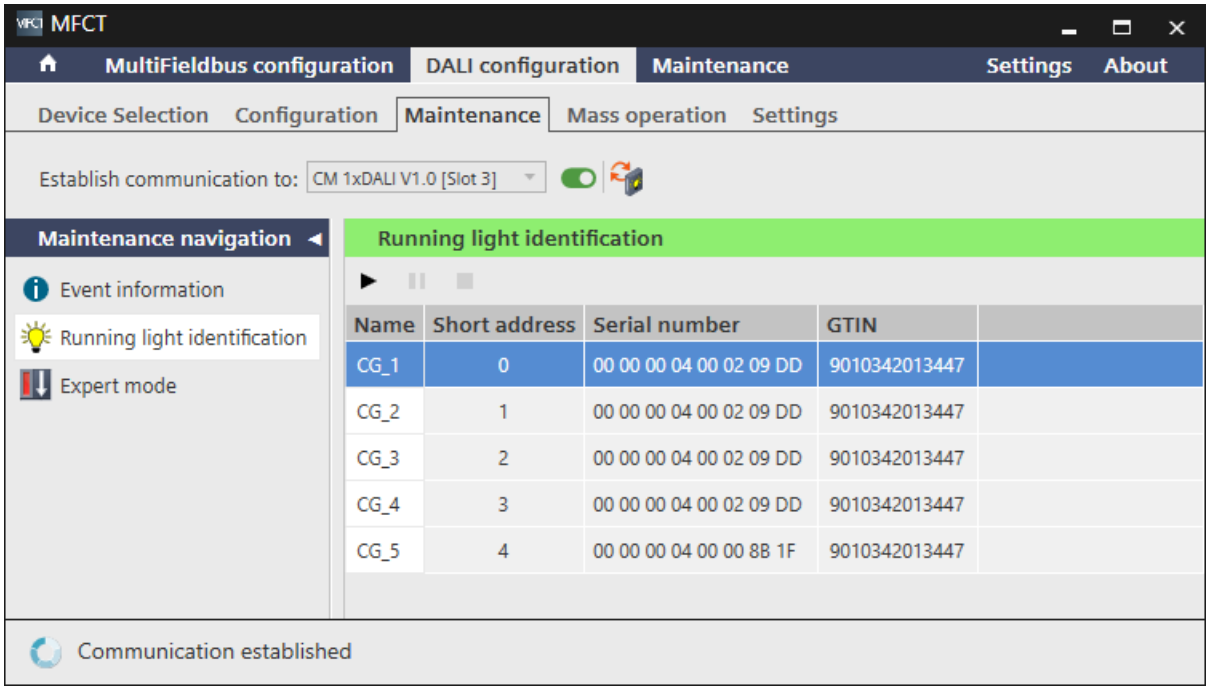
8.5.2 Running light identification

With the running light identification, you start a running light to identify the individual devices. For this purpose, the dimming values of the individual lights are set to 0 and then switched on one after another. After the running light function, the lights are returned to their original dimming value.

This makes it easy to check the arrangement of the short addresses once commissioning is complete. You can also monitor the progress of the running light identification in the list of existing short addresses.

You control the function using the Start, Pause and Stop buttons ▶ ⏸ ■.

You configure the duration and speed of the identification, for example, on the "Settings" tab. You can find more information in section Settings (Page 74).



8.5.3 Expert mode

Expert mode is a function in the "Maintenance" area of the DALI configuration and offers options, such as:

- Direct access to the DALI bus with free single frames
- Creation and sending of specific frame sequences

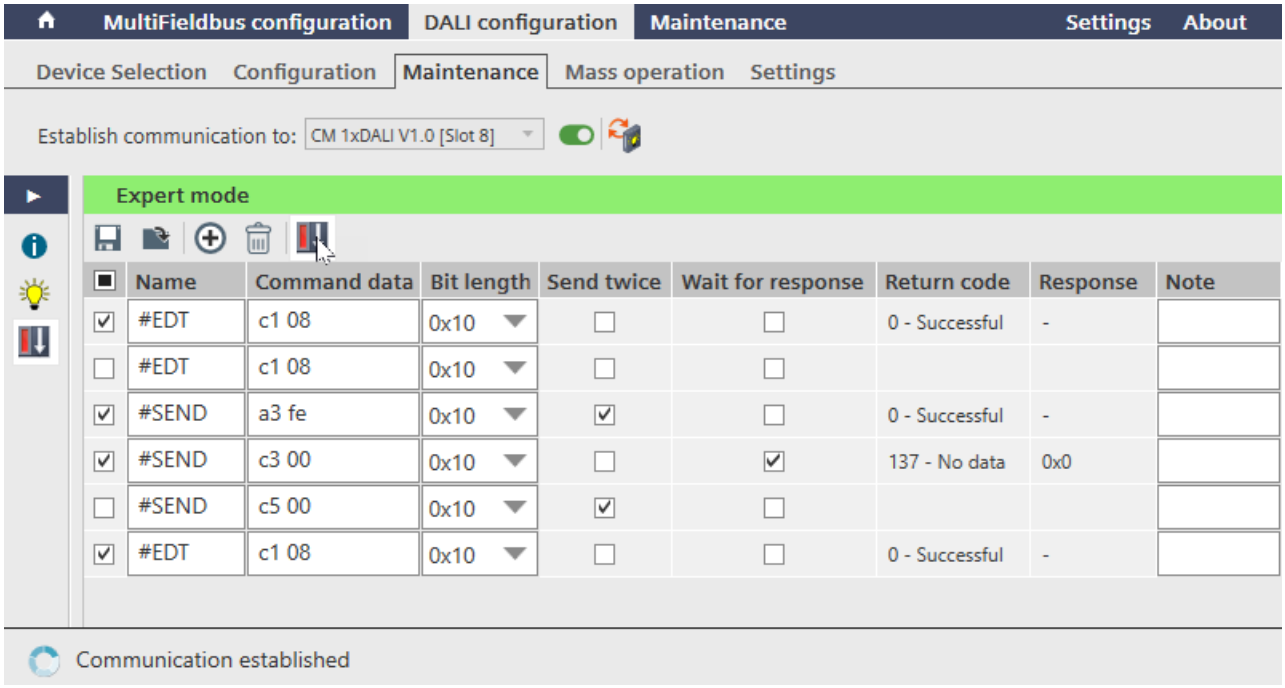
Requirement
For MFCT versions up to V1.5 SP3: You must be connected online to the DALI module.
As of MFCT version V1.5 SP4: You can also use expert mode without a connected DALI module and create or save frames.

Procedure - Creating and sending command data

To create and send a sequence of frames with command data in expert mode, proceed as follows:

1. Use the "Plus" and "Recycle bin" buttons to add entries or remove all entries.
   Use the "Save" and "Open" buttons to load a preconfigured sequence of frames or to save the sequence you created.
2. In the first table column, select which frames you want to send to the DALI bus.
3. In the selection menu, select the bit length in each entry to be sent.
4. Edit the command data in each frame to be sent.

5. Optional:
   - To send the command twice, select the "Send twice" option.
     Some configuration commands for DALI require repetition of the frame for successful execution.
   - To wait for the response from a device connected to the DALI bus, select the "Wait for response" option.
     A received response is shown in the corresponding row in the "Response" column.
   - Enter a meaningful name in the "Name" column and a note for the entries in the "Note" column.
6. Click the "Download" button .
   The transfer to the DALI bus starts and the created list is processed.



Result: You have configured the command data and transferred it to the DALI bus. The columns "Return code" and "Response" show the results of each row.

NOTE

Avoid simultaneous access attempts

An active DALI CTRL block accesses a DALI module in the user program of a CPU. At the same time, you want to access a DALI module with the MFCT. If the CPU is already communicating with the DALI module, the event is not displayed by the MFCT. The reason for this is that only the communication partner that first communicates with the DALI module after the message occurs receives the data. Either the CPU or the MFCT.

More information

You will find additional information on how to construct the command frames in the IEC 62386 standard and in the DALI device's manual.

8.6 Mass operation

As of MFCT version V1.5 SP4, the "DALI configuration" application includes the mass operation function. The mass operation feature allows you to edit multiple DALI devices across several DALI modules at the same time. The individual DALI modules may also be distributed across different ET 200SP stations.

In the mass operation, you search the network for devices that are accessible online and then select the desired DALI modules. This MFCT scans the selected DALI modules and automatically assigns short addresses to the connected devices. You can change the automatically assigned short addresses in the results list as required and reassign them to the connected devices of all DALI modules.

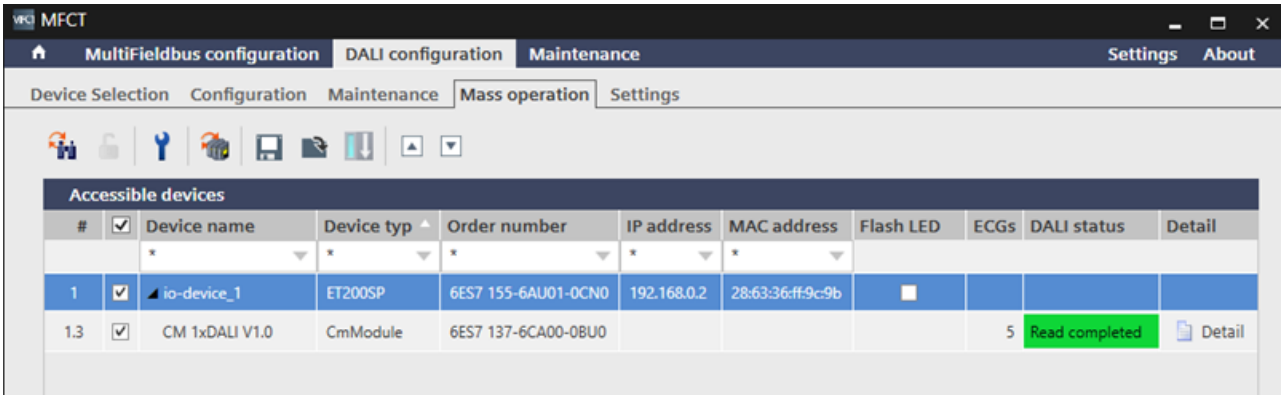
You can also export and save the results list locally as a CSV file. In the CSV file, you can assign pre-defined short addresses to the DALI devices based on the serial numbers or assign the DALI devices to a group. When editing the CSV file, you do not need a connection to the DALI modules.
If you are connected to the DALI modules, you can load the edited CSV file in the MFCT and load the changes into all the desired DALI devices.

You can find the mass operation as a tab in the "DALI configuration" application.

Procedure - Starting the mass scan

To start the mass scan for online-accessible DALI modules, proceed as follows:

1. Select the "Settings" tab in the "DALI configuration" application.
   The MFCT shows the settings for the DALI scan.
2. Select only the settings required for the DALI scan in order to keep the duration of the scan to a minimum.
   You can find information in section Settings (Page 74).
3. Select the "Mass operation" tab in the "DALI configuration" application.
4. Click the "Start scan" button .
   The MFCT shows the online-accessible devices as a list under "Accessible devices".
5. Select the desired DALI modules for the mass operation from the list.
6. Click the "Start mass scan" button .
   The MFCT scans the selected DALI modules and automatically assigns short addresses to the connected DALI devices. The "DALI status" column shows the progress for the respective DALI module.



Result: You have scanned the desired DALI modules. The "DALI status" column shows the progress as "Read completed" next to the modules. In the "Detail" column, you can find a list of the results of all DALI modules and the connected DALI devices for further processing.

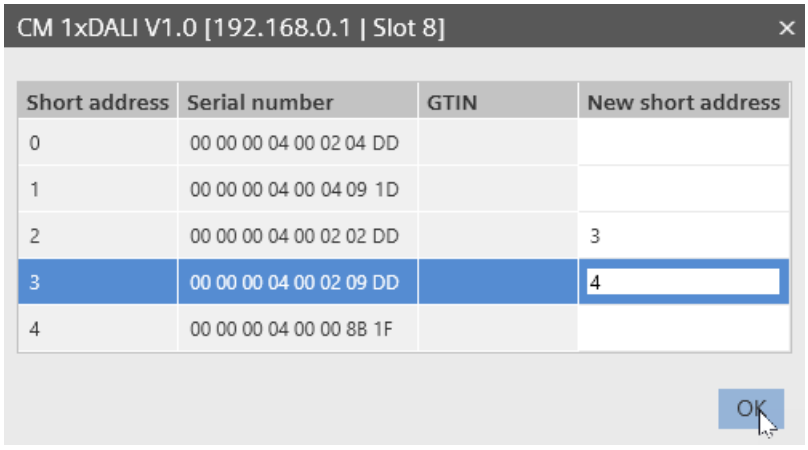
Procedure - Configuring short addresses online

Requirements:

- You have scanned the desired DALI modules.
- The "Detail" column shows a list of the results of the mass scan.

To configure the automatically assigned short addresses online, proceed as follows:

1. Click the list in the "Detail" column.
   The MFCT opens the list in a new window. The list shows the automatically assigned short address next to each serial number of the DALI device.
   – If you also want to read out the GTIN code, you must first enable the corresponding option in the Settings (Page 74).
2. Assign the desired short address to the devices in the "New short address" column.



3. Click the "OK" button.
   The MFCT closes the list and shows in the "DALI status" column that parameters have been changed.
4. Click the "Load changed parameters into the devices" button.
   The MFCT automatically loads the newly assigned short addresses into the DALI devices.

Result: You have changed the automatically assigned short addresses and loaded them into the DALI devices.

Procedure - Saving results list locally and configuring offline

Requirements:

- You have scanned the desired DALI modules.
- The "Detail" column shows a list of the results of the mass scan.

To save the results list locally, proceed as follows:

1. Click the "Save" button.
   The MFCT opens the "Save as" window.
2. Select the storage location for the file in Explorer.
3. Assign a name for the file.
4. Select the file type CSV.
5. Click "Save".

Intermediate result: You have saved the results list locally as a CSV file.

To configure the short addresses offline, proceed as follows:

1. Open the CSV file.
   The CSV file shows all the information about the DALI modules and the DALI devices connected to them.
2. Assign a new short address to the devices in the "New short address" column.
3. Save the changes to the CSV file.

Result: You have configured the short addresses offline in the CSV file.

Procedure - Loading results list as CSV file

Requirements:

- You have saved the results list locally on your PC as a CSV file and configured the short addresses.
- The MFCT is open and shows the "Mass operation" function in the "DALI configuration" application.

To upload the CSV file with the changes, proceed as follows:

1. Click the "Open" button.
   The MFCT opens the "Open" window.
2. Select the CSV file to be opened.
3. Click the "Open" button.
   The MFCT closes the "Open" window and loads the results list.

Intermediate result: You have loaded a results list as a CSV file.
Optionally, you can open the configuration again in the "Data" column and change the short addresses in the "New short address" column. If you have changed short addresses and close the list, the MFCT shows in the "DALI status" column that parameters have been changed.

To load the changed short addresses into the DALI devices, proceed as follows:

1. Click the "Load changed parameters into the devices" button.
   The MFCT automatically loads the newly assigned short addresses into the DALI devices.

Result: You have loaded the changed short addresses into the DALI devices.

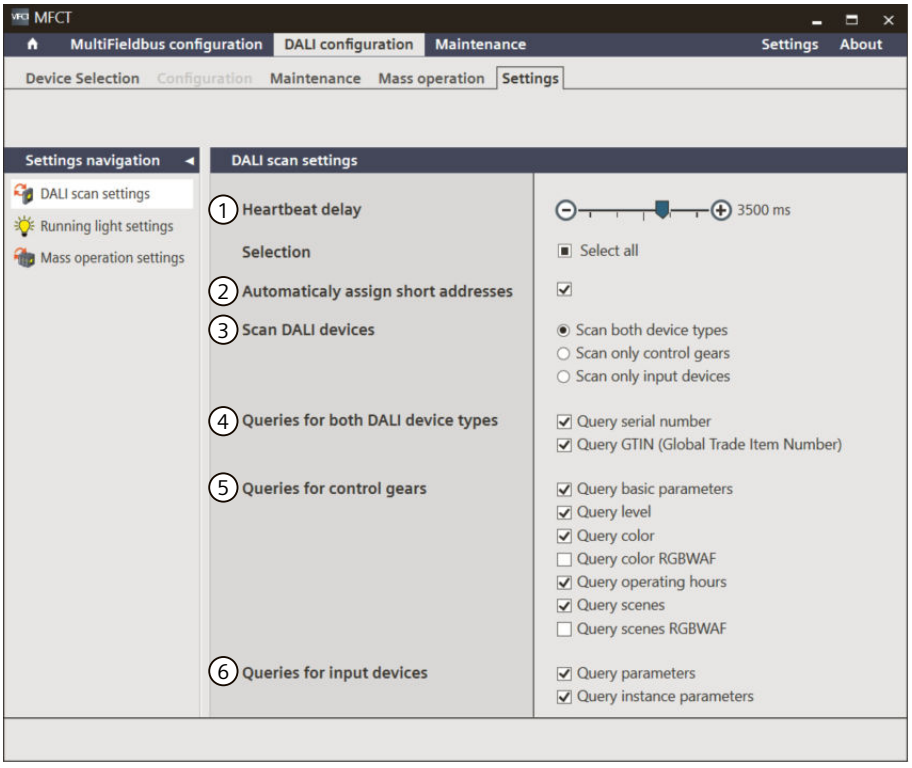
8.7 Settings

You can make various modifications to the following on the "Settings" tab:

- Basic configuration of the DALI scan
- Configuration of the running light for identification
- Parallel processing for the mass operation

Basic configuration of the DALI scan

Select the entry "DALI scan settings" in the "Settings navigation" column.



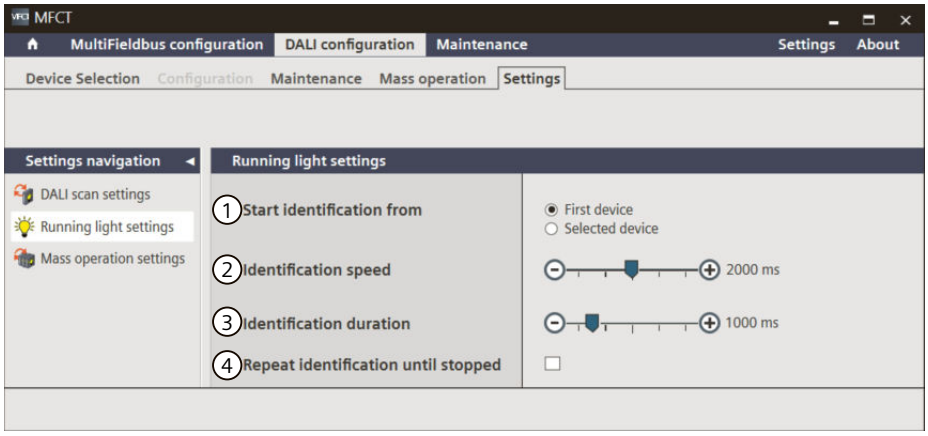
①	Heartbeat delay	Setting for the maximum time between two DALI frames to maintain communication.
②	Automatically assign short addresses	Specifies whether unaddressed devices on the DALI bus are automatically assigned an address.
③	Scan DALI devices	Specifies whether the MFCT should scan for control gear, input devices or all types on the bus.
④	Queries for both DALI device types	Specifies whether the GTIN code (Global Trade Item Number) and/or serial number should be queried for each device.
⑤	Queries for control gear	Specifies the parameters to be read out from the control gear.
⑥	Queries for input devices	Specifies the parameters queried for the input devices.

NOTE

A multiple selection is possible for items 4 to 6.
The more parameters that are queried, the longer the scan will take.

Configuration of the running light for identification

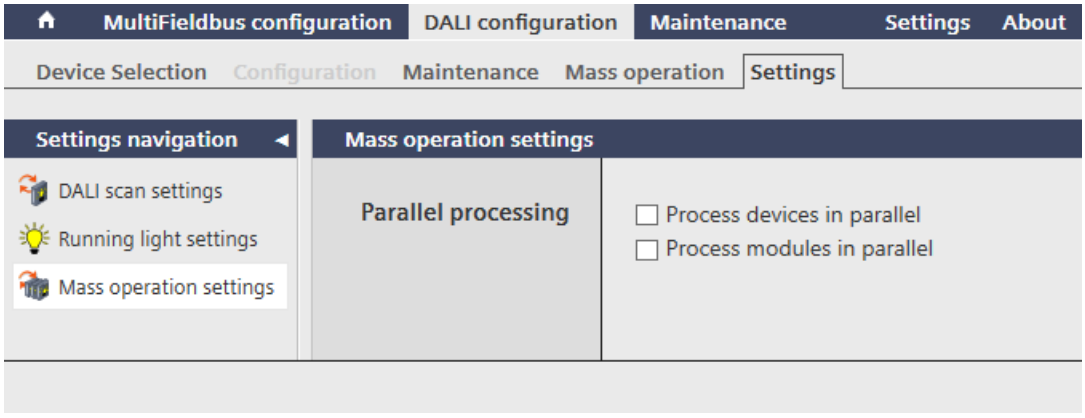
Select the entry "Running light settings" in the "Settings navigation" column.



①	Start identification from	Specifies where the identification should start: • Selected device • Lowest address on the bus
②	Identification speed	Changeover time from one connected lamp to the next.
③	Identification duration	How long each controlled lamp should be lit.
④	Repeat identification until stopped	Activates the identification in an endless loop until manually stopped.

Parallel processing for the mass operation

Select the entry "Mass operation settings" in the "Settings navigation" column. You can activate parallel processing for devices and/or modules.



TM FAST

9

The TM FAST application is available as a plug-in in the MFCT. To use the TM FAST application, activate the plug-in.

Once you have activated the plug-in, you can find the TM FAST on the start page as an application. In an opened application, you can find the TM FAST as a tab in the area of the button for the start screen.

You can generate the following in the TM FAST application:

- A UPD file (**Upd**ate file)
- A DB file (**D**ata**b**lock file)

In this case, you use the UPD file to load the TM FAST application. You perform loading using the MFCT or the TIA Portal.

You use the DB file in STEP 7 (TIA Portal) to write the user logic from the user program of the CPU to a TM FAST module.

More information

You can learn how to activate a plug-in in section Plug-ins (Page 30).

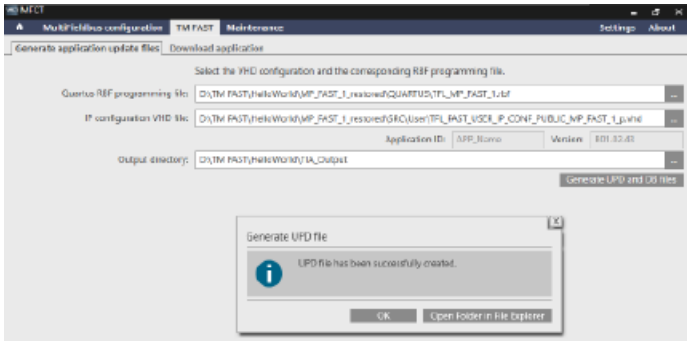
You can get detailed information on the TM FAST module in the technology module TM FAST equipment manual (https://support.industry.siemens.com/cs/us/en/view/109816087).

You can find an application example for handling DB files in the following Internet entry (https://support.industry.siemens.com/cs/ww/en/view/109823442). This application example shows how to load and activate a TM FAST application from a SIMATIC CPU to the TM FAST module. This enables you to replace a module without additional tools such as TIA Portal or the MFCT.

9.1 Generating UPD and DB files

To generate UPD or DB files with the TM FAST application, proceed as follows:

1. Generate the Raw Binary File *.rbf and the VHD file *.vhd from the development environment for programming the FPGA application logic (Quartus® Prime Software).
2. Select the path to your RBF file in the "Quartus RBF programming file" field.
3. Select the path to your VHD file in the "IP configuration VHD file" field.
4. Select the folder in which the generated files are to be stored in the "Output directory" field.
5. After successful creation of the UPD and DB files, the following dialog is displayed as confirmation.



The result is that you will find the following files in the selected output directory:

- 6ES7 554-1AA00-0AB0 APP_Name_UserLogic_B01.02.43.upd
- APP_Name.db

You need the UPD file to load the user program created in Quartus® Prime using the MFCT or the TIA Portal.

More information

The DB file can be imported into STEP 7 (TIA Portal) as an external source and interconnected with the function block "CheckUserlogicdata". More information can be found in the following Internet entry (https://support.industry.siemens.com/cs/us/en/view/109817062).

9.2 Download UPD files

Transferring UPD file to a TM FAST module

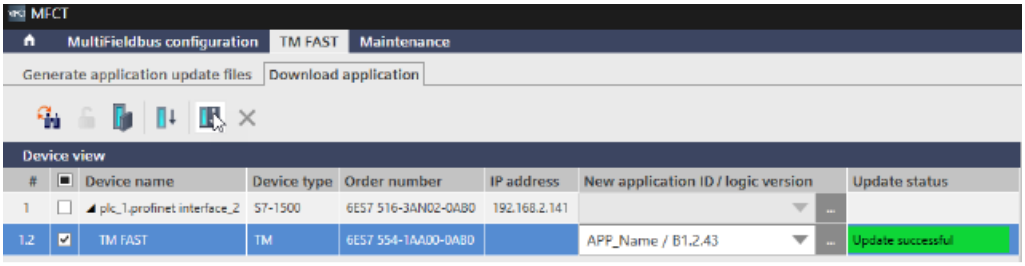
You can transfer the UPD file to a TM FAST module on the tab "Download application > Device view area". To do so, proceed as follows:

1. Click the "Start scan" button to display all accessible devices of the preset network interface.

   NOTE
   To find all modules in the central configuration, select the "Inclusion of central working modules" check box under "Communication with CPUs" in the general settings.
   You can find more information in section General settings (Page 27).

2. Click the button to sort by devices with TM FAST modules.

3. In the "New application ID/logic version" column, select the TM FAST user logic (*.upd) for the update.
4. Click the button to start the download.



Result: You have started the download of the UPD file. You can see the progress of the update in the "Update status" column.

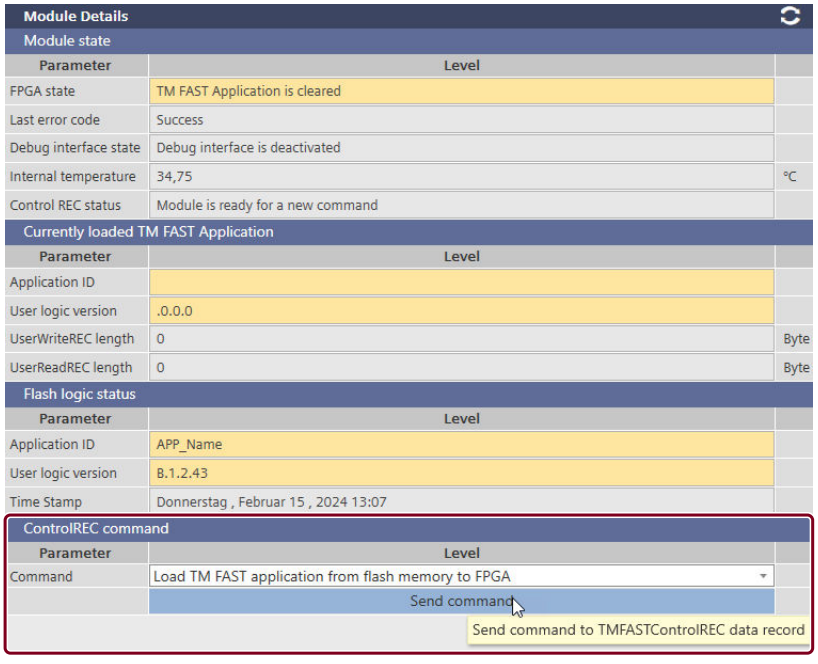
Loading and activating the application

In the "Module details" area, you see that the new TM FAST user logic has been loaded into the flash memory:

- Application ID: "APP_Name"
- User logic version: "B1.2.43".

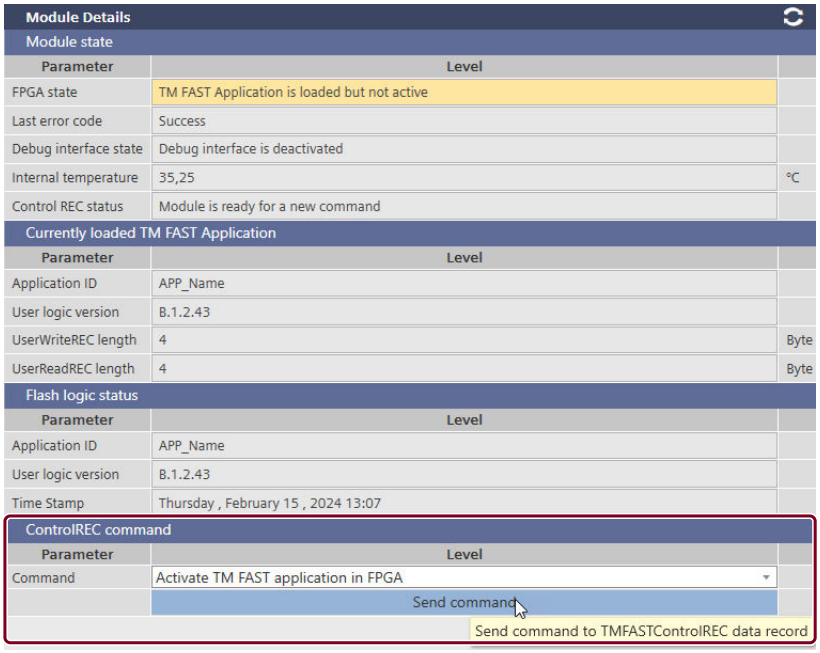
To load the application into the FPGA and activate it, proceed as follows:

1. Select the command "Load TM FAST application from flash memory to FPGA" in the "ControlREC command" area.
2. Click the "Send command" button.

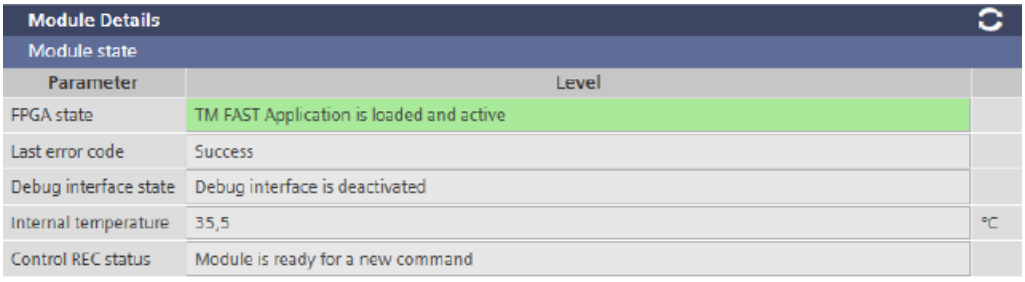


3. Select the command "Activate TM FAST application in FPGA" in the "ControlREC command" area.

4. Click the "Send command" button.



Upon successful activation, you will get the following message:



5. Enable the following parameters in the hardware configuration of the module:
   - Load TM FAST application during startup
   - Always activate TM FAST application

Result: You have loaded the application to FPGA and activated it. The application starts up automatically after a restart.

SIWAREX

10

The "SIWAREX" application is available as a plug-in in the MFCT. To use the "SIWAREX" application, activate the plug-in.

Once you have activated the plug-in, you can find SIWAREX on the start page as an application. In an opened application, you can find SIWAREX as a tab in the area of the button for the start screen.

You search the connected network for TM SIWAREX WP3x1 modules in the "SIWAREX" application. You have the following options for the found modules:

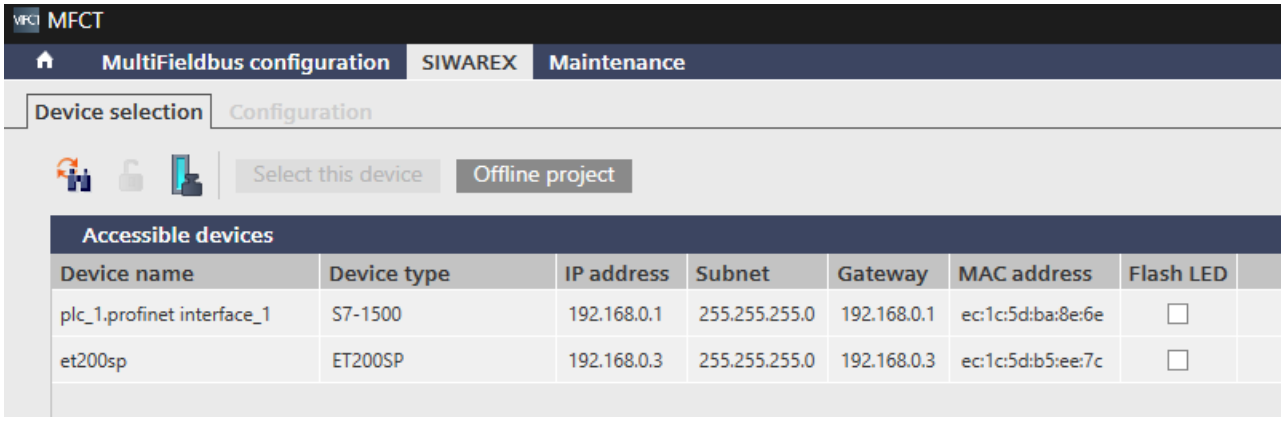
- Edit parameters
- Read, write or monitor data records

You can learn how to activate a plug-in in section Plug-ins (Page 30).

10.1 Scanning for SIWAREX assemblies

You scan for devices with connected SIWAREX modules on the "Device selection" tab. To do so, proceed as follows:

1. Click the "Start scan" button to search for accessible devices.



2. Optional: Click the "Set filter" button to show only the devices with connected SIWAREX WP3x1 modules.
3. Select the desired device in the selection list.
   If the ET 200SP station has multiple SIWAREX modules but you only want to select one of them, click its check box.

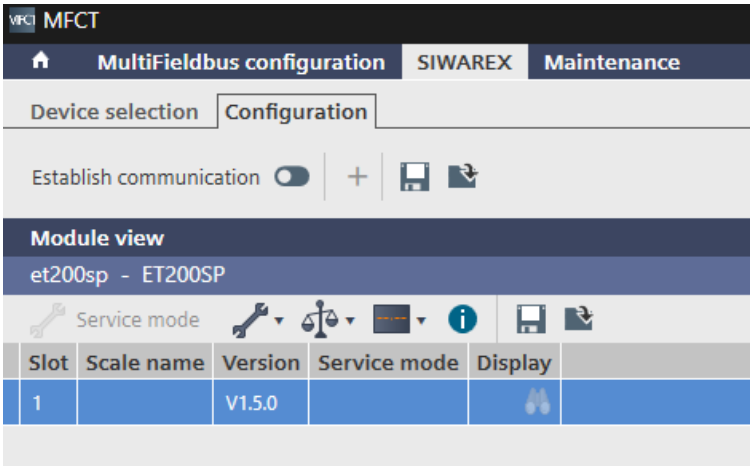
Result: You have scanned the network and selected the desired device. When you click the button Select this device, the station view opens.

Editing data offline

If you want to open and read backup files without an online connection, click the button Offline project. You can also prepare and store the parameters offline and transfer them to the modules later.

10.2 Setting up communication in the station view

You establish the communication with the SIWAREX module on the "Configuration" tab.

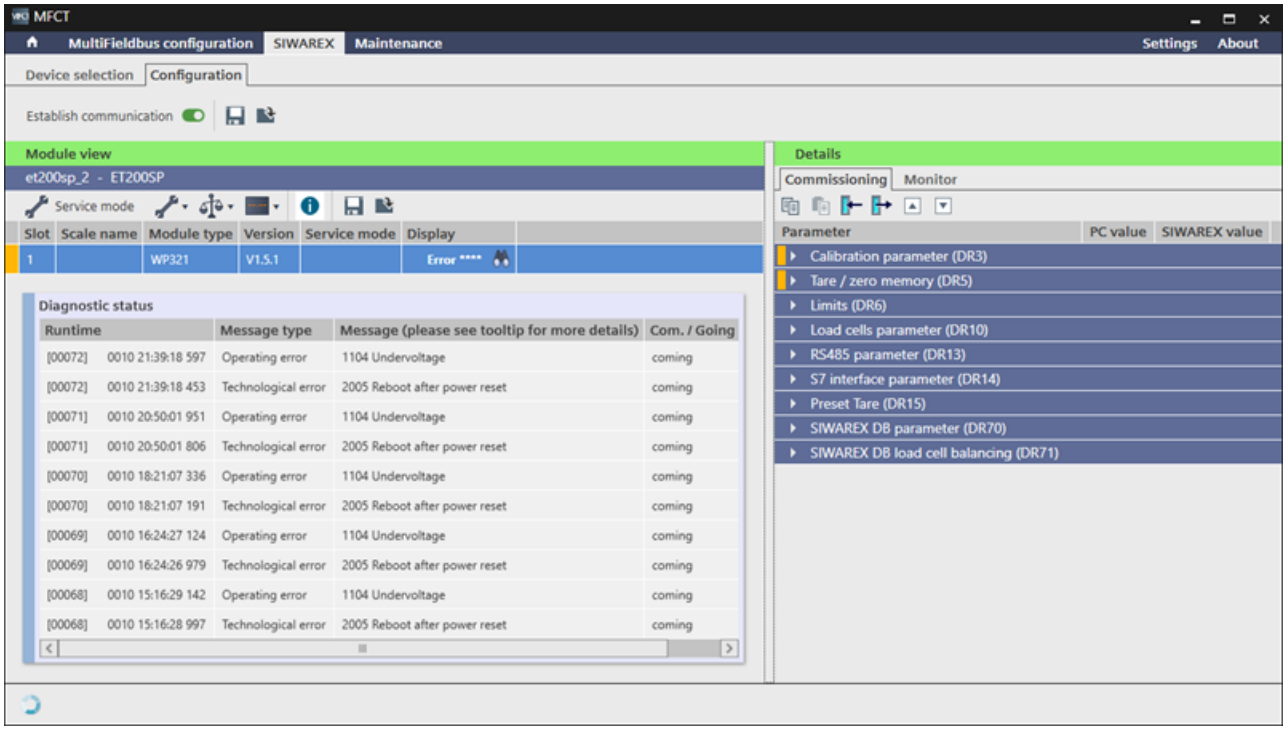


To establish the communication between the MFCT and the SIWAREX module, click the button Establish communication in the station view.

Result: The module view displays a list of all WP3x1 modules in the station.

10.3 Working in the station view

You can make different configurations on the "Configuration" tab. The figure below shows an example of the two areas "Module view" and "Details". You can find a detailed explanation of the icons in the following table.



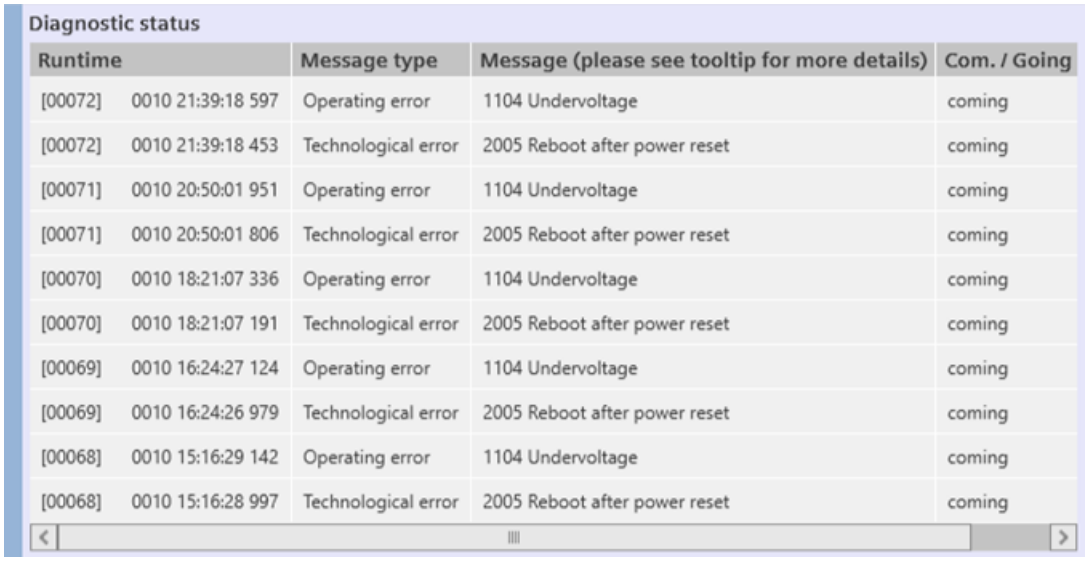
"Module view" area

	"Configuration" area: Create backup of the currently selected module. "Module view" area: Open/store configurations within the station.
	Activate/deactivate service mode.
	Execute service commands
	Execute scale commands
	Execute display commands
	Show diagnostics status Click the button to open the error buffer of the module.

Area "Details > Commissioning tab"

	Send data records from the MFCT to the module. You can only click the button if the PC values and the SIWAREX values are different from each other.
	Read in data records from the module to the MFCT.
	Open pop-up window with a strongly magnified weight display.

You see the error buffer of the module in the "Diagnostic status" display.



More information

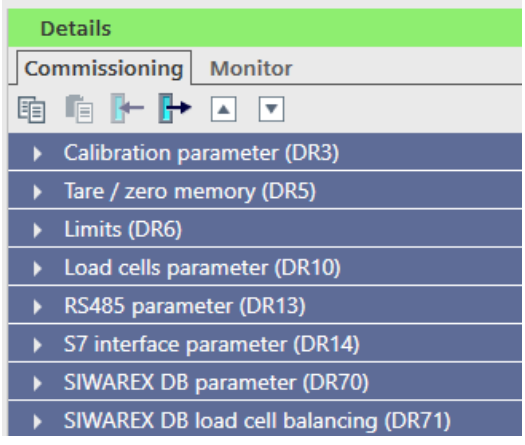
You can find more information on the commands and parameters in the respective equipment manuals.

- TM SIWAREX WP321 (https://support.industry.siemens.com/cs/ww/en/view/109770838)
- TM SIWAREX WP341 (https://support.industry.siemens.com/cs/ww/en/view/109813264)
- TM SIWAREX WP351 (https://support.industry.siemens.com/cs/ww/en/view/109825886)

10.4 Commissioning and monitoring

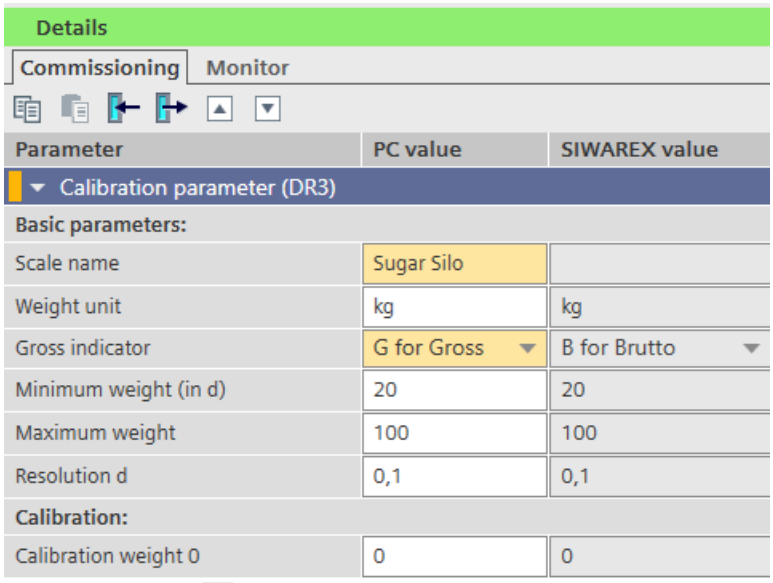
Commissioning

In the "Details > Commissioning tab" area, you can view the module's data records and edit their parameters.



To change, for example, the adjustment parameters in data record 3 (DR3) of the SIWAREX WP321 module, proceed as follows:

1. Click the button to read all data records from the WP321 module into the MFCT.
2. Change the desired parameters.
   Parameters that have been changed but not yet transferred are highlighted in yellow.



3. Click the button to write all data records from the MFCT to the WP321 module.

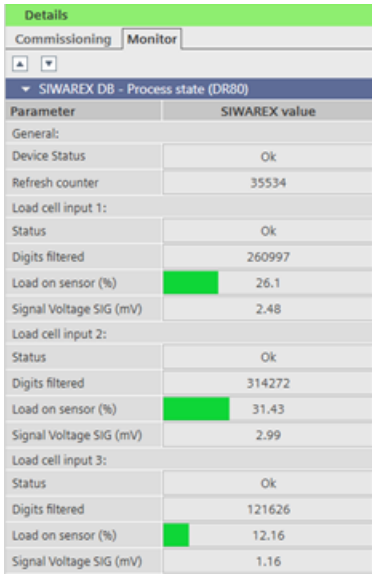
Result: The changed parameters have been transferred to the WP321 module.

You can expand or collapse all parameters by clicking the button .

A right-click in the "Parameters" area opens a context menu with further options for managing data records.

Monitoring

You can read-access and monitor all process data on the "Monitor" tab.



PtP Event Trace

11

The PTP Event Trace application is available as a plug-in in the MFCT. To use the "PtP Event Trace" application, activate the plug-in.

Once you have activated the plug-in, you can find PtP Event Trace on the start page as an application. In an opened application, you can find PtP Event Trace as a tab in the area of the button for the start screen.

You have the following options with the PtP Event Trace plug-in in combination with a SIMATIC CM PtP module:

- Read Event Traces
- Analyze serial communication
- Display the current configuration

More information

You can learn how to activate a plug-in in the section Plug-ins (Page 30).

You can find more information on the CM PtP module in the CM PtP (https://support.industry.siemens.com/cs/ww/en/view/109793681) equipment manual.

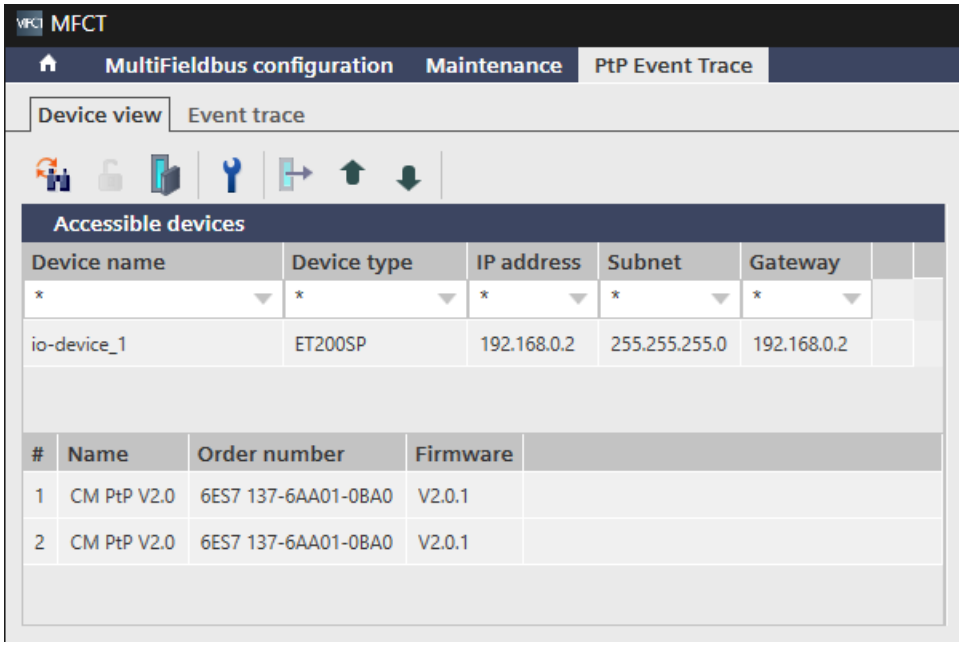
You can find more information on the configuration in the CM PtP - Configurations for point-to-point connections (https://support.industry.siemens.com/cs/ww/en/view/59057093) Function Manual.

11.1 Selecting a station with CM PtP module

You scan for stations with integrated CM PtP modules and can read out the traces of the modules on the "Device view" tab.

This offers you the following options:

- Analyze serial communication data
- Display the configuration of the serial interface



Procedure

To read out the trace from a CM PtP module, proceed as follows:

1. Click the "Start scan" button to scan for accessible devices.
2. Click the button to display only the devices with a CM PtP module.
3. To read out the trace from a CM PtP module:
   - Select the station
   - Select the CM PtP module
   - Click the button .

Result: The "Module details" tab shows the parameters of the CM PtP module.

Module details

Identification & Maintenance

Parameter	Value
Order number	6ES7 137-6AA01-0BA0
Serial number	S C-T7A10N7P2025
Firmware version	V2.0.1
Plant designation	
Location identifier	
Installation date	
Additional information	
Slot	1

Port configuration

Parameter	Value	
Specification of the operating mode	RS232C	
Receive line initial state	Keine	
Protocol	Freeport/Modbus	
Modbus CRC active	False	
Transmission rate	9600	bits/s

Importing/exporting trace files

To export a trace file, proceed as follows:

1. Read the trace of the selected module.
2. Click the "Export trace file" button .
3. Save the file in a location of your choice.

Result: You have saved the file in *.json format.

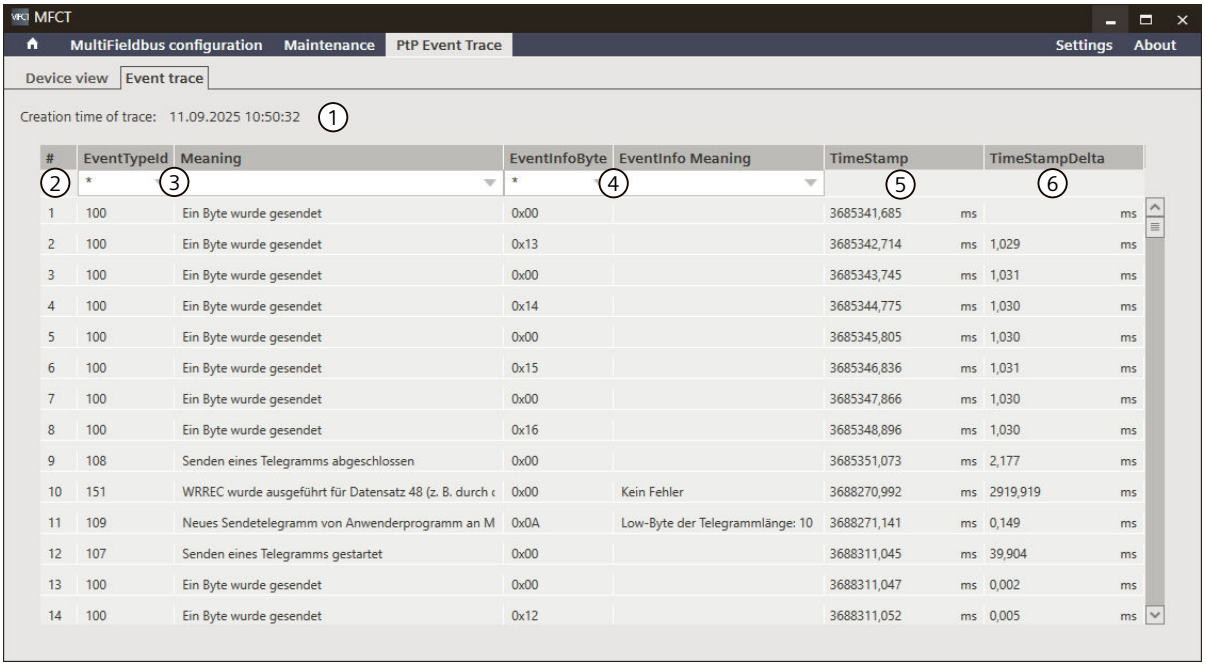
To import a trace file, proceed as follows:

1. Click the "Import trace file" button .
2. Select the desired file in *.json format.

Result: The "Module details" tab shows the saved parameters.

11.2 Analyzing a trace

The "PtP Event Trace" tab shows a table with the trace data.



#	EventTypeId	Meaning	EventInfoByte	EventInfo Meaning	TimeStamp	TimeStampDelta
1	100	Ein Byte wurde gesendet	0x00		3685341,685 ms	ms
2	100	Ein Byte wurde gesendet	0x13		3685342,714 ms	1,029 ms
3	100	Ein Byte wurde gesendet	0x00		3685343,745 ms	1,031 ms
4	100	Ein Byte wurde gesendet	0x14		3685344,775 ms	1,030 ms
5	100	Ein Byte wurde gesendet	0x00		3685345,805 ms	1,030 ms
6	100	Ein Byte wurde gesendet	0x15		3685346,836 ms	1,031 ms
7	100	Ein Byte wurde gesendet	0x00		3685347,866 ms	1,030 ms
8	100	Ein Byte wurde gesendet	0x16		3685348,896 ms	1,030 ms
9	108	Senden eines Telegramms abgeschlossen	0x00		3685351,073 ms	2,177 ms
10	151	WRREC wurde ausgeführt für Datensatz 48 (z. B. durch (	0x00	Kein Fehler	3688270,992 ms	2919,919 ms
11	109	Neues Sendetelegramm von Anwenderprogramm an M	0x0A	Low-Byte der Telegrammlänge: 10	3688271,141 ms	0,149 ms
12	107	Senden eines Telegramms gestartet	0x00		3688311,045 ms	39,904 ms
13	100	Ein Byte wurde gesendet	0x00		3688311,047 ms	0,002 ms
14	100	Ein Byte wurde gesendet	0x12		3688311,052 ms	0,005 ms

①	Creation time of the trace	Creation time with the date and time of the CPU.
②	#	Consecutive numbering of the entries.
③	EventType and meaning	Type of event as a decimal number (EventType) and text (meaning).
④	EventInfoByte and EventInfo meaning	Additional event information as a hexadecimal number (EventInfoByte) and text (EventInfo meaning).
⑤	Time stamp	Relative time stamp of the event in milliseconds, for time analysis between the individual events.
⑥	Time stamp delta	Time difference between two consecutive events. If the table has been filtered, the time difference from the previous event is displayed.

More information

A complete list of all possible events can be found in the "CM PtP - Configurations for point-to-point connections" Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59057093).

Maintenance

12

You have the following options in the "Maintenance" tab:

- Assign parameters (Page 92)
- Read service data (Page 93)
- Firmware update (Page 93)

After opening the MFCT, you can find "Maintenance" on the start page as an application. In an opened MFCT application, you can find "Maintenance" as a separate tab.

12.1 "Assign parameters" tab

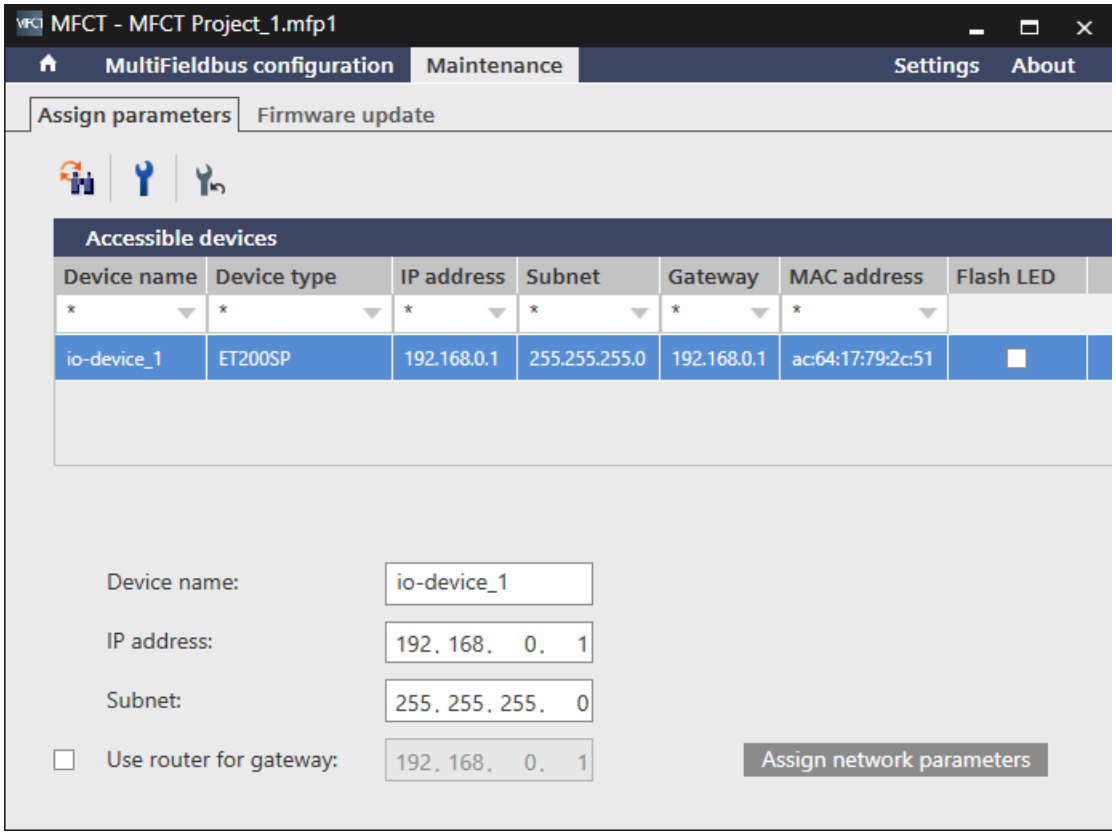
You have the following options in the "Assign parameters" tab:

- Assign network parameters (Page 92)
- Resetting to factory settings (Page 92)
- Defining scan settings (Page 92)

Procedure for displaying all accessible online devices

To display all accessible online devices, proceed as follows:

1. Click "Start scan" .
   The following figure shows the contents of the "Assign parameters" tab:



2. Select the desired device.
3. To more easily locate the selected device, you have the option of making the LEDs of the device flash. To do so, select the check box in the "Flash LED" column.

You have found your desired device and can now carry out the steps described below.

12.1.1 Assigning network parameters

Requirement: You have opened the view with your selected device.

To assign the network parameters for MF devices, proceed as follows:

1. In the lower area, you can find the device name, the IP address and the subnet in which the selected device is located. If necessary, change this information.
2. If you are using a gateway, select the "Use router for gateway" check box.
3. Enter the address of the router.
4. To complete the entries, click the "Assign network parameters" button.

You will receive a message that the assignment of the network parameters was successful.

12.1.2 Resetting to factory settings

Requirement: You have opened the view with your selected device.

To reset a device to factory settings, click the "Reset network parameters" button .

After a positive answer to the confirmation prompt, the network parameters are reset to the factory settings.

12.1.3 Defining scan settings

To define the scan settings, proceed as follows:

1. Click the "Scan settings" button .
2. In the "Scan range" selection menu, select the area you want to scan:
   - All devices
   - Devices in the IP address range
   - Devices with specific IP address
   - Use the grid filter for network scans
3. Use the "Communication with CPUs" check boxes to select the following options:
   - Inclusion of centrally working modules
   - Include devices found via IP forwarding in other subnets
4. Confirm the selection with the "OK" button.

You have made and completed the settings for the scan.

12.2 "Read service data" tab

Requirement

The ET 200 station supports this function.

Procedure

To read out and save provided service data, proceed as follows:

1. Click "Start scan" .
2. Select the desired device.
3. To locate the selected device, you have the option of making the LEDs of the device flash. To do so, select the check box in the "Flash LED" column.
4. Enter the path under which you want to save the service data in the "Service data output path" text box at the bottom.
5. Click the "Start" button.

You will receive a message that the reading of the service data has been successfully completed.

12.3 "Firmware update" tab

The firmware update allows you to load or activate new firmware in multiple devices in parallel during operation. The devices continue to run without interruption.

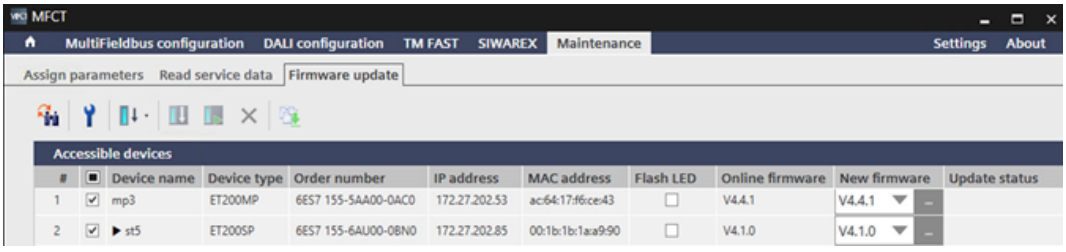
You have the following options in the "Firmware update" tab:

- Settings for firmware update (Page 94)
- Update firmware (Page 97)
- Activate firmware (Page 100)

Procedure to display all accessible online devices

To display all accessible online devices, proceed as follows:

1. Click the "Start scan" button .
   The following figure shows a section of the contents of the "Firmware update" tab:

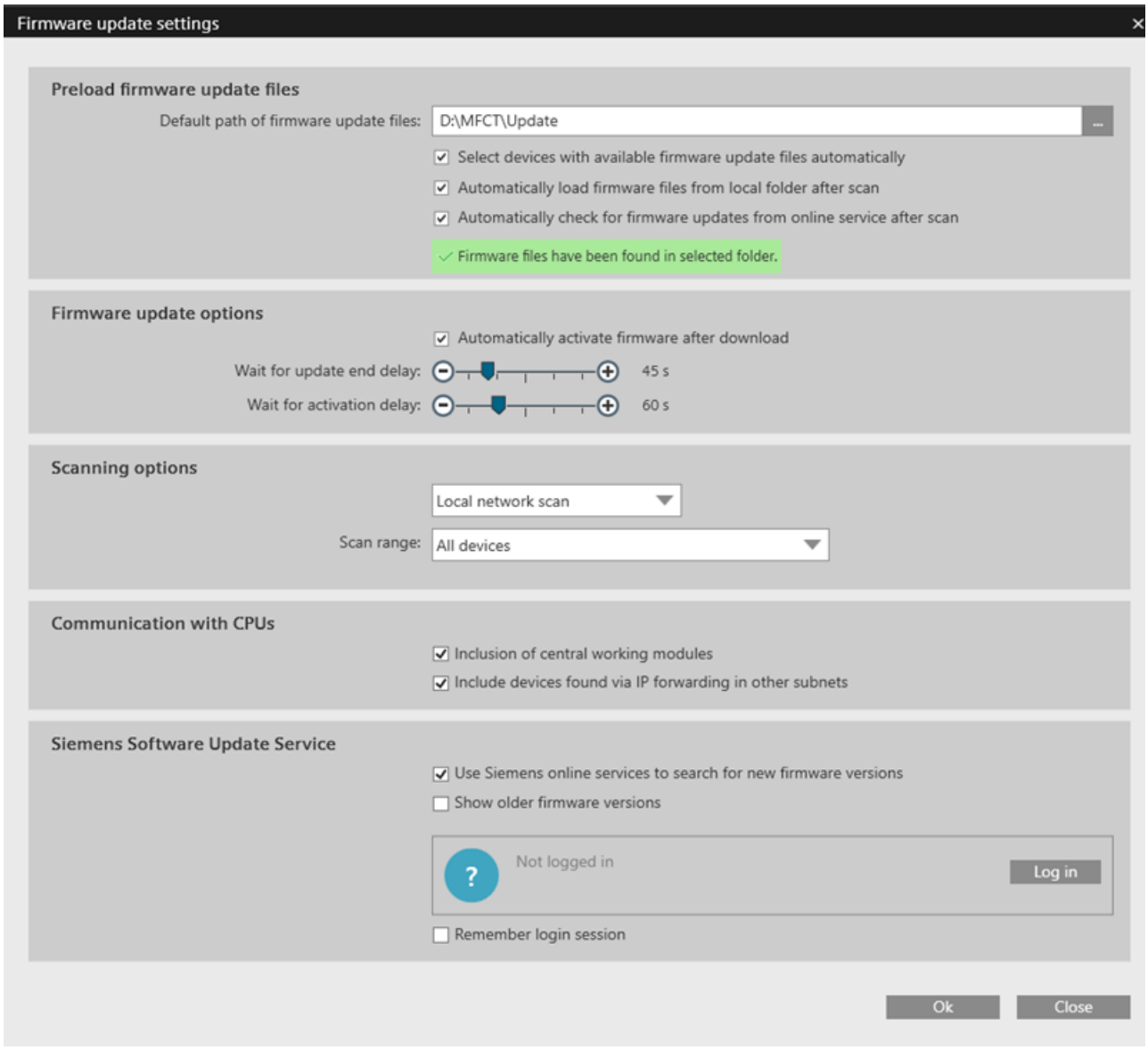


You have found your devices and can now carry out the steps described below.

12.3.1 Settings for firmware update

To make the settings for the firmware update, proceed as follows:

1. Click .
   The following figure shows the contents of the "Firmware update settings" window:



In the "Firmware update settings" window that opens, you can now make the settings explained below.

Preload the firmware update file

In the "Preload firmware update file" area, you can find the "Default path of firmware update file" text box. Here, you specify the storage path for the firmware update file.

When the "Select devices with available firmware update files automatically" check box is selected, all devices in the network for which the following criteria are met are automatically identified:

- a suitable firmware update file is available, and
- an update is possible or required, e.g. because the current firmware is out of date.

With the following options, you determine which firmware files the MFCT should display during updates:

- After the scan, automatically load firmware files from the local directory:
  The MFCT displays the locally stored firmware files in the selection menu during updates.
- After the scan, automatically check for firmware updates from the online service:
  The MFCT displays the firmware files provided by the Siemens Software Update Service in the selection menu during updates.
  This option is only available if the "Use Siemens online services to search for new firmware versions" option is enabled in the "Siemens Software Update Service" area.

Firmware update options

To activate the new firmware **directly after loading**, select the "Automatically activate firmware after download" check box. This option must be enabled in order for the two options below it to take effect.

- "Wait for update end delay": Specifies the delay time between the sending of the update file and the confirmation by the module that it received it.
  This prevents an unwanted cancellation of the download to the device.
- "Wait for activation delay": After the successful download, the MFCT waits the set amount of time before activating the firmware and restarting the device.

You can find information on the delay times in the respective equipment manual of the module. The times must be adjusted to the module with the longest delay time.

Scanning options

In the "Scanning options" area, you can determine whether the scan if to be run locally or whether subnets are also to be included.

You can find the further procedure in the section Set scanning options (Page 96).

Communication with CPUs

In the "Communication with CPUs" area, select the range in which the network scan should detect modules.

- "Inclusion of centrally working modules" check box:
  The network scan detects centrally plugged modules on a CPU.
- "Include devices found via IP forwarding in other subnets" check box:
  The network scan also detects devices in other subnets.

Siemens Software Update Service

If this section is not shown, this service is currently unavailable.

The Siemens Software Update Service is an automated service that ensures that your SIMATIC software is always up to date.

To use the service, you must register with the Siemens Software Update Service. After successfully registering, click the "Log in" button to connect your MFCT to the Siemens Software Update Service.

Select the "Use Siemens online services to search for new firmware versions" check box to allow the MFCT to search for available firmware files using the Siemens Software Update Service.

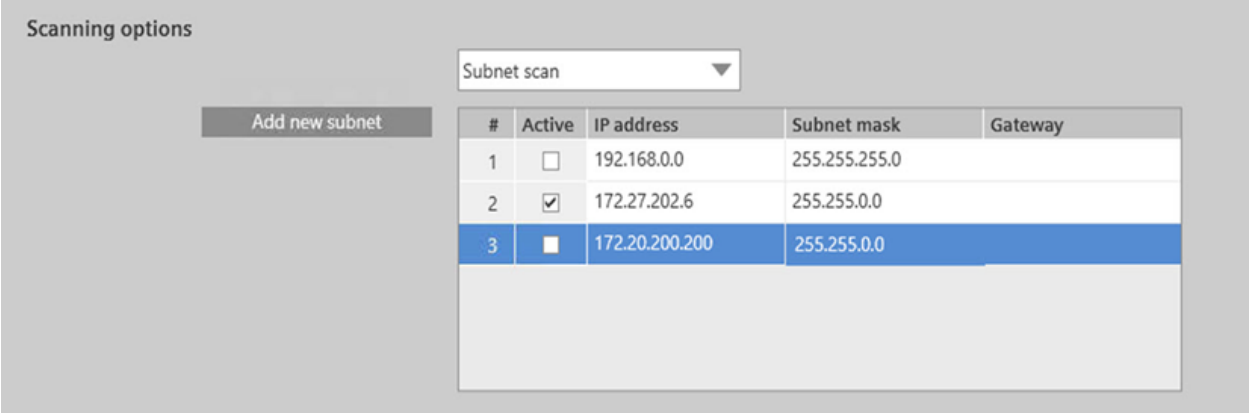
If you select the "Show older firmware versions" option, the Siemens Software Update Service will also display previous firmware files for the modules.

Select the "Remember login session" option to save your login credentials. If you are already logged in and you enable the option, you will be logged out of the Siemens Software Update Service and will need to log in again once.

12.3.1.1 Setting scanning options

To set the scan options, proceed as follows:

1. In the "Scan options" drop-down list, select the area you want to scan:
   - Local network scan: update the firmware in the local network
   - Subnet scan: update the firmware in multiple subnets
     The following figure shows an example of the three subnets found:



2. Enter the following details for each subnet:
   - IP address
   - Subnet mask
   - Address for the gateway
3. To create a new subnet and add it to the list, click the "Add new subnet" button.
4. To complete the entries, click the "OK" button.

You have made and completed the settings for the scan options.

12.3.2 Updating firmware

NOTE

We recommend that you do not connect directly with the device which you want to update. The activation of the new firmware can lead to a loss of the scanned devices due to a brief interruption of the network connection at the network adapter.

Procedure - Checking for updates

To check whether firmware updates are available for your devices, proceed as follows:

1. Click "Start scan" .
   All devices are displayed.
2. Optional: Use the incremental search function to locate the desired MF devices and modules. The search starts immediately after you enter the first character. The search query is refined with each additional character. The results are dynamically adapted according to your entry.

Accessible devices

#		Device name	Device type	Order number	IP address	MAC address	Flash LED	Online firmware	New firmware
		*	*	6ES7131	*	*		*	
2.07	☐	DI 8x24VDC HF V1.0	Digital	6ES7 131-6BF00-0CA0				V1.0.0	
2.08	☐	DI 8x24VDC HF V2.0	Digital	6ES7 131-6BF00-0CA0				V2.0.3	

3. Click the "Check for updates" button.
   The MFCT opens the selection menu with the available options for searching for firmware updates.
4. Select one of the following options in the shortcut menu:
   - Check for all updates:
     The MFCT searches online and locally for firmware updates.
   - Check for online updates:
     The MFCT searches the Siemens Software Update Service for firmware updates.
   - Check for local updates:
     The MFCT searches locally for firmware updates in the path you selected in the firmware update settings.

NOTE

Separation of the plant network and the Internet

To search online for firmware updates, your PG/PC must have an Internet connection. If it is not possible to connect to both the plant network and the Internet at the same time, proceed as follows:

1. After the scanning process, disconnect the plant network from your PG/PC.
2. Connect to the Internet.

Result: You have started the check for current firmware files.
The MFCT searches for available firmware updates based on your selection. The following subsections explain how to select firmware updates and load them onto the devices.

Procedure – Selecting and downloading the firmware file

Once the MFCT has finished checking for firmware updates, proceed as follows:

1. Navigate to the "New firmware" column.
2. In the selection menu, choose which firmware file you want to use for each device.
   Firmware files that are available online are indicated by the Internet icon | V2.0.3 | in the MFCT.



Intermediate result: You have selected the desired firmware file for all the required devices.

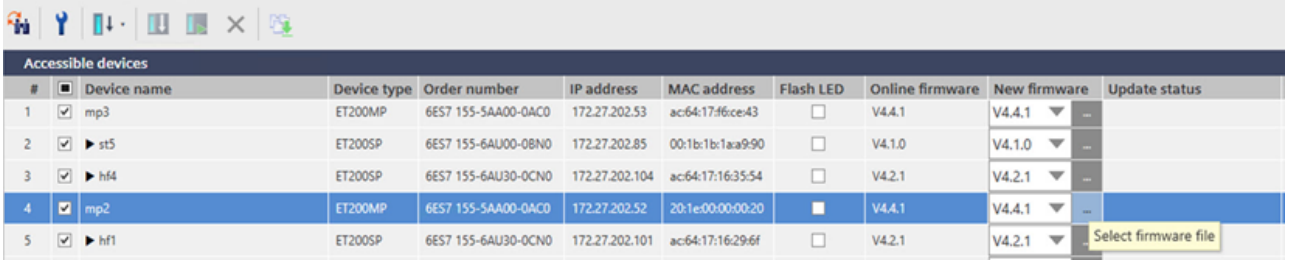
If you want to use firmware files that are available online but you are not connected to your plant network, click the "Download all online firmware" button. The MFCT downloads the selected firmware files and saves them in the path you specified in the firmware update settings. The "Update status" column shows the current progress.

The downloaded firmware files are then displayed in the device selection menus just like locally stored firmware files.

Procedure - Loading firmware to the devices

To load the firmware on the devices, proceed as follows:

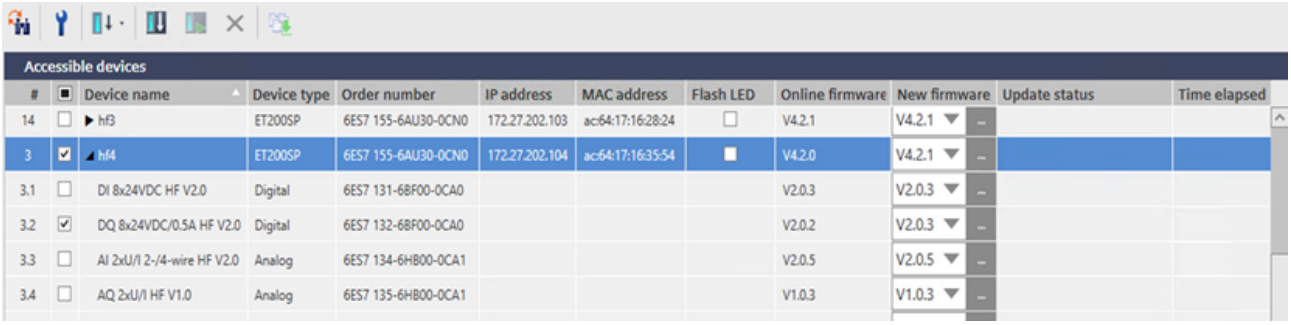
1. Optional: Reconnect your plant network to the PG/PC where the firmware updates are stored.
2. Set the appropriate firmware file for each device.
   Recommendation: If you are using a STEP 7 firmware update file, select the file: header.upd.



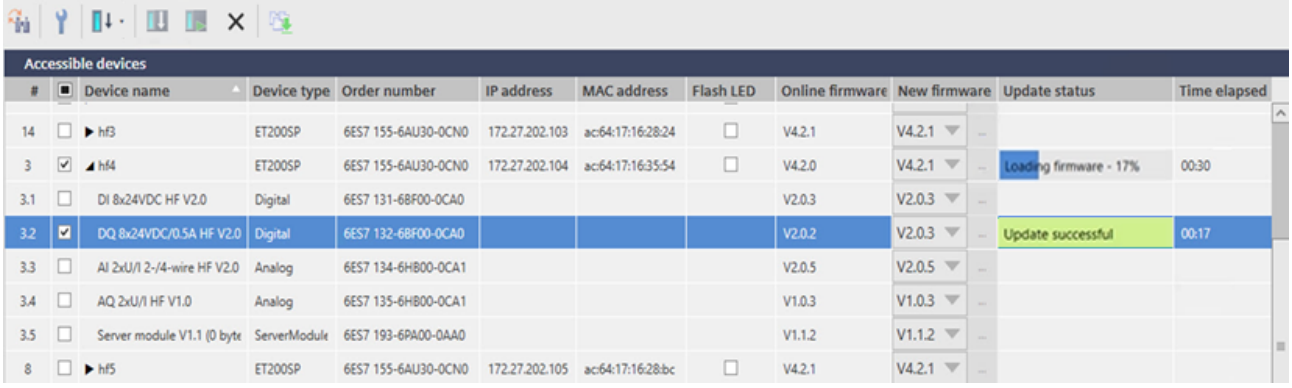
NOTE

Select a directory, which contains subdirectories with firmware files.
If you select large directories, entire hard disks (for example C:\) or directories on network drives, the corresponding access can take very long or MFCT can no longer react.

3. Select the devices to be updated.



4. To start the firmware update for the selected devices, click the "Update firmware" button .
   The update can be canceled at any time using the "Cancel" button .



NOTE

If you cancel the update of the firmware in the "Initialization" or "Waiting" phase, it takes some minutes until the MF devices are ready again and you can restart the update.

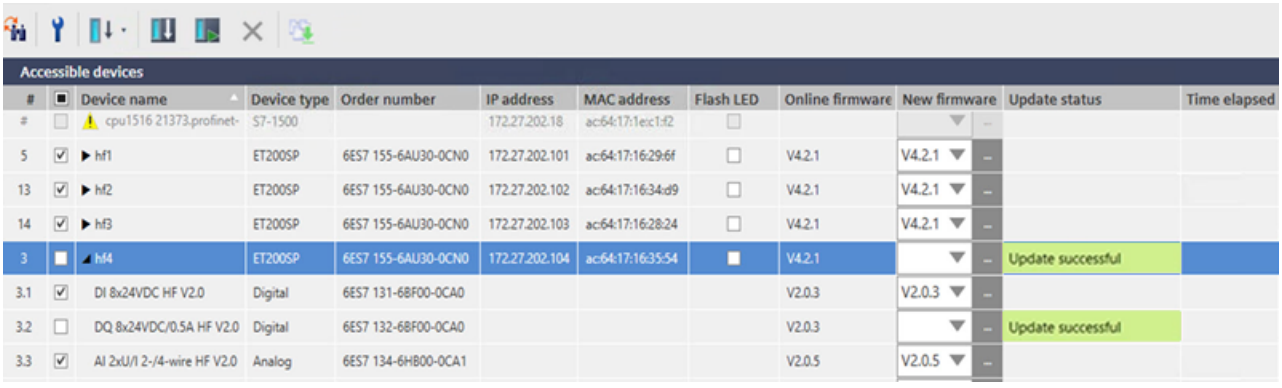
12.3.3 Activating the firmware

The new firmware is not active yet once the firmware update has been successfully performed. You can activate the firmware on the device later.

Procedure

To activate the firmware, proceed as follows:

1. Click the "Start scan" button . You can recognize devices with updated firmware that has not been activated yet in the device table by scanning again.
2. Select the devices whose firmware you want to activate.



3. Click the "Activate firmware" button . This activates the firmware of the selected devices one after the other.
4. If activation fails, scan the network again.

Once activation is complete, all selected devices should have the latest firmware version.

SIEMENS

System overview 1

Integration into the automation system 2

SIMATIC

IO-Link system

Function Manual

05/2024
A5E31637677-AB

Introduction

Purpose of the documentation

This function manual provides a general overview of the IO-Link communication system.

It shows the interaction of the various components of an IO-Link system and will help you improve your general understanding of IO-Link.

Basic knowledge required

The following knowledge is required in order to understand the documentation:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Proficiency with STEP 7

Scope of the documentation

This documentation is the basic documentation for IO-Link systems at Siemens. The product documentation is based on this documentation.

Conventions

In this documentation, "STEP 7" is used as a synonym for all versions of the configuration and programming software "STEP 7 (TIA Portal)".

Please also observe notes marked as follows:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Additional support

- Information about Technical Support is available in section Siemens Industry Online Support (Page 4).
- The range of technical documentation for the individual SIMATIC products and systems can be found on the Internet (https://support.automation.siemens.com/WW/view/en/58649293).
- Information about the online catalog and online order system is available in section SiePortal (Page 4).

Guide

Documentation

Various IO-Link products are available from Siemens. Each of these products has a separate documentation. The IO-Link products are embedded in systems, e.g. ET 200SP. The documentation for the system consists of the respective system manual, function manuals and manuals. In addition, the STEP 7 online help and the Port Configuration Tool S7-PCT online help assist you in configuring and programming your automation system with IO-Link.

IO-Link components from Siemens

Siemens offers a wide range of products and support for IO-Link:

- Master
- Device, I/O modules
- Device, industrial switchgear
- Device, RFID systems (RFID = radio-frequency identification)
- Device, process instrumentation
- Device, signaling columns
- Device, power supplies
- Port Configuration Tool - S7-PCT (https://support.industry.siemens.com/cs/ww/en/view/32469496)
- IO-Link library (https://support.industry.siemens.com/cs/ww/en/view/82981502) with the blocks "LIOLink_Master" and "LIOLink_Device"
- Overview of the topic IO-Link (http://www.siemens.com/io-link)
- IT connection of IO-Link devices via OPC UA with the Field Data Enabler PN

Additional information on the products can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109737170).

Additional documentation for IO-Link

You can find a free download of the latest documentation on the IO-Link products on the Internet (https://support.industry.siemens.com/cs/CN/en/ps/15818/man).

Siemens Industry Online Support

You can find current information on the following topics quickly and easily here:

- **Product support**
  All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.
- **Application examples**
  Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.
- **Services**
  Information about Industry Services, Field Services, Technical Support, spare parts and training offers.
- **Forums**
  For answers and solutions concerning automation technology.
- **mySupport**
  Your personal working area in Industry Online Support for messages, support queries, and configurable documents.

This information is provided by the Siemens Industry Online Support in the Internet (http://www.siemens.com/automation/service&support).

SiePortal

SiePortal is the catalog and ordering system of Siemens AG for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).

You can find catalogs for all automation and drive products on the Internet (https://mall.industry.siemens.com).

Open-source software

Open-source software is used in the firmware of the SIMATIC Drive Controller. The open-source software is provided free of charge. We are liable for the product described, including the open-source software contained in it, pursuant to the conditions applicable to the product. Siemens accepts no liability for the use of the open-source software over and above the program sequence intended for our product, or for any faults caused by modifications to the software.
For legal reasons, we are obliged to publish the original text of the license conditions and copyright notices.

You will find these on the Internet with the firmware downloads

Table of contents

1 System overview 6

1.1 Advantages of IO-Link 6

1.2 Overview of IO-Link system 7

1.3 IO-Link interface 9

1.4 IO-Link protocol 11

1.5 Device profiles 13

1.6 IODD and Port Configuration Tool - S7-PCT 14

1.7 Differences between IO-Link specifications V1.0 and V1.1 16

2 Integration into the automation system 17

2.1 Configuration of the IO-Link system 17

2.1.1 Configuration with S7-PCT 20

2.1.2 Configuration without S7-PCT 22

2.1.3 Comparison of the configuration options 24

2.2 Data access of the automation system and the HMI device 25

2.3 Changing and saving device parameters during plant operation 26

2.4 Replacing a master or device during operation 28

System overview

1

Introduction

A continuous communication down to the lowest field level ensures enhanced use of the functions and performance capability of sensors and actuators. Enhanced use of sensors and actuators allows you to operate your machines and plants more productively.

No data other than the actual process value can be exchanged via the standard interfaces (digital, analog) used at the sensor/actuator level. Sensors and actuators with integrated intelligence are now used for increasingly complex functions and require a communication interface tailored to these requirements.

Definition

IO-Link is an innovative, point-to-point communication interface for the sensor/actuator area that is specified in IEC 61131-9.

IO-Link consists of the following system components:

- IO-Link master
- IO-Link device and device-specific description files (IODD)
- Unshielded 3-wire or 5-wire standard cable
- Engineering tool for configuring and assigning parameters of IO-Link

1.1 Advantages of IO-Link

The IO-Link system offers significant advantages as digital interface when connecting sensors/actuators:

- Open standard in accordance with IEC 61131-9
  - Devices can be integrated in the same way in all conventional fieldbus systems and automation systems
- Tool supported parameter setting and central data management
  - Fast configuration and commissioning
  - Simple creation of current plant documentation even for sensors/actuators
- Single, uniform wiring and far fewer different interfaces at the sensors/actors
  - Standardized, uniform interface for sensors and actuators independent of their complexity (switching, measuring, multi-channel, binary, mixed signals, etc.)
  - Reduction in the variety of types and inventory
  - Fast commissioning
  - Any combination of IO-Link devices and sensors/actuators without IO-Link at IO-Link master

- Continuous communication between sensors/actuators and the CPU
  - Access to all process data, diagnostic data and device information
  - Access to device-specific data, such as energy data
  - Remote diagnostics can be performed
- Continuous diagnostic information down to sensor/actuator level
  - Reduction in troubleshooting effort
  - Minimizing risk of failure
  - Preventive maintenance and optimization of service and maintenance planning
- Dynamic change of sensor/actuators parameters by the controller or the operator at the HMI
  - Reduction in downtimes during product change
  - Increased variability of the machine
- Automatic reassignment of parameters when devices are replaced during operation
  - Minimization of downtimes
  - Device replacement by untrained personnel without additional aids
  - Avoidance of incorrect settings
- Integrated device identification
  - Identification of the installed devices
  - Ensure quality of result in production and manufacturing when replacing the device

1.2 Overview of IO-Link system

Components

A Siemens IO-Link system consists of the following components:

- IO-Link master
- IO-Link device, for example:
  - Sensors/actuators
  - RFID readers
  - I/O modules
  - Signaling columns
  - ...
- Unshielded 3-wire or 5-wire standard cables
- Engineering tool for configuring and assigning parameters of IO-Link
- IT connection via OPC UA

Example plant with IO-Link

The figure below shows an example of plant architecture with IO-Link.

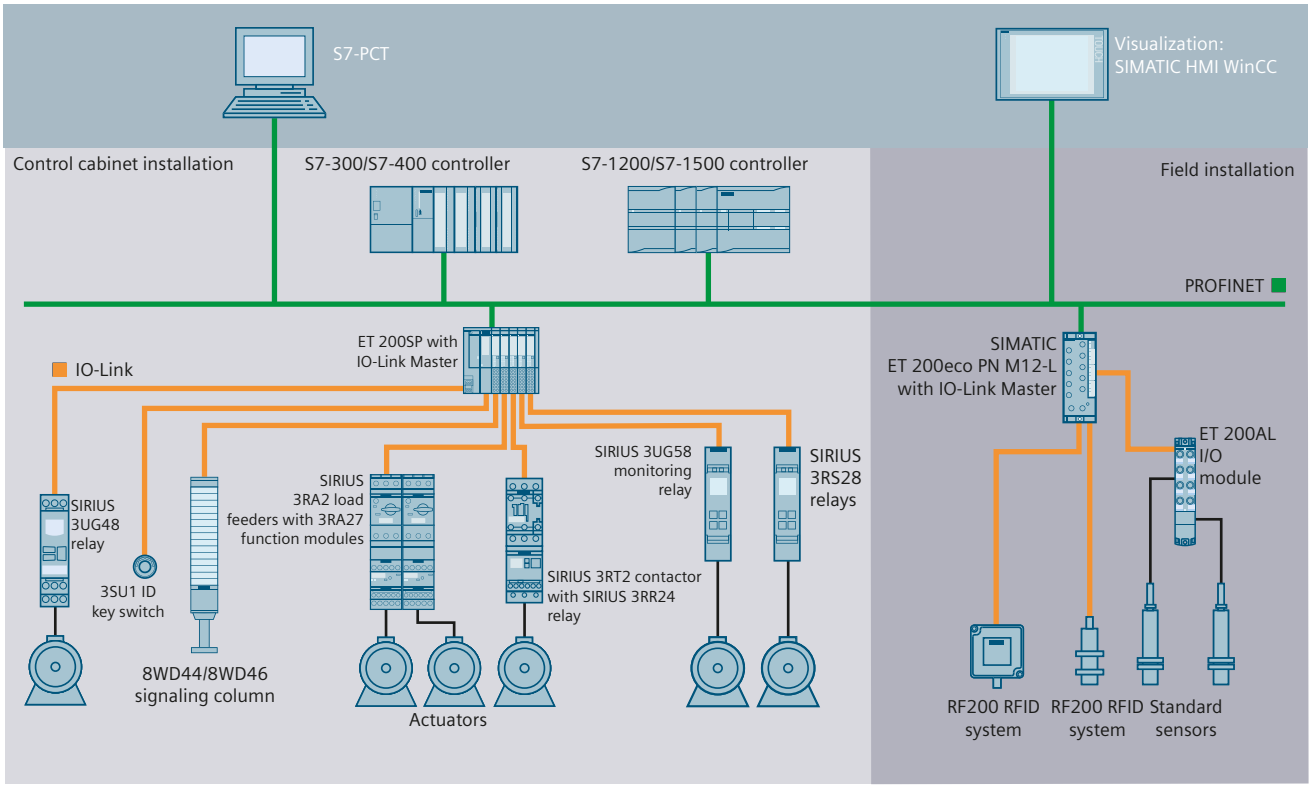


Figure 3-541 Plant architecture with IO-Link

The IO-Link master establishes the connection between the IO-Link devices and the automation system. If the IO-Link master is a component of the I/O system, it is installed either in the control cabinet or directly in the field as remote I/O in degree of protection IP65/67/69K. The IO-Link master communicates by means of various fieldbuses or product-specific backplane buses. An IO-Link master can have multiple IO-Link ports (channels). An IO-Link device can be connected (point-to-point communication) to each port.

Engineering

The IO-Link system is engineered parallel to the overall automation system and can be embedded in it and intermeshed with it.

1.3 IO-Link interface

Introduction

The IO-Link is a serial, bidirectional point-to-point connection for signal transmission and power distribution under any network, fieldbus or backplane bus.

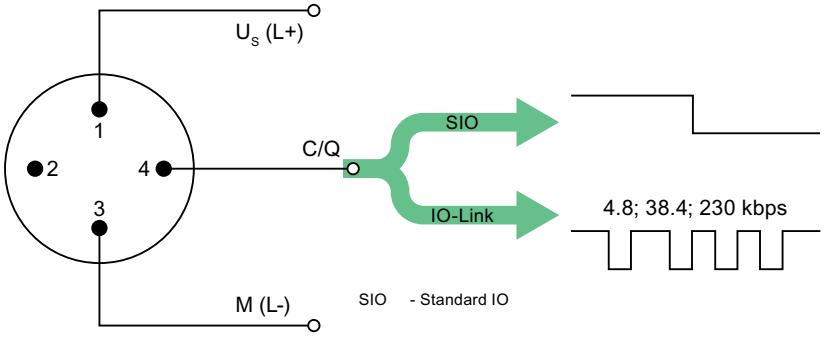
Connection system in IP65/67/69K

M12 connectors and other connectors are defined for the connection system in IP65/67/69K; sensors have a 4-pin connector, actuators a 5-pin connector. IO-Link masters are always equipped with a 5-pin M12 socket.

The pin assignment according to IEC 60974-5-2 is specified as follows:

- Pin 1: 24 V
- Pin 3: 0 V
- Pin 4: Switching and communication cable (C/Q)

In addition to IO Link communication, these three pins also implement the power supply of the device.
Detailed information about the power supply can be found in the documentation of the utilized IO-Link master.



Pin	Signal	Definition	Standard
1	U_S (L+)	24 V	IEC 61131-2
2	-	not defined	-
3	M (L-)	0 V	IEC 61131-2
4	Q	Switching signal DI, DQ (SIO)	IEC 61131-2
4	C	"coded switching signal" (IO-Link)	IEC 61131-9

Figure 3-542 Pin assignment IO-Link device

Port types in IP65/67/69K

Two types of ports are distinguished in the specifications for IO-Link masters:

- Port Class A (Type A)
  With this type, the functions of pins 2 and 5 are not assigned. The manufacturer defines this function. Generally, an additional digital channel is assigned to pin 2.

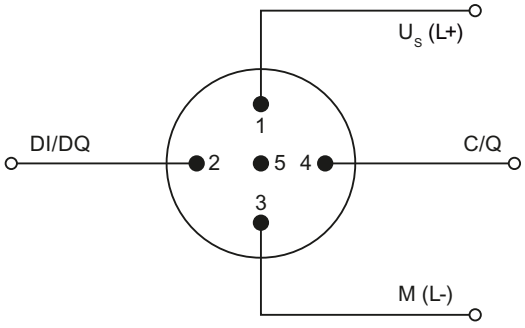


Figure 3-543 Pin assignment Port Class A

- Port Class B (Type B)
  This type offers an additional supply voltage and is suitable for the connection of devices that have an increased power requirement. In this case an additional (galvanically isolated) supply voltage is made available by pins 2 and 5. A 5-wire standard cable is required to use this additional supply voltage.

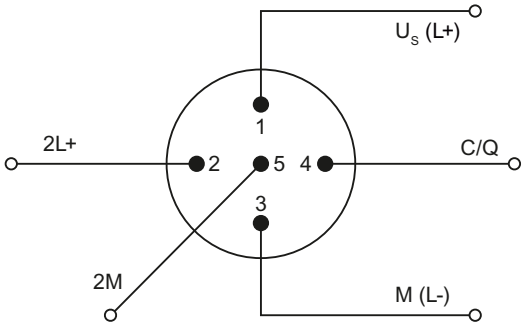


Figure 3-544 Pin assignment Port Class B

Connecting cables

The devices are connected to the master with unshielded 3-wire or 5-wire standard cables with a maximum length of 20 m. Standard cables can be used to wire the sensors. No shielding or compliance with specific regulations is necessary for the installation of the cables.

1.4 IO-Link protocol

Operating modes

The IO-Link port of the master can be operated in the following modes:

- IO-Link:
  The port is located in the IO-Link communication.
- DI:
  The port behaves like a digital input.
- DQ:
  The port behaves like a digital output.
- Disabled:
  The port is disabled.

Transmission rate

In the IO-Link specification V1.1, three data transmission rates (baud rates) are specified for the IO-Link operating mode:

- COM 1 = 4.8 kBaud
- COM 2 = 38.4 kBaud
- COM 3 = 230.4 kBaud (optional according to Specification V1.0)

The IO-Link device only supports one of the defined data transmission rates. The IO-Link master to Specification V1.1 supports all data transmission rates and adjusts automatically to the data transmission rated supported by the device.

Response time of the IO-Link system

The response time of the IO-Link system provides information about the frequency and speed of the data transmission between device and master. The response time depends on various factors.

A value for the minimum cycle time of the device is stored in the device description file IODD of the device (Page 14). This value indicates in which time intervals the master may address the device. The value has a big influence on the response time. The master also has an internal processing time that is factored into the calculation of the response time.

Devices with different minimum cycle time can be configured on a master. The response time for these devices differs accordingly. In other words, the response time for various devices connected to a master can vary greatly.

When you configure the master you can specify a fixed cycle time in addition to the device-specific minimum cycle time stored in the IODD. The master then addresses the device according to this specification.

The typical response time for a device thus results from the effective cycle time of the device and the typical internal processing time of the master.

Transmission performance

IO-Link is a very robust communication system. This communication system operates with a 24V level. If transmissions fail, the frame is repeated two more times. The IO-Link master only detects a break in communication after the failure of the second repeat attempt and reports this to the higher-level CPU.

Data types

Four data types are available:

- Process data → Cyclic data
- PQI → Cyclic data
- Device data → Acyclic data
- Events → Acyclic data

Process data

The process data of the devices is transferred cyclically in a data frame with the process data size being determined by the device. Process data from 0 to 32 bytes is possible per device (input and output, respectively).

Port Qualifier Information (PQI)

Each port has a Port Qualifier Information (PQI). This PQI provides information on the device status of the port and IO-Link (value status). The PQI is transmitted cyclically with the process data.

Device data

Device data can be parameters, identification data or diagnostic information. The data is exchanged cyclically and at the request of the IO-Link master. Device data can be written to the device and also read from the device.

Events

When an event occurs, the device signals to the master that an event is present. The master then reads the event. Events can be error messages (for example, short-circuit) and warning/maintenance data (for example, dirt, overheating).

Error messages are transferred from the device to the CPU or the HMI by the IO-Link master.

The IO-Link master can also transfer events and states. Such events are, for example, wire break, break in communication or overload.

Device parameters or events are transmitted independently of the cyclic transmission of process data. The transmissions do not influence or impair each other.

Startup of the IO system

If the port of the master is set to IO-Link mode, the IO-Link master attempts to communicate with the connected IO-Link device. For this purpose the IO-Link master sends a defined signal and waits for the reply of the IO-Link device.

The IO-Link master first attempts a communication with the highest defined data transmission rate. If this transmission attempt fails the IO-Link master attempts a communication with the lowest data transmission rate. The device always supports only one defined data transmission rate.

If the master receives a reply, communication starts. First they exchange communication parameters. If necessary the parameters stored in the system are transferred to the device.

Then the cyclic data exchange of process data and value status starts.

1.5 Device profiles

Introduction

Device profiles are defined for IO-Link to standardize access of the CPU user program to the devices.

Data structure, data contents and basic functionality are defined in the device profiles. A standard user view and an identical program access is thus achieved for a number of different devices that have the same device profile.

IO-Link profiles

The device profile "Smart Sensor Profile" is currently defined for IO-Link. This profile is especially suited for measurement sensors. In other words, measured values are transmitted in addition to switching points.

For the Smart Sensor Profile, the TIA Portal library for IO-Link ("LIOLink") contains function blocks (FBs) for "Adjustable Switching Sensors" (FB LIOLink_AdjSwitchingSensor), for "Multiple Adjusting Switching Sensors" (type 2, FB LIOLink_MultAdjSwitchingSensor), "Digital Measuring Sensors" (type 3) and "Digital Measuring Switching Sensors" (type 4) (both in LIOLink_MeasuredDataChannel FB).

The "Common Profile" profile is used for the manufacturer-independent reading of identification and diagnostics data from the devices and enables the writing of application-specific tags - it is supported by the FB LIOLink_IdentAndDiag.

In addition, the switchgear (for example, contactors) support the LVSG (Low Voltage Switchgear) profile defined in IEC 61915-2.

1.6 IODD and Port Configuration Tool - S7-PCT

Device description IODD

An electronic device description, the IODD file (IO Device Description) is available for each device. The IODD provides a wealth of information for system integration:

- Communication properties
- Device parameters with value range and default value
- Identification, process and diagnostic data
- Device data
- Text description
- Image of the device
- Manufacturer logo

The structure of the IODD is identical for all devices from all manufacturers. The structure of the IODD is always represented in the identical manner by the IO-Link Configuration Tool of the master manufacturer (for Siemens, S7-PCT). This ensures that the handling is the same for all IO-Link devices regardless of the manufacturer.

Two different IODD versions are available for devices that support both V1.0 and V1.1 functionality.

IODDfinder

The IODDfinder is a cross-vendor, central IO-Link database.
This database provides you with the latest IODDs of the device manufacturers and offers an information and download platform.
The IODDfinder is available on the Internet (https://ioddfinder.io-link.com).

As of version V3.5 SP3 update 2, S7-PCT can automatically access the IODD database and download missing IODDs, see SIOS (https://support.industry.siemens.com/cs/ww/en/view/32469496) under "What's New in PCT Version V3.5 SP3 update 2".

IO-Link configuration tool

Configuration tools are required to configure the entire IO-Link system. The IO-Link configuration tools of the master manufacturers are able to read IODDs.

The main tasks of the IO-Link configuration tool include:

- Assigning the devices to the ports of the master
- Address assignment of ports within the address area of the master
- Assigning parameters for the IO-Link device

Diagnostics can also be carried out on the connected devices.

This means the IO-Link configuration tool supports the transparent representation of the IO-Link system down to field level.

Siemens provides S7-PCT for engineering of the IO-Link system.

S7-PCT with IODD of a device

The following figure shows a section from S7-PCT with IODD of a device and the device information contained therein.

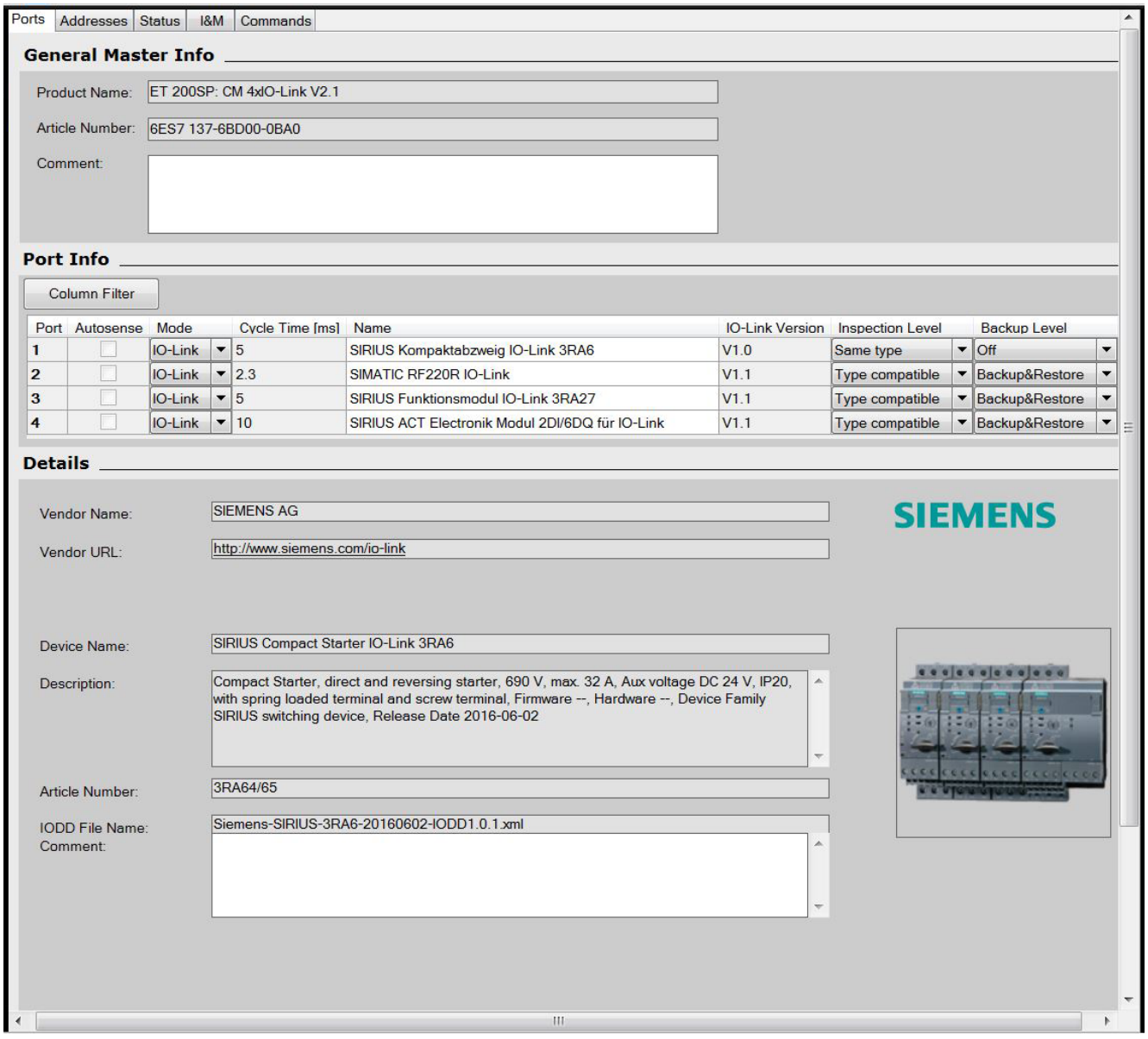


Figure 3-545 S7-PCT with IODD of a device and the device information contained therein

1.7 Differences between IO-Link specifications V1.0 and V1.1

Specification

The technical definition of the IO-Link system is described in a specification of the IO-Link consortium. The first step was the creation of specification version 1.0. The further development and added functions of the IO-Link system led to version 1.1.

The main enhancements of version 1.1 are:

- Data backup for device replacement during operation (Backup&Restore)
- Data transmission rate 230.4 kBaud is mandatory for the IO-Link master

Combination of IO-Link devices

Note the following when combining IO-Link devices:

- Only IO-Link devices that comply with V1.0 can be operated on the IO-Link master to V1.0.
- IO-Link devices that comply with V1.0 and V1.1 can be operated on the IO-Link master to V1.1.
- Data backup and a data transmission rate of 230.4 kBaud of the IO-Link master after V1.1 can only be used when these functions are also supported by the IO-Link device and the IO-Link master (optionally as of V1.0).
- IO-Link master after V1.0 only optionally supports 230.4 kBaud. If IO-Link master V1.0 does not support 230.4 kBaud, then communication with an IO-Link device with 230.4 kBaud is not possible.

Integration into the automation system 2

2.1 Configuration of the IO-Link system

Introduction

An IO-Link system is configured in several steps. In the first step, the master is integrated in the automation system and configured. In the second step, the IO-Link devices are configured.

Integration in the automation system

When using a SIMATIC S7 CPU, use the engineering tool STEP 7, V5.x or STEP 7 (TIA Portal) for configuration.
The IO-Link system is represented by the IO-Link master in the configuration of the automation system or the fieldbus and integrated with STEP 7 or a GSD file.
The IO-Link master itself can be a field bus node (e.g. ET 200eco PN IO-Link master) or a part of the modular IO system that is connected to the field bus (e.g. ET 200SP IO-Link master). In both cases, the number of ports, the address range and the module properties are described in STEP 7 or in the GSD file.

Example configuration in STEP 7 (TIA Portal)

The figure below shows a PROFINET configuration with integrated PROFINET devices ET 200SP and ET 200eco PN with IO-Link masters.

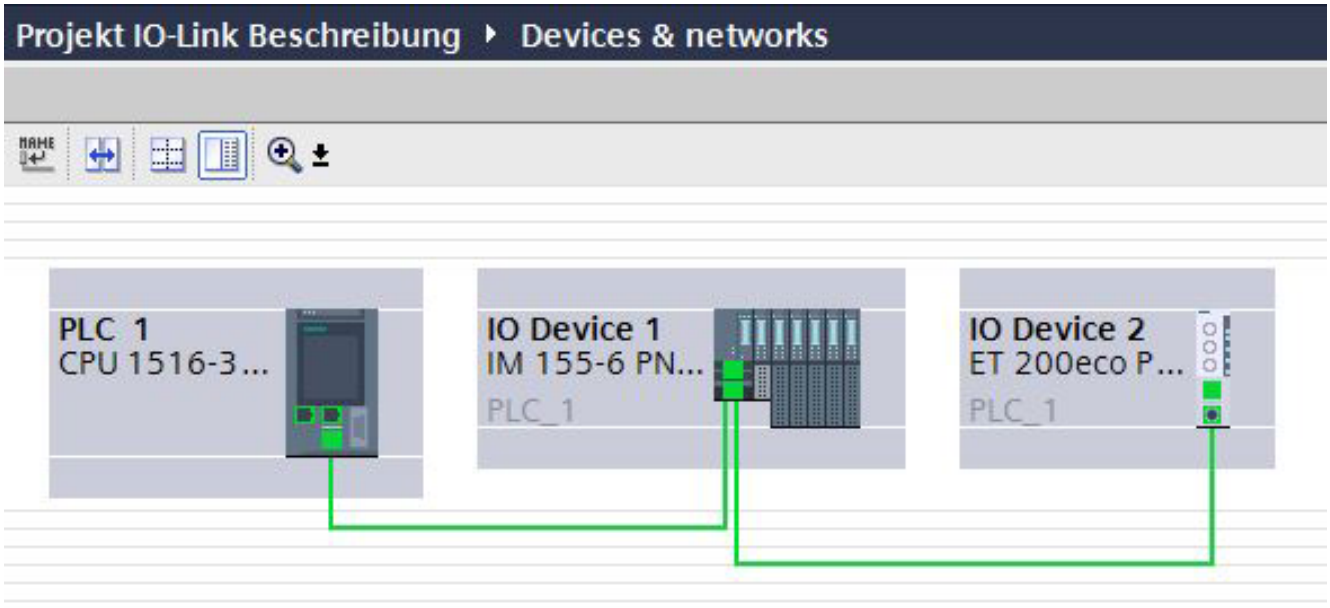


Figure 3-546 Configuration of a PROFINET network with lower-level IO-Link masters

In the device view of the PROFINET device, you can:

- Parameterize the ports
- Specify the input and output address ranges of IO-Link for exchange of cyclic data (process values).

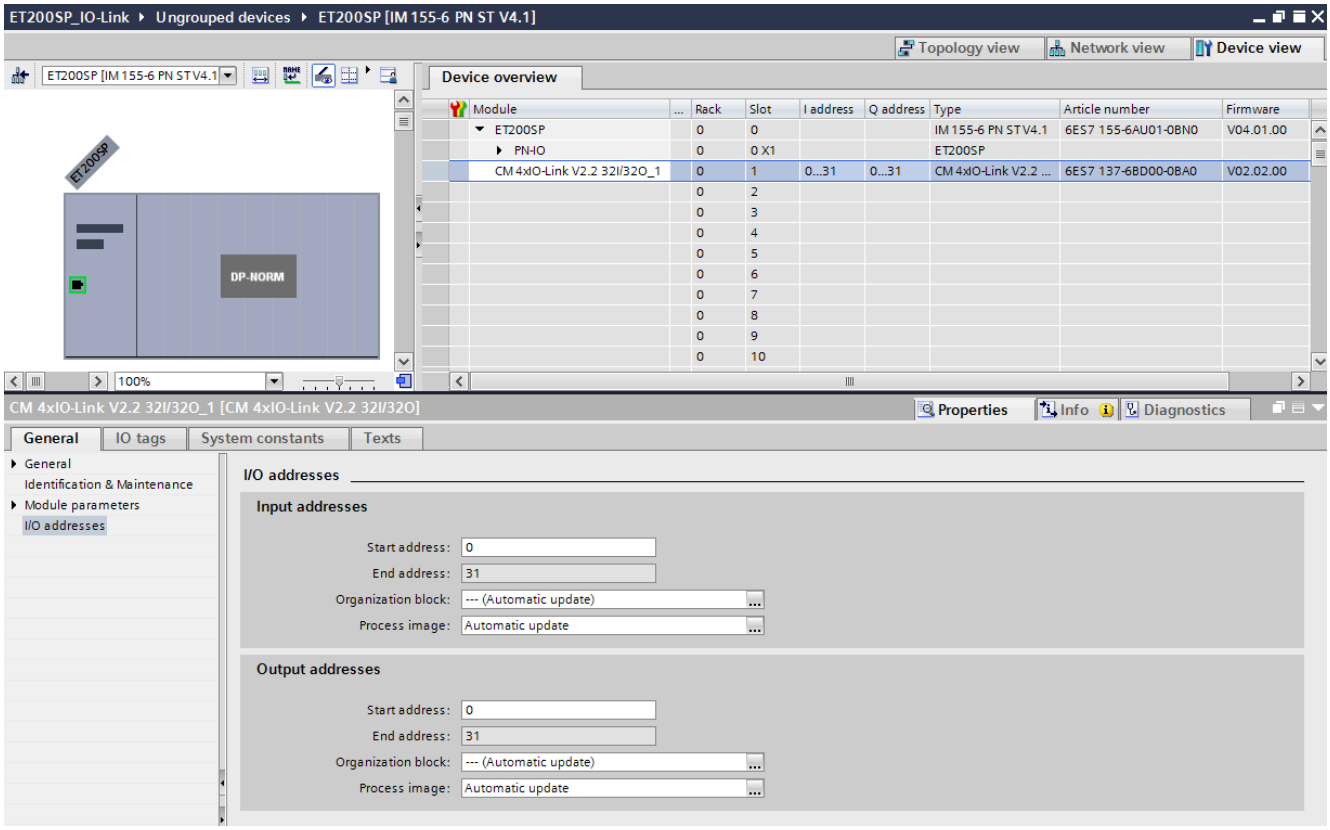


Figure 3-547 Device view with setting of the IO-Link address range

In addition, you can set in the module properties of the IO-Link master how the IO-Link system is to be configured and parameterized.
In doing so, you can select whether or not you also want to work with the S7-PCT configuration tool.

NOTE

IO data length

To ensure smooth operation, select an IO data length during configuration of the IO-Link master that corresponds at least to the IO data length of all connected IO-Link devices. If necessary, the IO-Link master offers the option of configuring the IO data length for each individual port. In this case, the IO data length must at least correspond to the IO data length of the connected IO-Link device.

2.1.1 Configuration with S7-PCT

Introduction

The following sections describe how you configure your IO-Link master with the S7-Port Configuration Tool (S7-PCT).

You need S7-PCT to display the system architecture completely and transparently all the way to the IO-Link device and to configure and parameterize the IO-Link system in detail.

With S7-PCT you can easily configure the IO-Link devices with the help of the IODD (IO-Link Device Description) supplied by the device manufacturer.
In the S7-PCT online view you can display the diagnostics states and process values of the IO-Link devices in detail.

Configuration with S7-PCT

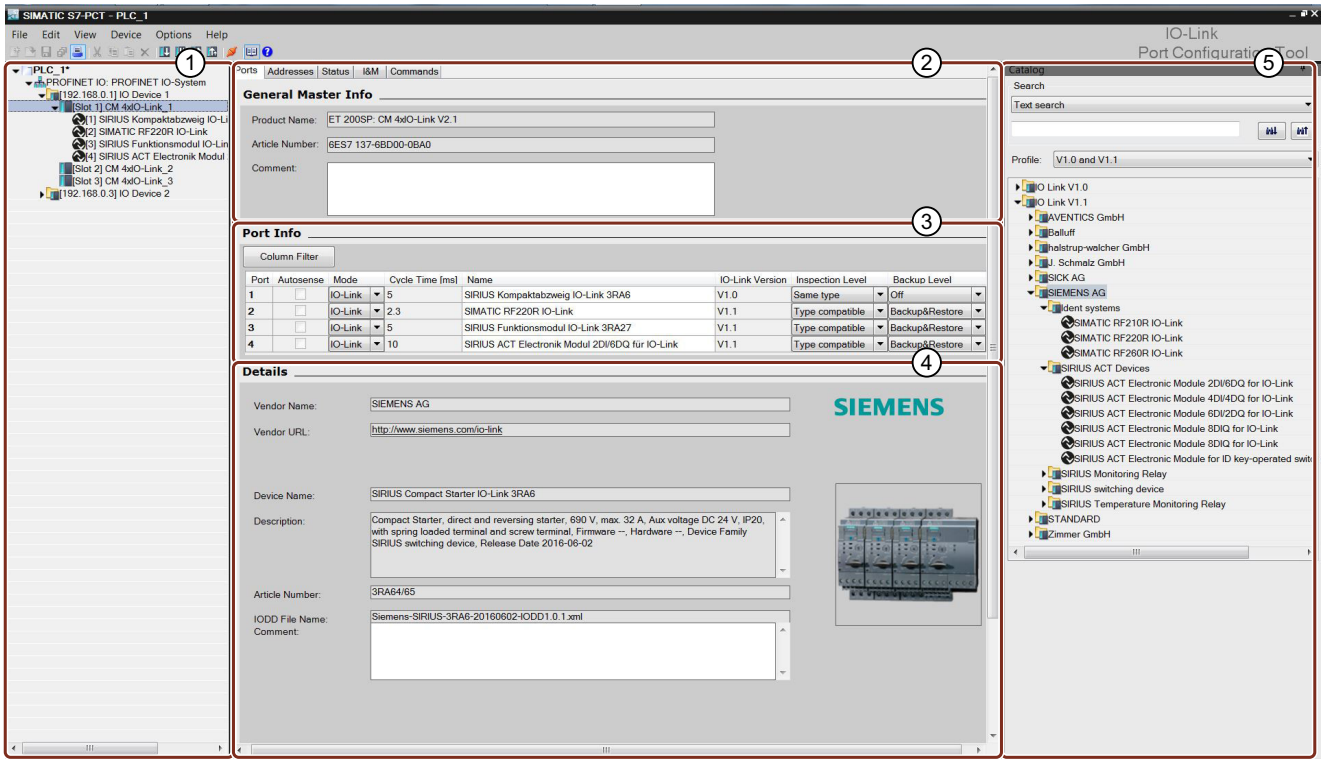
When you have selected the option "Configuration with S7-PCT", you are also making the settings of the IO-Link master ports with S7-PCT. See Figure 3-5 (Page 22).
These settings include:

- Specification of the address range for each port
- Behavior when replacing an IO-Link device
- Setting the identification data for checking the connected IO-Link device type

Start S7-PCT from HW Config in STEP 7.
S7-PCT shows you all Siemens IO-Link masters you have configured in your automation system.
After selecting an IO-Link master, you can assign its IO-Link ports to the desired IO-Link devices.
To do so, select the corresponding IO-Link devices (or their IODDs) from the device catalog and drag them to the port of the IO-Link master.

Example configuration in S7-PCT

The following figure shows the configuration of an IO-Link master in S7-PCT.
This S7-PCT view shows you a wide variety of information:



① Higher-level field bus and overview or structure of the lower-level IO-Link master
② Detailed information on the selected IO-Link master
③ Current configuration of the IO-Link ports of the selected IO-Link master
④ Detailed information on the selected IO-Link device
⑤ Device catalog with the IODDS of the IO-Link devices from different manufacturers

Figure 3-548 Configuration of an IO-Link master in S7-PCT

Address range of the ports

In addition to the assignment of the IO-Link devices to the IO-Link master ports, the default address ranges of the ports can be changed. The IO-Link master transfers the process values that it receives from the IO-Link device in these address ranges and makes the process values available to the higher-level automation system.

To set the address range, select the "Addresses" tab.

Setting device parameters

Specific parameter settings are required to adjust the device to the respective application task. The possible parameters and set values are contained in the IODD of each device. You set the device parameters directly in S7-PCT.

After selecting the corresponding device in the project tree (left tree), set the device parameters in the "Parameters" tab.

The figure below shows you an example of the parameter assignment of an IO-Link device:

Identification | Parameters | Monitoring | Diagnostics | Connection

Column Filter

Parameter	Value	Icon	Unit	Status	Help
Parameters					
Parameter Data					
System command					
Device Reset	Device Reset				
Restore Factory Setting	Restore Factory Setting				
Device access locks					
Parameter (write) Access	Locked			changed	
Data Storage	Unlocked				
Operating system functions					
index131 - Group diagnostics	enabled				enable/disable automatic signaling to PLC
index131 - Group error diagnostics	enabled				enable/disable automatic signaling of error messages to PLC
index131 - Local threshold change	enabled				enable/disable local threshold changing via buttons
index131 - Local parameter change	enabled				enable/disable local parameter changing via buttons
index131 - Local reset	enabled				enable/disable local reset via buttons
index131 - Retentive error memory	disabled				enable/disable remanent saving of error messages in the event of a power fa...
index131 - Analog value coding	Tmax [°C] (5)				choose the analog value trasmitted cyclically in the process image
Temperature monitoring					
index131 - Temperature monitoring mode	Range monitoring			changed	set the value of temperature monitoring mode
index131 - Temperature unit	°C				choose the temperature unit for display and monitoring (°C or °F)
index131 - ON-delay time (at Power ON)	enabled				enable/disable starting of delay time at Power-ON
index131 - ON-delay time (at manual reset)	enabled				enable/disable starting of delay time at manual reset of the device
index131 - ON-delay time	0.0		s		set the value of ON-delay time
index131 - Tripping delay time (if the temperat...	0.0		s		set the value of tripping delay time (temperature overshoot or undershoot)
index131 - Temperature sensor type	PT100				choose the type of the connected temperature sensor(s)
index131 - Hysteresis	3			changed	set the value of hysteresis for automatic reset after overshoot or undershoot
index131 - Relay switching response	Closed-circuit principle (NC)				choose the circuit principle of relay switching
Thresholds					
index131 - Threshold ϑ1	30			changed	set temperature threshold 1 for tripping (overshoot or undershoot depends o...
index131 - Threshold ϑ2	20			changed	set temperature threshold 2 for tripping (overshoot or undershoot depends o...
index131 - Warning threshold for ϑ1	28			changed	set temperature warning threshold 1 (overshoot or undershoot depends on ...
index131 - Warning threshold for ϑ2	22			changed	set temperature warning threshold 2 (overshoot or undershoot depends on ...

Figure 3-549 Setting the parameter values of the IO-Link device

Starting from the displayed defaults, you can edit and save the values in the defined value range.

The configuration of the IO-Link system and the parameters of the devices are available to the IO-Link system and the entire automation project. You have the option of saving and printing the configuration and the parameters.

It is not possible to change parameters in online mode.

2.1.2 Configuration without S7-PCT

Introduction

The following sections describe how you configure your IO-Link master without the S7-Port Configuration Tool (S7-PCT).

Your options for configuration of the IO-Link system without S7-PCT are limited.
You can configure the port of the IO-Link master using STEP 7 or the GSD file, but you cannot set any parameters of the lower-level IO-Link devices.

Configuration without S7-PCT

You can activate the following parameters in STEP 7 or the GSD file during port configuration:

- Port Qualifier Information (PQI):
  provides information on the status, such as process data of the IO-Link port; is transmitted with the input data of the IO-Link device.
- Operating mode
  - IO-Link Autostart:
    The IO-Link master accepts each connected IO-Link device and starts it automatically.
  - IO-Link Manual:
    The IO-Link master only accepts IO-Link devices that match the Vendor ID and Device ID set below.
    The connected IO-Link device is started automatically after a successful Vendor ID and Device ID check.
  - DI:
    The port is operating as a standard digital input.
  - DQ:
    The port is operating as a standard digital output.
  - Disabled:
    The port is disabled.
- Input Data Length:
  Process data length of the input data
- Output Data Length:
  Process data length of the output data
- Vendor ID
  ID number of the device manufacturer. You can find the Vendor ID on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).
- Device ID
  ID number of the device. You can find the Device ID on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109748852).
- The IODD - and thus Device and Vendor ID - can be loaded into the TIA project as a .zip file (as of TIAP V17)
- Inspection level for data backup:
  - Identical type (V1.0) without Backup&Restore
  - Type-compatible (V1.1) without Backup&Restore
  - Type-compatible (V1.1) with Backup&Restore
  - Type-compatible (V1.1) with Restore

The figure below shows you an example of the settings of a port configuration in STEP 7 or with GSD file:

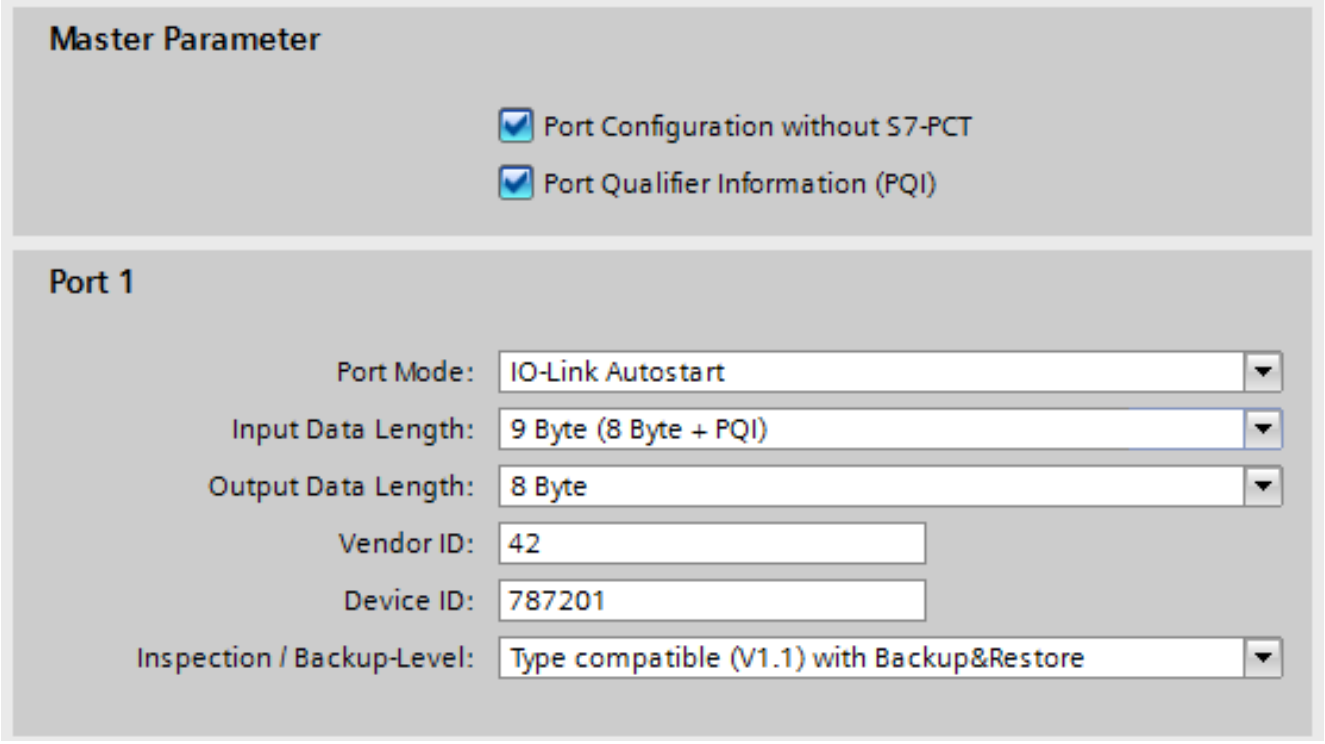


Figure 3-550 Settings of the port configuration in STEP 7 or with GSD file

2.1.3 Comparison of the configuration options

The following table provides an overview of the available options for configuration with and without S7-PCT:

Requirement	Configuration with S7-PCT	Configuration without S7-PCT	
		IO-Link Autostart	IO-Link Manual
Use of the IO-Link device description IODD	Yes	No	No
Setting the length of input and output data (per port)	Automatic	Manual	Manual
Assignment of the Vendor ID and Device ID	Automatic	-	Manual (see FAQ (https://support.industry.siemens.com/cs/ww/en/view/109748852))
Behavior during IO-Link device replacement	Programmable	-	Programmable
Adjustable IO-Link cycle time	Yes	No	No
Adjustable IO-Link device parameters	Yes	No	No

Requirement	Configuration with S7-PCT	Configuration without S7-PCT	
		IO-Link Autostart	IO-Link Manual
Display of the IO-Link process data structure	Yes	No	No
Monitoring of IO-Link process data	Yes	No	No
Display of IO-Link device diagnostics messages	Yes	No	No

2.2 Data access of the automation system and the HMI device

Cyclic data exchange

To exchange cyclic process data between an IO-Link device and a CPU, the IO-Link data is assigned by the IO-Link master to the previously set address ranges. The user program of the CPU accesses and processes the process values by using these addresses. The cyclic data from the CPU to the IO-Link device (for example, IO-Link actuator) takes place in reverse order.

Acyclic data exchange

Acyclic data, such as device parameters or events, is exchanged by means of a fixed index and subindex area. The CPU accesses the data using system mechanisms (for example, for online functions such as reading the status). You can use the index and subindex area to access specific device information (for example, to re-assign parameters of the device or master during operation).

Function blocks "LIOLink_Master" and "LIOLink_Device"

The programming of the CPU user program is another task in addition to the configuration and parameterization of the IO-Link system and its integration into the overall automation system.

For acyclic data exchange, you can use the function blocks "LIOLink_Master" and "LIOLink_Device" for controllers of the S7-300, S7-400, S7-1200 and S7-1500 product lines.

The function block "LIOLink_Master" reads all relevant functions and access to the IO-Link master, the function block "LIOLink_Device" reads all access to the IO-Link devices.
With the "LIOLink_Master" function block, you can save (Backup) and retrieve (Restore) the device parameters and settings of an IO-Link master via the S7 program (master replacement without engineering tool). A typical application is the replacement of the IO-Link master.

NOTE

Function blocks "LIOLink_Master" and "LIOLink_Device"
The function blocks "LIOLink_Master" and "LIOLink_Device" replace the functions of the previously available block "IOL_CALL".

Reference

The IO-Link block library with a description of the integration is available on the Internet (https://support.industry.siemens.com/cs/ww/en/view/82981502).
You can find an application example of using the block library with HMI devices on the Internet (https://support.industry.siemens.com/cs/ww/en/view/90529409).

2.3 Changing and saving device parameters during plant operation

Changing device parameters

You can adjust the device parameters during operation.
The changed parameters will become effective on the device in the process and are retentively saved in the device.
The parameters can be adapted during operation with:

- the engineering tool used (e.g. during plant commissioning)
- the CPU user program (program-controlled)
- HMI (through plant operator during batch change, process optimization)
- Locally through operation on the device (local operating unit on the device)

Saving device parameters (backup)

You can also automatically save the parameters set in the device during commissioning or changed during operation of the plant in the IO-Link master.
This data backup takes place depending on the set behavior of the IO-Link master ports.
You can set the following data backup levels:

- None
  No data backup in the IO-Link master.
- Backup&Restore
  Every time the device parameters are changed, the changed data is automatically saved in the IO-Link master (see section "Triggering a backup").
- Restore
  No automatic data backup in the IO-Link master.

IO-Link Version	Inspection Level	Backup Level
V1.0	No check	Off
V1.1	Type compatible	Backup&Restore
V1.1	Type compatible	Backup&Restore
V1.1	Type compatible	Backup&Restore

Figure 3-551 Overview of data backup level in S7-PCT

NOTE

IO-Link Specification V1.0
IO-Link master and devices to IO-Link specification V1.0 do not offer this function; a data backup cannot be set (Data backup: None).

Note that the behavior of the IO-Link master and the IO-Link devices during device replacement depends directly on the set data backup level.
You can find additional information on this dependency in the section Replacing a master or device during operation (Page 28).

NOTE

We strongly recommend resetting an IO-Link device to the factory settings before performing a restore by the IO-Link master. This prevents a permanently stored backup prompt of the device from accidentally overwriting the restore parameters.

Triggering a backup

Requirements

- You have set the correct data backup level.
- The IO-Link master and the IO-Link devices you are using support this function (IO-Link Specification V1.1).

Procedure

There are several ways to trigger a backup:

- In the engineering tool:
  After you have downloaded the engineering settings to the device, the IO-Link device immediately triggers a backup.
- In the CPU user program:
  IO-Link device parameters can be changed successively by the user program.
  A backup is only triggered by a system command. The system command must be triggered by the user program after the parameter changes.
  You can implement the parameter changes and the system command for triggering the backup with function blocks of the CPU.
- Using the HMI:
  You proceed as with triggering by the user program.
  The plant operator then triggers the necessary system command on the HMI device.
- Locally by operating the IO-Link device:
  After confirming the input on the IO-Link device, the IO-Link device initiates the backup.

2.4 Replacing a master or device during operation

Replacing a device

Replacing a device during operation is a scenario that occurs again and again and has to be completed without longer plant downtimes. Replace a device quickly and avoid incorrect settings. Devices can also be replaced by operators without special knowledge and aids.

When you use the backup function of the master, the master automatically supplies the saved parameters to the new device during device replacement.
You have the following setting options for device replacement:

- Backup&Restore
  You have set the master port to Backup&Restore. The new device behaves as the replaced device because the master has saved the last parameter change with the backup function.
- Restore
  You have set the master port to Restore. The new device applies the parameter settings that were saved in the master at the time of the last backup.
  If you have made parameter changes since the last backup, these are not saved in the master and are not available to the new device.
  The behavior of the new device can deviate from the behavior of the replaced device. This may be useful if you want to make short-term plant optimizations but do not want to save them in the plant backup.

NOTE

Field calibration of sensors
When you are using sensors that must be adapted to specific rated conditions on site (field calibration), you must repeat this calibration after replacing the device.
The backup does not include the data of the field calibration. After repeating the field calibration, the new device works just like the replaced device.

Replacing a master

Replacing a master during operation is a rather rare scenario. Here, too, longer plant downtimes are to be avoided. Replace a device quickly and avoid incorrect settings. Devices can also be replaced by operators without special knowledge and aids.

The "Toolchanger" function enables the deliberate replacement of devices without error messages (e.g. when replacing tools with IO-Link functionality).

You can save the configuration and parameter data of the master and the devices connected to the master in the CPU and download this information to the new master after the replacement.
When using an S7-CPU, you can use function blocks for this purpose.
You can find additional information on function blocks in the section Data access of the automation system and the HMI device (Page 25).

SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro, ET 200eco PN Analog value processing

Function Manual

Documentation guide 1

What you should know about analog technology 2

Representation of analog values 3

Connecting transducers 4

Thermocouples 5

Wiring loads/actuators 6

Supported functions 7

High-speed analog modules 8

06/2014
A5E03461439-AC

Preface

Purpose of the documentation

This documentation covers general topics applicable to all products.

In addition to introductory information about analog value processing, this manual covers the following topics:

- Wiring transducers to analog inputs
- Wiring actuators/loads to analog outputs
- Compensating for reference junction temperatures
- Calibrating analog modules
- Diagnostics options of an analog module
- High-speed analog modules

Basic knowledge required

The following knowledge is required in order to understand the documentation:

- General knowledge of automation technology
- Knowledge of analog value processing (analog technology)
- Knowledge of the industrial automation system SIMATIC
- Knowledge about how to use STEP 7 (TIA Portal)

Scope of the documentation

This manual is considered the basic documentation for all analog input and analog output modules of the S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro and ET 200eco PN product series.

Changes compared to previous version

Changes / enhancements described in this manual, compared to the previous version (version 12/2013):

- Extension of the scope of validity to the distributed I/O system ET 200AL

Conventions

STEP 7: In this documentation, "STEP 7" is used as a synonym for "STEP 7 as of V12 (TIA Portal)" and subsequent versions of the configuration and programming software. This documentation includes images of the products it describes. The products supplied may differ slightly from these images.

Please observe notes labeled as follows:

NOTE

Notes contain important information on a point in the documentation of particular importance.

Additional support

Additional information on SIMATIC products is available on the Internet. The associated documentation is also available on the Internet.

- The portfolio of technical documentation for SIMATIC products and systems can be accessed on the Internet (http://www.siemens.com/simatic-tech-doku-portal).
- The online catalog and the ordering system are available on the Internet (http://mall.automation.siemens.com).

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security on the Internet (http://www.siemens.com/industrialsecurity).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find more information on the Internet (http://support.automation.siemens.com).

Table of contents

1 Documentation guide 6

2 What you should know about analog technology 8

2.1 Overview 8
2.2 Precision/resolution 12
2.3 Scaling analog values 15
2.4 Unscaling analog values 17
2.5 Linearity errors 20
2.6 Repeat accuracy 20
2.7 Operational and basic error limits 21
2.8 Temperature error 23
2.9 Interference frequency suppression 24
2.10 Common mode interference (UCM) 25
2.11 Series mode interference (USM) 27
2.12 Interference voltage suppression 28
2.13 Crosstalk between channels 29
2.14 Diagnostics 31
2.15 Value status 39
2.16 Conversion time of an analog module 42
2.17 Cycle time of an analog module 43
2.18 Settling and response times of analog output modules 44
2.19 Smoothing 46
2.20 Burden with 2-wire transducers 48

3 Representation of analog values 51

3.1 Overview 51
3.2 Representation of input ranges 52
3.3 Representation of output ranges 53

4 Connecting transducers 55
4.1 Overview 55
4.2 Wiring analog inputs with MANA connection 56
4.3 Wiring analog inputs without MANA connection 57
4.4 Wiring voltage transducers 59
4.5 Wiring current transducers 59
4.6 Wiring thermal resistors and resistors 61
4.7 Wiring thermocouples 63

5 Thermocouples 65
5.1 Selecting thermocouples 65
5.2 Structure and operating principle of thermocouples 66
5.3 Compensation for the reference junction temperature 67
5.3.1 Overview 67
5.3.2 Compensation with internal reference junction 70
5.3.3 Compensation with reference channel of the module 71
5.3.4 Compensation, reference channel of Group 0 73
5.3.5 Compensation with fixed reference temperature 75
5.3.6 Compensation by means of dynamic reference temperature 77
5.3.7 "None" or external compensation 80
5.3.8 Compensation type RTD (0) 82

6 Wiring loads/actuators 85
6.1 Overview 85
6.2 Wiring loads/actuators 85

7 Supported functions 88
7.1 Calibrating analog modules 88
7.1.1 Overview 88
7.1.2 Calibrating analog modules 89
7.1.3 Canceling a calibration 92
7.1.4 Resetting analog modules to factory settings 92

8 High-speed analog modules 94
8.1 Basics 94
8.2 ST modules vs HS modules 99

Documentation guide

1

Introduction

The documentation of the SIMATIC products has a modular structure and covers diverse topics concerning your automation system.

The complete documentation for the S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro and ET 200eco PN systems consists of the respective system manuals, function manuals and product manuals.

Overview of additional documents related to analog value processing

The following table lists further references that supplement this description of analog value processing.

Table 3-79 References for analog value processing

Topic	Documentation	Most important contents
System description	System manual S7-1500 Automation System (http://support.automation.siemens.com/WW/view/en/59191792)	• Application planning • Installation • Connecting • Commissioning
	System manual ET 200SP distributed I/O system (http://support.automation.siemens.com/WW/view/en/58649293)	
	System Manual ET 200MP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/59193214)	
	System manual Distributed I/O System ET 200AL (http://support.automation.siemens.com/WW/view/en/89254965)	
	Operating instructions ET 200pro Distributed I/O System (http://support.automation.siemens.com/WW/view/en/21210852)	
	Operating instructions ET 200eco PN Distributed I/O System (http://support.automation.siemens.com/WW/view/en/29999018)	
Configuring interference-free controllers	Function manual Configuring Interference-Free Controllers (http://support.automation.siemens.com/WW/view/en/59193566)	• Basics • Electromagnetic compatibility • Lightning protection
Analog module	Product manual of the respective analog module	• Connecting • Parameters • Technical specifications • Parameter data record • Tables of analog values

SIMATIC manuals

All current manuals for SIMATIC products are available for download free of charge from the Internet (http://www.siemens.com/automation/service&support).

What you should know about analog technology 2

2.1 Overview

Introduction

This chapter is intended to familiarize you with the essential parameters of analog input modules and analog output modules based on the fundamentals of analog technology. The descriptions and examples provided on the following pages serve as a reference to the manuals for the respective analog module and are intended to facilitate the handling of these manuals.

Analog and binary signals

Binary signals can assume only 2 signal states: signal state 1 (voltage present) and signal state 0 (no voltage present). In control engineering, it is frequently necessary to read, process and output analog signals in addition to binary signals. In contrast to binary signals, analog signals take on any number of values within a specific range. Possible analog variables include:

- Temperature
- Pressure
- Speed
- Fill level
- pH value

Transducers

Controllers are only capable of processing analog values in the form of bit patterns. For this purpose, transducers which can be connected to the analog module measure physical variables such as pressure or temperature. The analog input module reads this analog value in the form of current, voltage or resistance. To enable the CPU to process the current or voltage measured, an integrated analog-to-digital converter in the analog input module converts the value into a 16-bit integer value. Depending on the type of measurement, you can use the following transducers:

- Voltage transducers
- Current transducers
  - 2-wire transducers
  - 4-wire transducers
- Resistance transducers
  - 4-wire connection
  - 3-wire connection
  - 2-wire connection
- Thermocouples

Additional information on wiring various types of transducers to analog inputs can be found in Wiring transducers (Page 55).

Example
Speed is acquired using a transducer which converts the speed range of 0 to 1500 rpm to a voltage range of 1 to 5 V. At a measured speed of 865 rpm, the transducer outputs a value of 3.3 V.

The resulting voltage value is calculated as follows:

$$U = \frac{5\ V - 1\ V}{1500\ \frac{U}{min}} * 865\ \frac{U}{min} + 1\ V = 3.3\ V$$

The graph below illustrates voltage acquisition:

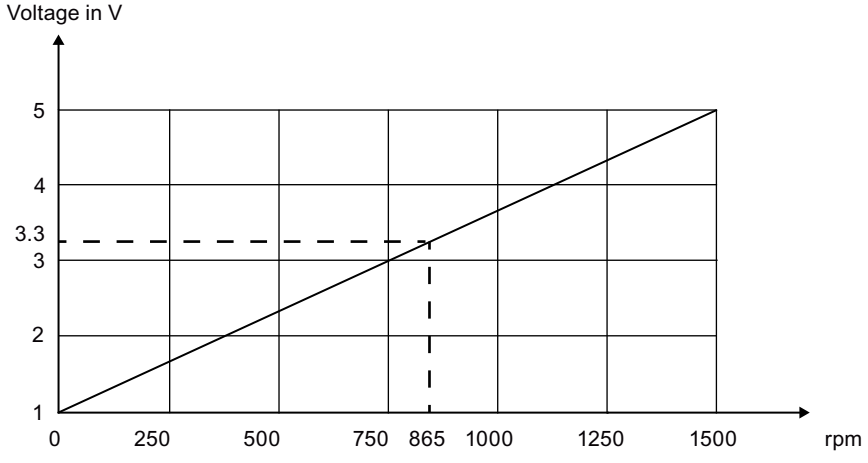
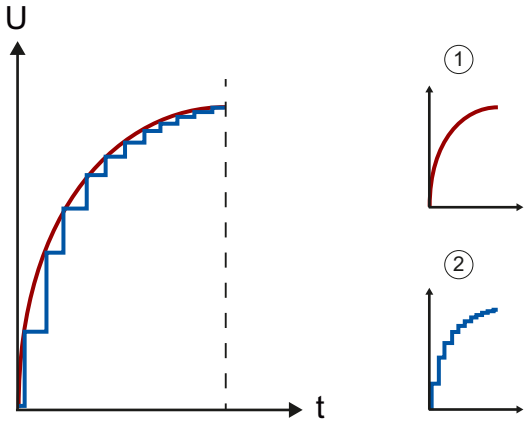


Figure 3-552 Speed measurement

Analog-to-digital conversion

A CPU processes information exclusively in digital format. The analog value is therefore converted into a bit pattern. Conversion is done using an integrated ADC (analog-to-digital converter) in the analog input module. For the CPU, this conversion always returns a 16-bit word for SIMATIC products. The ADC used digitalizes the analog signal and approximates its value with a stepped curve. Resolution and conversion speed are the most important ADC parameters.



① Analog value
② Digital value

Figure 3-553 Approximation of an analog graph with low- and high-resolution stepped curves

Digital-to-analog conversion

Once the CPU has processed the digital signal, an integrated DAC (digital-to-analog converter) in the analog output module converts the output signal to an analog current or voltage value. The resulting value of the output signal corresponds to the output value used to control the analog actuators. Such actuators include, for example, small servo drives or proportional valves. You will find more information on wiring actuators in Wiring loads/actuators (Page 85).

Important parameters of analog modules

Alongside the type and range of measurement, the precision, resolution and conversion time are the main points to consider when selecting an analog module. For some applications such as systems which cover a large area, common mode or channel isolation are also important. The parameters listed here are examined in more detail in the following pages.

Processing analog signals

The following figure demonstrates analog signal processing in a PLC.

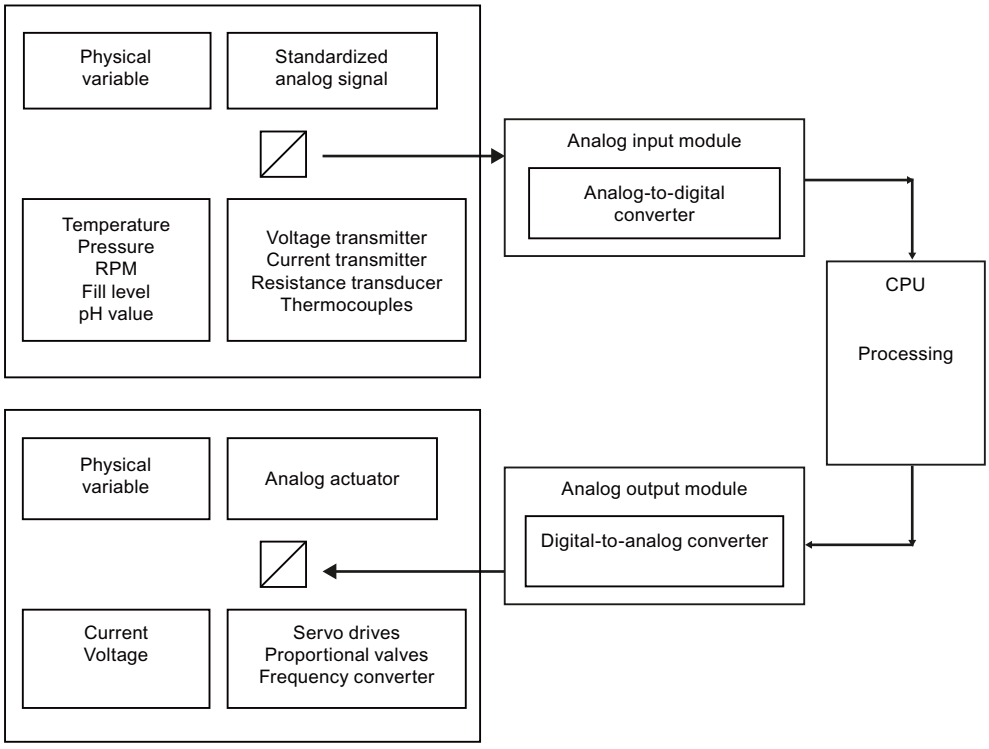


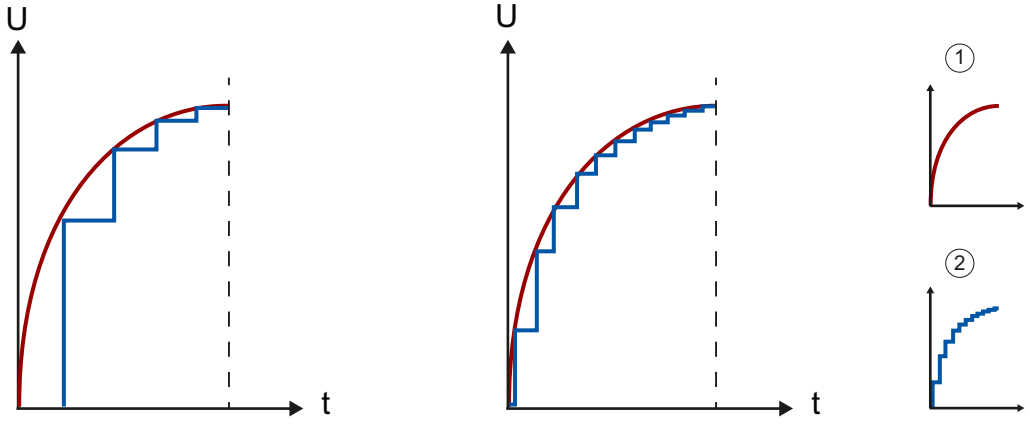
Figure 3-554 Analog value processing

2.2 Precision/resolution

The resolution of an analog module depends on the converter and its external circuitry. An approximation of the analog signal to be acquired/output is returned by a stepped curve. The resolution determines the number of increments of the analog value along this stepped curve. A higher module resolution reduces the length of increments and adds precision to the digitization of the analog signal.

Approximation of an analog value

The figures below show the approximation of an analog value by means of a stepped curve. A low resolution only returns a rough approximation of the actual curve (left figure), while the approximation is more precise at higher resolutions (right figure).



① Analog value
② Digital value

Figure 3-555 Approximation of an analog curve with a stepped curve

Visualization of the measuring range at a resolution of 13 bits and 16 bits

The unipolar measured value from a module having a resolution of 13 bits (= 12 bits + S) is segmented into a total of 2^{12} = 4096 increments. The smallest increment in a measuring range of 0 to10 V is 10 V/4096, equal to 2.4 mV.

A module with16-bit (= 15 bits + S) resolution thus provides an increment of 0.3 mV. If the resolution increases by one bit, the number of increments doubles and the width of an increment halves.

If the resolution increases from 13 bits to 16 bits, the number of increments increases eightfold from 4096 to 32768. With a resolution of 13 bits, the smallest value that can be displayed is therefore 2.4 mV. By contrast, this value is approximately 0.3 mV at a resolution of 16 bits.

Measuring ranges

For the display of the measuring range, SIMATIC S7 distinguishes between the rated range, the overrange and underrange, and the overflow or underflow. This distinction allows you to recognize whether the measured value is actually in the measuring range determined in the technical specifications. The overflow and underflow ranges are reserved for error detection.

At a resolution of 16 bits the theoretically possible 32768 increments are distributed across a voltage range of 11.852 V, which means that only 27648 increments are actually available for the resolution of a measuring range of 10 V. The minimum value which can be represented is therefore 0.3617 mV (see table).

Table 3-80 Example of resolution for the 0 to 10 V measuring range of a SIMATIC S7 module

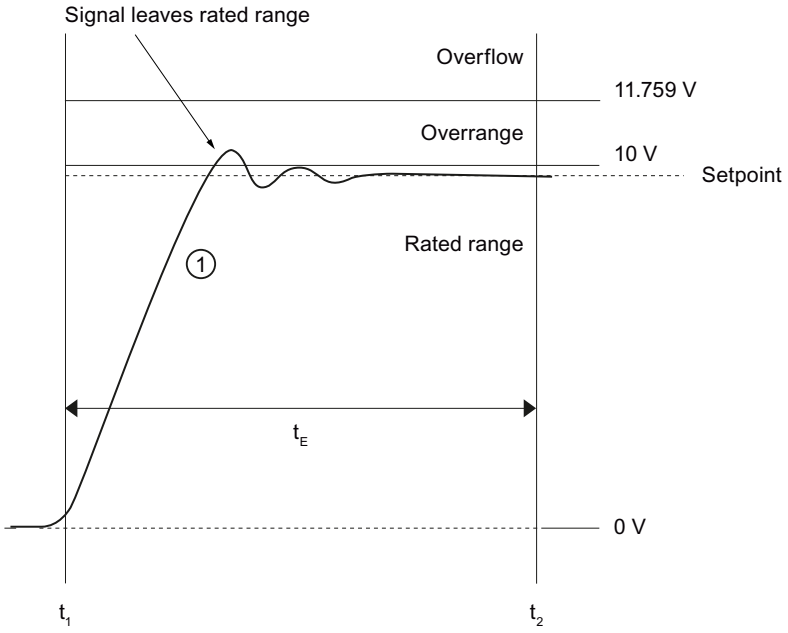
Value (increments)	**Voltage measuring range**	
Decimal	**0 to 10 V**	**Range**
32767	11.852 V	Overflow
32512		
32511	11.759 V	Overrange
27649		
27648	10.0 V	Rated range
20736	7.5 V	
1	361.7 µV	
0	0 V	
not relevant for this example as negative values are not possible		Underrange
		Underflow

The digitized visualization of the input ranges, separated into bipolar and unipolar input ranges, is shown in the section Visualization of the input ranges (Page 52). The digitized visualization of the output ranges, separated into bipolar and unipolar output ranges, is shown in the section Visualization of the output ranges (Page 53). You will find a summary of all measuring ranges which you can use with your analog module in the corresponding device manual.

Over and underrange

It may happen for control processes with high signal jumps that the settling curve of the signal briefly leaves the rated range until it reaches the setpoint. The over and underrange ensures that no error is reported while the signal is not in the rated range. If the signal exceeds the over or underrange, however, and reaches the overflow or underflow range, the error state "Overflow" or "Underflow" is diagnosed. This means the over or underrange correspond to a tolerance range between the rated range and the overflow or underflow. Additional information on the settling time is available in the section Settling and response times of analog output modules (Page 44).

The figure below shows the rated range, the overrange and overflow of a unipolar measuring range. The signal leaves the rated range briefly during the settling phase.



① Analog output signal
t_E Settling time of the signal to the setpoint
t_1 Module ends conversion at the terminal of the analog output channel and outputs the signal
t_2 Signal has settled and the specified analog output value has been reached

Analog module precision

The precision of an analog module is specified as a percentage value or absolute value, for example, in K or °C. This characterizes the total error of measured value acquisition. The basic error limit at 25 °C, as well as the operational limit, are specified in accordance with international standard IEC 61131, which also forms the basis for European Standard EN 61131. For more information on the operational/basic error limits, refer to the Operational and basic error limits (Page 21) section.

Relation between resolution and precision

A certain resolution must be given to reach a specific precision (operational error).

Example

Measuring error as a result of digitization at a resolution of 8 bits and 14 bits
An analog module has a measuring range of 0 V to 10 V. A resolution of 8 bits represents a total of 256 values. This is equivalent to a minimum possible voltage step of 39 mV or 0.4% of the measuring range end value. A resolution of 14 bits represents a total of 16384 values. This is equivalent to a minimum possible voltage step of 0.61 mV or 0.006% of the measuring range end value.

The percentages derived in this way also represent the theoretical best-case values for the operational limit. With a resolution of 8 bits and a measuring range of 0 to 10 V, it is therefore impossible to achieve a precision of more than 0.4 %. In practical life, this value would be clearly worse, depending on the implemented circuitry.

Calculating the maximum measuring error

The maximum measuring error of a 0 to 10 V analog module with an operational limit of ±0.5 % across the entire temperature range is calculated as follows:

10 V x 0.5/100 = 50 mV

This means the maximum measuring error is approximately ±50 mV. This also means that each analog voltage input is subject to a distortion of ±50 mV across the entire input range. A voltage of 3.5 V that is to be measured can therefore be visualized by any value between 3.45 V and 3.55 V.

For more information on the operational/basic error limits, refer to the Operational and basic error limits (Page 21) section.

2.3 Scaling analog values

Scaling

It is often necessary to calculate the actual process value rather than increments (e.g., 10 V = 27648 increments) for further processing of digitalized analog values. The conversion of a value range (e.g., -27648 to +27648 increments) to the original physical quantity (e.g., 0 to 500 liters) is referred to as scaling.

Scaling blocks

STEP 7 offers the suitable program block for scaling of analog values. The SCALE block is included in the STEP 7 scope of delivery and permits input of a high and low limit (e.g., 0 to 500 liters).

Example

In the example below the fill level of a tank with a capacity of 500 liters is to be measured. The transducer used measures a voltage of -10 V with an empty tank and a voltage of +10 V with a full tank. The analog module converts the voltage range from -10 V to +10 V into the value range -27648 to +27648 and converts this range into the original quantity of 0 to 500 liters with the SCALE program block.

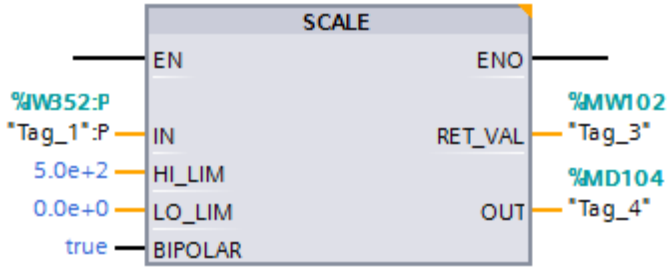


Figure 3-556 Scaling in the SCALE program block

The analog value at input **IN** is read directly by the module or is transferred by a data interface in INT format. The input **LO_LIM** is used to determine the low limit (0 liters) and **HI_LIM** to determine the high limit (500 liters) of the physical quantity. The output **OUT** outputs the scaled value (physical quantity) as floating-point number (LO_LIM <= OUT <= HI_LIM). You can assign parameters via the input **BIPOLAR** to specify if only positive or only negative values are to be converted. If the parameter receives an operand with the state '0', there is a unipolar scaling. An operand with the state '1' results in a bipolar scaling. The output **RET_VAL** outputs an error code in case of an error (e.g., overflow) and the value '0' in case of an error-free execution.

Additional information on the SCALE block can be found in the STEP 7 online help.

Unipolar and bipolar measuring ranges

The measurement of the fill level in our example took place within a bipolar measuring range. In addition to the positive voltage the transducer also provides negative voltage. Because the tank volume is mapped to the range from -27648 to +27648 increments, the measurement of the fill level takes place with twice the resolution (Δ) as in the unipolar measuring range.

NOTE

Transducers

The prerequisite for a measurement within a bipolar measuring range is that the used transducer supports bipolar measuring ranges.

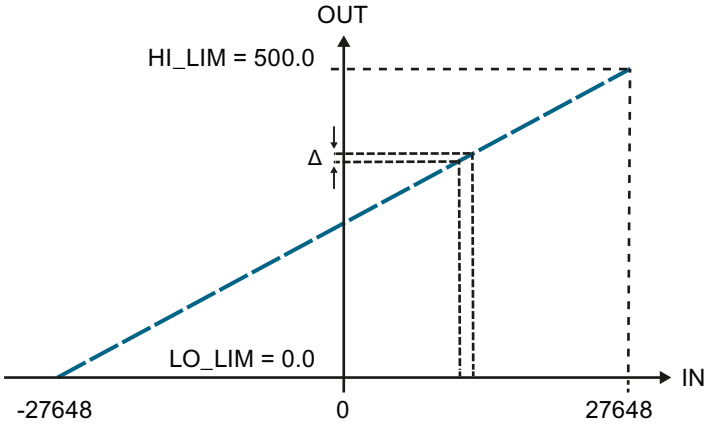


Figure 3-557 Bipolar measuring range

The measurement of the fill level in the bipolar measuring range takes place with twice the resolution (Δ) as in the unipolar measuring range.

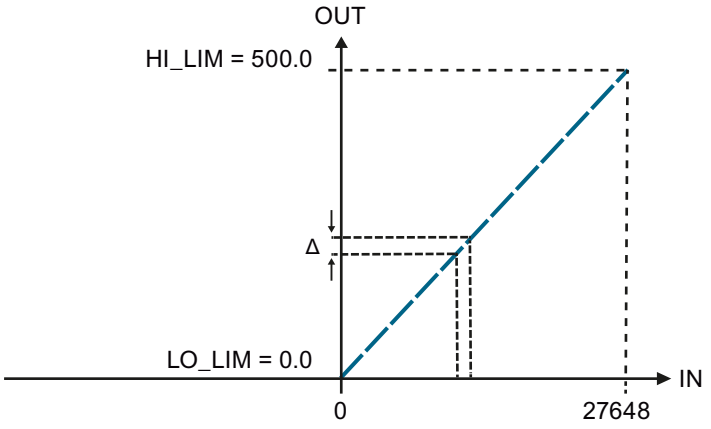


Figure 3-558 Unipolar measuring range

2.4 Unscaling analog values

Unscaling

The output of scaled analog values often requires conversion of the analog value calculated by the user program into the value range of the analog output module. This conversion is referred to as unscaling.

Unscaling blocks

STEP 7 offers the suitable program block for unscaling of analog values. The UNSCALE block is included in the STEP 7 scope of delivery and permits the input of a high and low limit that defines the range of the program value.

Example

An analog value from 0.0 to 100.0% calculated by the user program is to be converted with the UNSCALE block to the value range -27648 to +27648. When the unscaled value is output to an analog output module, this module addresses an analog actuator (e.g., modulating valve). The actuator is to be addressed at a program value of 0% with the minimum value (-10 V or -20 mA) and at 100% with the maximum value (+10 V or +20 mA).

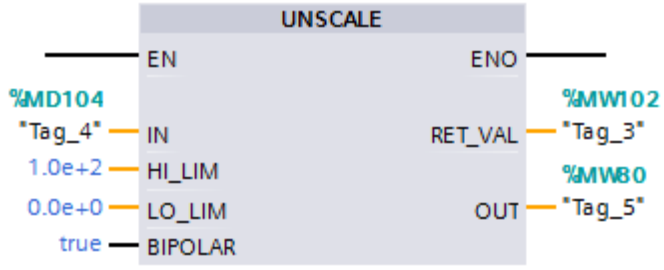


Figure 3-559 Unscaling in the UNSCALE program block

The value calculated by the program must be transferred in the REAL format (**IN**). You use the input **LO_LIM** to determine the low limit (0.0%), and **HI_LIM** to determine the high limit (100.0%) within which the program value moves. The unscaled value is output in INT format at the **OUT** output. You can assign parameters via the input **BIPOLAR** to specify if only positive or only negative values are to be converted. If the parameter receives an operand with the state '0', there is a unipolar scaling. An operand with the state '1' results in a bipolar scaling. The output **RET_VAL** outputs an error code in case of an error and the value '0' in case of an error-free execution.

Additional information on the UNSCALE block can be found in the STEP 7 online help.

Unipolar and bipolar measuring ranges

The figure below shows the scaling for an actuator that is to be addressed at a program value of 0% with the minimum value 0 (0 V or 0 mA) and at 100% (+27648) with the maximum value (10 V or 20 mA).

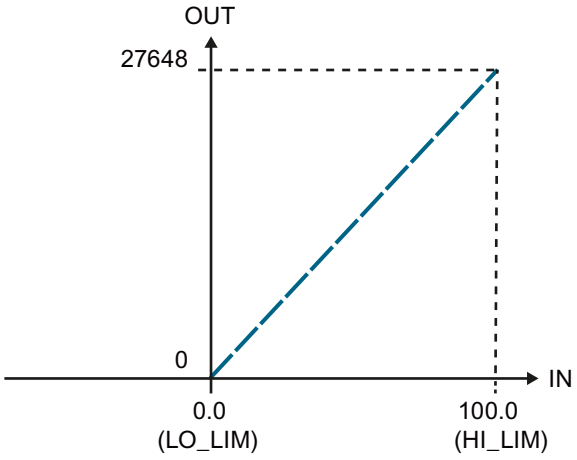


Figure 3-560 Unipolar measuring range

The figure below shows the scaling for an actuator that is to be addressed at a program value of 0% (-27648) with the minimum value 0 (-10 V or -20 mA) and at 100% (+27648) with the maximum value (+10 V or +20 mA).

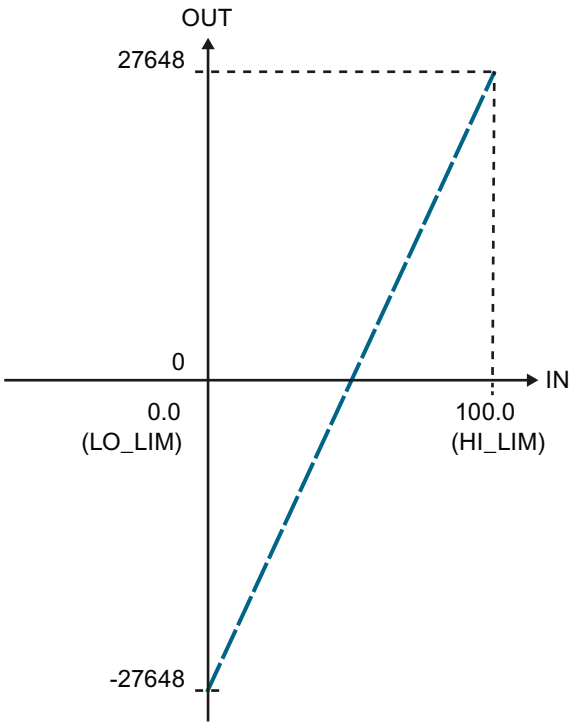


Figure 3-561 Bipolar measuring range

2.5 Linearity errors

Definition

Linearity denotes the deviation of the actual A/D or D/A conversion from the ideal lines within a specified measuring range. The linearity error therefore represents the deviation of the real transmission function from the ideal straight line. The error is given in the technical data as a percentage of the rated range of the analog module.

The figure below shows the linearity error of an ADC, magnified for better visibility.

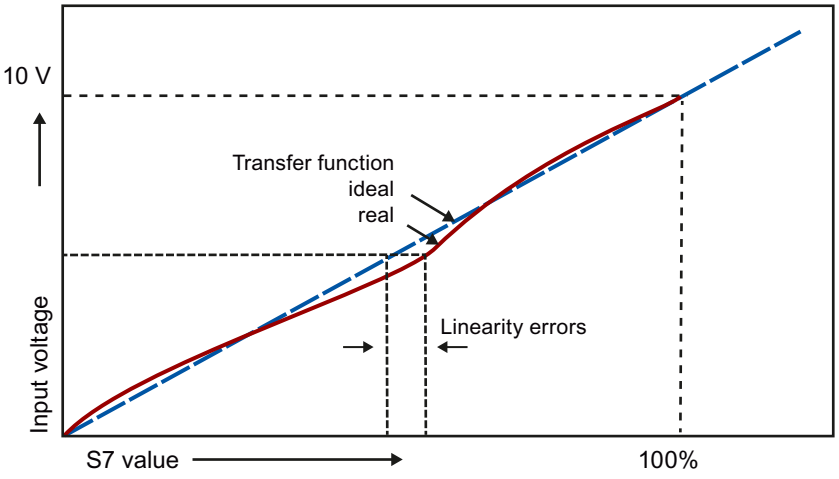


Figure 3-562 Linearity errors

Example

An error of ±1 mV is returned at an input range of ±10 V and a linearity error of ±0.01%. The error is calculated as follows: 10 V · 0.01 % = 1 mV

The linearity error information given in the technical specifications is taken into account in the operational limit. You will find a detailed description of the operational limit in Operational and basic error limits (Page 21).

2.6 Repeat accuracy

Definition

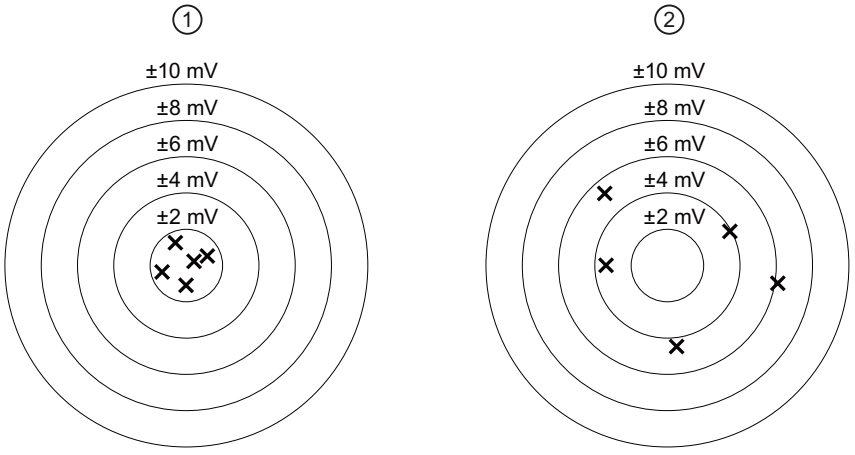
The repeat accuracy is the maximum deviation in measured/output value for the same input signal or output value after another value has been created or output. Other parameters, e.g. the Temperature parameter, remain unchanged. The repeat accuracy refers to the rated range of the module and applies in a steady temperature state.

Measured value variance

The repeat accuracy provides information on the variance of individual measurements. The smaller the variance, the greater the repeat accuracy. The repeat accuracy is therefore one of the most important properties of measuring devices. In the technical data, the repeat accuracy is given as a percentage of the input or output range at 25°C in the steady state.

Example

The specified repeat accuracy for an analog input module as a percentage of the measuring range end value is ±0.02 %. This corresponds to a repeat accuracy of 2 mV for any value within the measuring range of ±10 V. If you change the measured value from 10 V to -10 V, for example, and then measure with 10 V again, the measured value deviation may not exceed ±2 mV.



① Good repeat accuracy
② Poor repeat accuracy

Figure 3-563 Repeat accuracy of measured values output

2.7 Operational and basic error limits

Introduction

The following section shows you how to determine the operational or basic error limits and thus the measurement error or output error with the help of the technical specification. The worst-case configuration ensures that the module will not exceed the specified value within the valid operational range.

The precision of analog input or output modules is only part of the precision of the entire measurement section. A measurement section usually consists of transducer, transmitter, transmission line as well as input / output module.

Operational limit

The operational limit is the entire measurement or output error rate of the analog module in the rated range in temperature-settled state within the approved temperature range.

Basic error limit

The basic error limit is the entire measurement or output error rate in the rated range at an ambient temperature of 25 °C and temperature-settled state.

The basic error limit of the module is more or less a theoretical value, because a constant ambient temperature of 25 °C is rarely maintained in plants. For this reason, the operational limit always takes priority in terms of the practical selection and assessment of a module.

NOTE

The operational limit and basic error limit percentages listed in the technical specifications always relate to the **maximum possible** I/O value (the measuring range end value) in the rated range of the module.

The following image shows an example of operational and basic error limits in comparison with the ideal curve.

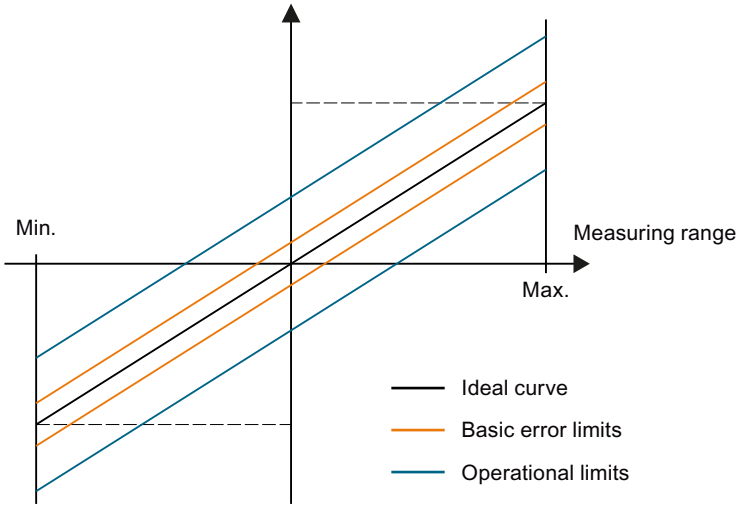


Figure 3-564 Operational and basic error limits

Example of output error calculation

An analog output module is used for voltage output in a range of 0 to 10 V. The module is operating at an ambient temperature of 30 °C, which means that the operational limit applies. Technical specifications of the module:

- Operational limit for the voltage output: ±0.1 %

The result is an output error of approximately ±10 mV (±0.1 % of 10 V) across the rated range of the module.

For example, the output value may range from 2.49 V to 2.51 V at an actual voltage of 2.50 V.

NOTE

Bipolar measuring ranges

The calculation also applies to bipolar measuring ranges.

An error of ±10 mV is also returned at an input range of ±10 V and a linearity error of ±0.1%.

2.8 Temperature error

Introduction

Analog modules are exposed to operational conditions that have an impact on their precision and on the measurement results they return. Temperature errors develop, for example, if the operating temperature of the module deviates from the ambient temperature of 25 °C. These temperature errors within the approved temperature range are taken into account in the operational limit.

Definition

The temperature error identifies the maximum drift of measuring/output values caused by fluctuation of the ambient temperature at the analog module. The maximum drift can occur at any ambient temperature. The temperature error is specified depending on the module used in percent per degree Celsius and/or percent per Kelvin, e.g. ±0.005%/K, and relates to the measuring range end value of the analog module.

Operational limits of compensation

The temperature error of the reference junction temperature compensation function only occurs with thermocouple measurements. The temperature error of compensation is added to the actual temperature error if "Internal reference junction" operating mode is selected. The temperature error of compensation is defined in the technical specifications as a percentage of the physical rated range of the analog module or as an absolute value in °C.

NOTE

Calculating the error in thermocouple measurements

Add the error of a thermocouple measurement to the error of the compensation measurement to determine the total error of a thermocouple measurement. These errors are defined in the respective manual.

Example

In this example, the total error of the temperature measurement is determined with the help of a type K thermocouple. The type K thermocouple takes measurements at a temperature range from -270 °C to +1372 °C.

The technical specifications state an operational limit of >-200 °C ±2.4 K for the type K thermocouple. The temperature error of compensation amounts to ±6 °C. The total temperature error is measured as follows at a temperature of >-200 °C:

Operational error (±2.4 K) + temperature error of compensation (±6 °C) = ±8.4 °C.

2.9 Interference frequency suppression

Definition

The interference frequency suppression function is applied to analog input modules to suppress the noise caused by the frequency of the AC voltage supply used.

The frequency of the AC voltage supply is likely to have a negative effect particularly on the values returned by measurements in the low voltage range and on thermocouples.

Parameter assignment

The line frequency at which the system is operated can be set by means of module parameters, for example, in STEP 7.

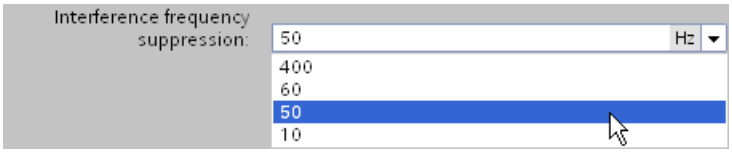


Figure 3-565 Interference frequency suppression

The conversion time changes depending on the set interference frequency suppression. The data sheets of the respective module define this dependency.

Please note the following when selecting interference frequency suppression:

The higher the frequency setting, the shorter the conversion time.

NOTE

Line frequency

Always select the interference frequency based on the line frequency used. Mismatch errors must be expected if a frequency that deviates from this line frequency is set, for example, to reduce the conversion time. In this case, the specified technical data and, in particular, precision are possibly outside the specified range.

Smoothing

By smoothing analog values, you achieve an additional improvement for the suppression of interference frequencies. For more information on the smoothing of analog values, refer to the section Smoothing (Page 46).

Line frequencies used

The line frequency is the frequency used in an electricity network for AC supply. It is measured in hertz and indicates the number of oscillations per second in a periodic signal. A line frequency of 50 Hz, for example, means 50 oscillations per second.

Europe, Australia and most countries in Asia and Africa use a line frequency of 50 Hz. North and Central America and most countries in South America have electricity networks with a line frequency of 60 Hz.

Frequencies of 400 Hz are most commonly used in on-board networks for airplanes, in the aerospace sector and for military applications. One reason for this is that engines with a line frequency of 400 Hz can usually be made smaller and lighter. As, however, it is not economic to transport such high frequencies over large distances, 400 Hz applications are usually subject to significant spatial limits.

A frequency of 16 2/3 Hz is used for the traction power supply in Germany, Austria and Switzerland. Some modules of the SIMATIC S7 product range also support the interference frequency suppression of this line frequency. The configurable interference frequency suppression in these cases is 16.6 Hz.

2.10 Common mode interference (UCM)

Definition

Common mode interference denotes interference voltages and currents in the lines connecting electrical devices and system components. They affect both the positive and negative line with the same phase angle and amplitude. The interference signal needs an additional current path to affect the utility signal. This current path is usually provided by common reference potential, e.g. earth or ground connection, of the utility signal and interference source.

Common mode interference in analog modules

Common mode interference occurs in analog input and output modules if their reference potential is different from the reference potential of the connected sensor or actuator.

Common mode interference is most likely to occur when analog modules are operated with grounded sensors. The size of the overall system means that voltage differences may develop between machine components with grounded sensors and the analog module reference. These voltage differences affect both the positive and negative signal path equally, which is why they are termed common mode interference.

In operation with non-grounded sensors, the occurrence of common mode interference is not as obvious as in grounded operation. Nevertheless, capacitive or inductive coupling can also create voltage differences in such cases which have the effect of common mode interference. Depending on the conditions in grounded and non-grounded operation, common mode voltage can occur as direct or as alternating voltage.

Example

The following figure of an analog module with two inputs (Ch_1/Ch_2) shows the coupled interference voltages at the inputs (U_{CM1}/U_{CM2}) as well as an interference voltage coupled between these inputs (U_{CM3}). Common mode rejection indicates the extent to which these interference signals can be suppressed. It is calculated using the following equation:
CMR [dB] = 20 · log (U_{CM} / U_a)

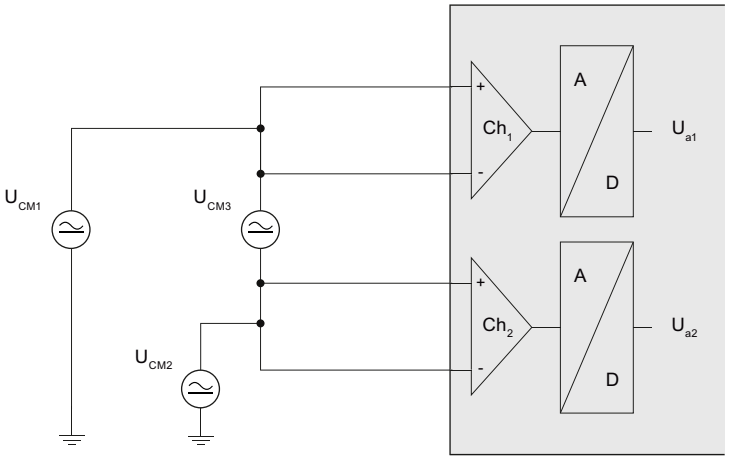


Figure 3-566 Common mode voltage coupled between two inputs

If there is common-mode voltage (U_{CM}), the equation is solved for U_a to calculate the measuring error (U_a):

$$U_a = U_{CM} * 10^{-\frac{CMR}{20}}$$

NOTE

The common mode rejection (CMR) is detailed in "Common mode interference" in the technical data of the device manual for your analog module.

2.11 Series mode interference (USM)

Definition

Series mode interference is interference voltages and currents affecting the connection lines in opposite directions. They have opposite polarity in the positive and negative directions. Series mode interference currents cause a voltage drop at the input impedance that has the effect of an interference voltage.

Causes

Series mode interference is caused by capacitive or inductive coupling. Inductive coupling generates a magnetic flow that is radiated between adjacent current-carrying conductors. This induces an interference voltage in the conductor. Galvanic coupling is given where different circuits influence each other due to common conductor sections, e.g. common ground connection.

The diagram below shows series mode interference as a voltage source (U_{SM}) connected in series to the actual measuring signal (U_M). The index "SM" stands for "Series Mode". Series Mode rejection indicates the extent to which these interference signals are suppressed. It is calculated using the following equation: SMR [dB] = 20 · log (U_{SM} / U_a)

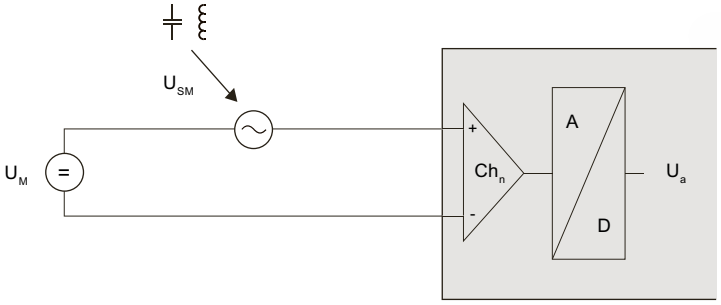


Figure 3-567 Capacitive or inductive interference coupling to the signal cable

The voltage (U_a) measurement error is calculated by solving the equation for U_a.

$$U_a = U_{SM} * 10^{-\frac{SMR}{20}}$$

The following equation shows the calculation of current (I_a) measuring errors using a current input.

$$I_a = \frac{U_{SM}}{R_{ein}} * 10^{-\frac{SMR}{20}}$$

NOTE

The series mode rejection (SMR) is detailed in "Series mode interference" in the technical data of the device manual for your analog module. The level of input resistance (R_{ein}) is also specified in the technical data.

2.12 Interference voltage suppression

Definition

Interference voltage suppression gives the factor by which the interference signal is suppressed in measurement value acquisition. Higher values reduce the effect of interference on the measurement signal. The technical data differentiates between "Common mode interference" and "Series mode interference". Interference voltage suppression is specified in decibels.

Example

The diagram below shows the measuring error for interference voltages in volts and interference voltage suppression of 0 to 120 dB.

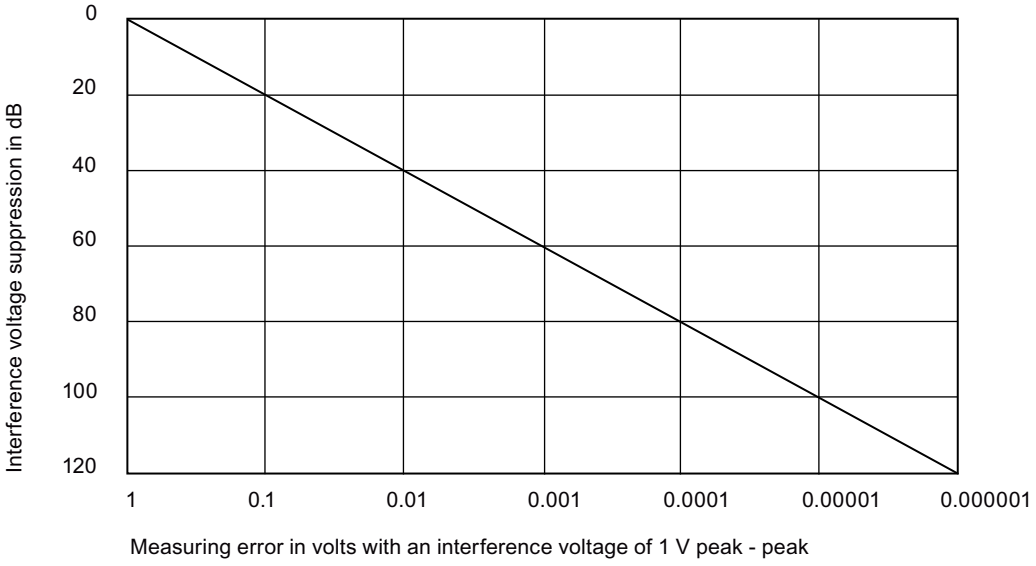


Figure 3-568 Interference voltage suppression

With an interference voltage suppression of 40 dB and an interference voltage of 1 V, the measured value is only distorted by 0.01 V.

NOTE

Interference-free design

Disturbance variables can be substantially reduced by means of appropriate grounding and shielding to increase interference immunity of the configuration. You will find a detailed description of how to avoid interference in the Configuring interference-free controllers (http://support.automation.siemens.com/WW/view/en/59193566) function manual.

Common mode rejection

The table below sets out the possible common mode rejection specifications in the technical data of an analog input module:

Interference voltage suppression for f = n x (f1 ± 1 %), (f1 = interference frequency), n = 1, 2, ...	
Common mode interference	> 100 dB
Common mode voltage, max.	10 V

If the interference frequency is configured as 50 Hz, the specified interference voltage suppression for common mode interference will only apply for the frequencies 50 Hz ±1 %, 100 Hz ±1 %, 150 Hz ±1 %, etc. Immunity is lower for all other frequencies. Interferences caused by the line voltage distort the measured utility signal in the ratio of 100,000 : 1. An interference voltage amplitude of 1 V, for example, will affect the utility signal by 10 µV.

The Common Mode voltage (U_{CM}) defines the maximum permitted deviation of the potential between two channels and between one channel and analog ground. The interference voltage suppression defined in the technical specifications must not be exceeded. If the maximum common mode voltage specified, for example, 10 V, is exceeded, the analog signal is processed incorrectly. Depending on the module used, this error may be diagnosed and an error message output. The maximum common mode voltage may be exceeded as a result of varying input or overly long lines.

Series mode rejection

The table below sets out the possible series mode rejection specifications in the technical data of an analog module:

Interference voltage suppression for f = n x (f1 ± 1 %), (f1 = interference frequency), n = 1, 2, ...	
Series mode interference	> 60 dB

If the interference frequency is configured as 50 Hz, the specified interference voltage suppression for series mode interference will only apply for the frequencies 50 Hz ±1 %, 100 Hz ±1 %, 150 Hz ±1 %, etc. Immunity is lower for all other frequencies. Overall, interference caused by the line voltage distorts the utility signal measured by 1000 : 1. For example, an interference voltage amplitude of 1 V will affect the utility signal by 1 mV.

2.13 Crosstalk between channels

Origin of the term

The term crosstalk/XT was originally used in the field of telecommunication to denote unwanted coupling of voice signals between two cable conductors of different subscribers.

Definition

Crosstalk between signal channels denotes the interactive influence between two independent channels as a result of leakage currents and capacitive or inductive coupling. Crosstalk between the channels changes the signal by the value of the amplitude of the crosstalk signal.

Causes

Technically, it is not feasible to totally isolate the module channels from environmental conditions. This means that it is always possible for leakage currents or disturbance coupling having an interactive effect.

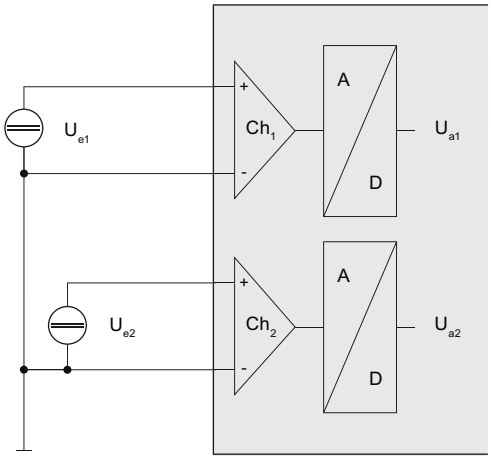


Figure 3-569 Crosstalk between two channels

The diagram shows the effects of crosstalk for the user with two channels (Ch_1/Ch_2) of an analog module. The crosstalk value is the factor by which the utility signal at a second channel U_{a2} is affected by the signal at the first channel U_{e1}. The measuring error (U_{a1}) can be calculated using the following equation:

$$U_{a1} = U_{e2} * 10^{\frac{XT\,[dB]}{20}}$$

Example of crosstalk attenuation

The "crosstalk between inputs" value in the technical specifications is defined as a value of >-100 dB at a measuring range of -10 V to +10 V on channel 1 of an eight-channel analog input module. The voltage at the input has an amplitude of 10 V. What is the error caused by crosstalk at channel 0 (measuring range ±10 V) and channel 2 (measuring range ±80 mV)?

100 dB are equal to a factor of 100,000. The measured values at channels 0 and 2 to 7 are therefore affected by 10 V / 100,000 = 100 µV. This distortion is added to or subtracted from the pending measuring signal and its effect depends on the selected measuring range.

- Channel 0: 100 µV / 10 V = 0.001 %
- Channel 2: 100 µV / 80 mV = 0.125 %

A voltage of 10 V set at channel 1 distorts the measured value at channel 0 by 0.001% and the measured value at channel 2 by 0.125%. The measuring error resulting from crosstalk in this example is therefore 0.001 % or 0.125 %. The basic error limit already includes the error generated as a result of crosstalk between the channels.

Calculating measuring error

You calculate the measurement error at channel 1 in this example based on a change in the measurement voltage of 10 V at channel 2. The crosstalk (XT [dB]) value is defined in the technical specifications in the manual of the analog module that you are using.

$$\text{Measured value error channel 1 [in V]} = \text{measured value change at channel 2 [in V]} * 10^{\frac{\text{XT [dB]}}{20}}$$

$$\text{Measured value error channel 1 [in V]} = 10\ \text{V} * 10^{\frac{-80\ \text{dB}}{20}} = 0.001\ \text{V}$$

A change in the measurement voltage of 10 V at channel 2 causes a measurement deviation of 0.001 V at channel 1.

2.14 Diagnostics

Diagnostics for analog modules

SIMATIC analog modules can diagnose errors. A number of different types of diagnostics are available for analog modules in STEP 7. Please note that the parameter assignment options vary depending on the analog module and product family used. More detailed information on the types of diagnostics can be found in the device manual for your analog input or analog output module.

Proceed as follows to select the diagnostics types of the analog module used:

1. Open STEP 7.
2. Select the analog module in the Device view.
3. Select the "Properties" tab.
4. Select the inputs or the required channel of the analog module in the Inspector window.

Table 3-81 Overview of diagnosable errors

Type of diagnostics	Analog input module	Analog output module
Wire break	✓	✓
No supply voltage L+	✓	✓
Overflow	✓	✓
Underflow	✓	✓
Common mode error	✓	-
Short-circuit	✓	✓
Overload	-	✓
Reference junction	✓	-

Diagnostics of the analog module are carried out while the system is in operation, on the basis of the current output variables such as current or voltage. If the output current or output voltage is no longer sufficient, the module will not be able to run reliable diagnostics. The limits within which diagnostics are possible are specified in the technical data for each module.

The module reports the diagnosed state to the CPU using a diagnostics error interrupt. If several diagnostics are pending at the same time, the diagnostics with the highest priority is reported to the CPU first. Diagnostics are output on LED displays on the affected module, on the CPU display, on the Web server or on an HMI device.

The configurable diagnostics types depend on the respective selected measuring type or output type. The following tables shows the relationship between the diagnostics types, measuring types or output types of an analog input module or analog output module.

Diagnostics Analog input modules

Table 3-82 **Diagnostics types of an analog input module to be configured depending on the measurement type "Voltage"**

	No supply voltage L+	Wire break (1 to 5 V)	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	✓	-	-
ET 200MP	✓	✓	✓	✓	✓	-	-
ET 200SP	✓	-	✓	✓	-	-	✓
ET 200AL	-	✓	✓	✓	-	-	✓
ET 200eco PN	✓	✓	✓	✓	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	✓

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-83 **Diagnostics types of an analog input module to be configured depending on the measurement type "**Current (4-wire transducer)**"**

	No supply voltage L+	Wire break (4 to 20 mA)	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	✓	-	-
ET 200MP	✓	✓	✓	✓	✓	-	-
ET 200SP	✓	✓	✓	✓	-	-	✓**
ET 200AL	-	✓	✓	✓	-	-	✓**
ET 200eco PN	✓	✓	✓	✓	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	✓

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

** Diagnostics for encoder supply only

Table 3-84 **Diagnostics types of an analog input module to be configured depending on the measurement type "**Current (2-wire transducer)**"**

	No supply voltage L+	Wire break (4 to 20 mA)	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	✓	-	-
ET 200MP	✓	✓	✓	✓	✓	-	-
ET 200SP	✓	✓	✓	-	-	-	✓**
ET 200AL	-	✓	✓	✓	-	-	✓**
ET 200eco PN	✓	✓	✓	✓	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	✓

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

** Diagnostics for encoder supply only

Table 3-85 **Configurable diagnostics types of an analog input module depending on the measurement type "**Resistor (4-wire connection)**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	-	-	-
ET 200MP	✓	✓	✓	✓	-	-	-
ET 200SP	✓	✓	✓	✓	-	-	-
ET 200eco PN	✓	✓	✓	-	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-86 **Configurable diagnostics types of an analog input module depending on the measurement type "**Resistor (3-wire connection)**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	-	-	-
ET 200MP	✓	✓	✓	✓	-	-	-
ET 200SP	✓	✓	✓	✓	-	-	-
ET 200AL	-	✓	✓	-	-	-	-
ET 200eco PN	✓	✓	✓	-	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-87 **Configurable diagnostics types of an analog input module depending on the measurement type "**Resistor (2-wire connection)**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	-	-	✓	-	-	-
ET 200MP	✓	-	-	✓	-	-	-
ET 200SP	✓	✓	✓	✓	-	-	-
ET 200AL	-	✓	✓	-	-	-	-
ET 200eco PN	✓	✓	✓	-	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-88 **Configurable diagnostics types of an analog input module depending on the measurement type "**Thermal resistor (4-wire connection)**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	-	-	-
ET 200MP	✓	✓	✓	✓	-	-	-
ET 200SP	✓	✓	✓	✓	-	-	-
ET 200eco PN	✓	✓	✓	✓	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-89 **Configurable diagnostics types of an analog input module depending on the measurement type "**Thermal resistor (3-wire connection)**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	-	-	-
ET 200MP	✓	✓	✓	✓	-	-	-
ET 200SP	✓	✓	✓	✓	-	-	-
ET 200AL	-	✓	✓	✓	-	-	-
ET 200eco PN	✓	✓	✓	✓	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-90 **Configurable diagnostics types of an analog input module depending on the measurement type "**Thermal resistor (2-wire connection)**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	-	-	-	✓	-	-	-
ET 200MP	-	-	-	✓	-	-	-
ET 200SP	✓	✓	✓	✓	-	-	-
ET 200AL	-	✓	✓	✓	-	-	-
ET 200eco PN	✓	✓	✓	✓	-	-	-
ET 200pro	-	✓	✓*	✓*	-	-	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Table 3-91 **Diagnostics types of an analog input module to be configured depending on the measurement type "**Thermocouple**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Common mode error	Reference junction	Short-circuit
S7-1500	✓	✓	✓	✓	✓	✓	-
ET 200MP	✓	✓	✓	✓	✓	✓	-
ET 200SP	✓	✓	✓	✓	-	✓	-
ET 200eco PN	✓	-	✓	✓	-	✓	-
ET 200pro	-	-	✓*	✓*	-	✓	-

* For ET 200pro, the parameters "Overflow" and "Underflow" are combined to the parameter "Overflow/Underflow"

Diagnostics for analog output modules

Table 3-92 **Diagnostics types of an analog output module to be configured depending on the measurement type "**Voltage**"**

	No supply voltage L+	Wire break	Overflow	Underflow	Short-circuit	Overload
S7-1500	✓	-	✓	✓	✓	-
ET 200MP	✓	-	✓	✓	✓	-
ET 200SP	✓	-	✓	✓	✓	-
ET 200eco PN	✓	-	-	-	✓	✓
ET 200pro	-	-	-	-	✓	-

Table 3-93 **Diagnostics types of an analog output module to be configured depending on the measurement type "**Current**"**

	No supply voltage L+	**Wire break**	**Overflow**	**Underflow**	**Short-circuit**	**Overload**
S7-1500	✓	✓	✓	✓	-	-
ET 200MP	✓	✓	✓	✓	-	-
ET 200SP	✓	✓	✓	✓	-	-
ET 200eco PN	✓	✓	-	-	-	✓
ET 200pro	-	✓	-	-	-	-

NOTE

Measuring ranges

Note that the diagnostics types that can be parameterized depend on the selected measurement/output type as well as on the respective measuring range.

NOTE

Minimum output values

Certain errors such as wire break and short circuit cannot be diagnosed below a given current or voltage value. Diagnostics are only possible again once the output returns to above this minimum value.

No supply voltage L+

You can diagnose a missing or low supply voltage L+ at the analog module by activating the "No supply voltage L+" checkbox. If the supply voltage is missing or too low, the status and error display on the analog module will provide the relevant information. The entry in the diagnostics buffer also makes this information available to the CPU.

If there is no supply voltage, no other types of diagnostics available are possible either.

Wire break

The term wire break denotes a failure state that is triggered by the interruption of a usually closed electrical circuit.

Wire break in analog input modules

The "Wire break" diagnostics function facilitates the detection of errors during system operation. In STEP 7 you define the module properties by setting various parameters. Depending on the module used, you may, for example, be able to set a current limit parameter at which a wire break is to be reported.

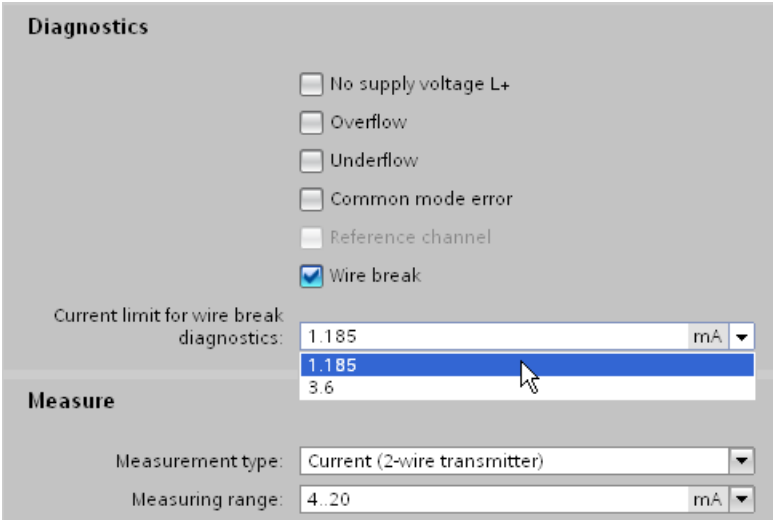


Figure 3-570 Configuring the wire break current limit for an analog input module in STEP 7

Usually, the live zero technique is deployed to detect wire breaks. The start of the measuring range for the standard live zero signal of 4 to 20 mA is assigned the 4 mA signal value. A wire break between the input and sensor can therefore be detected based on the missing current flow. Instead of a current signal, you may also use a voltage signal from 1 to 5 V to detect a wire break. The "Wire break" diagnostics function can therefore only be configured for a range of 4 to 20 mA or 1 to 5 V.

For "Resistor", "Thermal resistor" and "Thermocouple" measurements, a current is impressed into the line. If a wire break occurs, the flow of current is interrupted and the analog module therefore detects the wire break.

Wire break in analog output modules

The analog signal output is used for wire break detection. Reliable wire break diagnostics is not possible if the voltage is too low. In this case, the diagnostics function is deactivated without triggering a change of the diagnostics status.

The current limit up to which the module will diagnose wire break can be found in the technical data for the module.

Overflow/underflow

The resolution of the measuring range of an analog input module distinguishes between the rated range, the overrange or underrange, and the overflow or underflow. The following table assign the number of increments into which the measured signal is divided to the various voltage measuring ranges.

Table 3-94 Voltage measuring range ±10 V of an analog input module

Value (increments)	Voltage measuring range	Range
Decimal	**±10 V**	
32767	> 11.759 V	Overflow
32511	11.759 V	Overrange
27649		
27648	10.0 V	Rated range
0	0 V	
-27648	-10 V	
-27649		Underrange
-32512	-11.759 V	
-32768	< -11.759 V	Underflow

As of a decimal value of 32512, the value acquired is beyond the overrange and is no longer valid. If this is the case, the error status "Overflow" is diagnosed. The overrange is a tolerance range before overflow is reached.

As of a decimal value of -32513, the value acquired is below the configured measuring range and is no longer valid. If this is the case, the error status "Underflow" is diagnosed. The underrange is the equivalent of the overrange, but for negative values.

An "Overflow" or "Underflow" diagnostics may be caused, for example, by a wire break, an incorrect measuring range or incorrect wiring.

NOTE

Accuracy

The accuracy specified in the technical data of the relevant module is only guaranteed within the rated range.

Common mode error

Activating the "Common mode" checkbox diagnoses a violation of the maximum potential difference U_{CM}. A violation of the permitted potential difference U_{CM} has occurred, for example, between the reference point of the measuring inputs and the analog ground M_{ANA} .

Possible causes:

- Wiring error
- Environments with EMC disturbance
- Incorrectly grounded transducers
- Long line lengths
- Sensor not connected
- 2-wire transducer connected to M_{ANA}

NOTE

With 4-wire transducers, a current meter connected in series will result in too great a drop in voltage.

Potential differences U_{CM} beyond the valid limits may lead to measurement errors and malfunctions. If you want to ensure that the maximum value is not exceeded, interconnect the measuring inputs and analog ground M_{ANA} with an equipotential bonding cable. More detailed information can be found in Wiring transducers.

Short-circuit

Activating the "Short circuit" checkbox activates short-circuit diagnostics for an analog channel. The diagnostics function is triggered by channel overload.

Possible causes:

- Wiring error (e.g. short circuit between conductors at the connections or in the cable)
- Use of faulty or incorrect actuators (e.g. internal short circuit or low input resistance as a result of actuator failure)

The analog signal output is used for short circuit detection. If the voltage is too low, reliable short-circuit diagnostics are not possible. In this case, the diagnostics function is deactivated without triggering a change of the diagnostics status. The voltage limit up to which the module will diagnose a short circuit can be found in the technical data for the module.

SIMATIC modules have a special protective circuit to prevent short circuit. The short circuit current is limited internally in the module. The level of short circuit current is specified in the technical data of your analog module.

NOTE

Overload

Please note that overload exposes the modules are exposed to a greater thermal load. This can affect the output channels. You should therefore avoid continuously running analog output modules in overload.

Reference junction

This type of diagnostics can only be selected for analog input modules for "Thermocouple" measuring. Selecting the "Reference junction" check box diagnoses an error on the reference channel for compensating the reference junction temperature.

The temperature at the reference junction of a thermocouple is measured at the reference channel of the module using an external thermal resistor (RTD). If an error occurs, for example as a result of a wire break, the temperature measured at the reference junction of the thermocouple will no longer be compensated. The reference temperature may then be outside the valid range.

Additional information on connecting thermocouples and thermal resistors and on how they operate can be found in Thermocouples and Wiring transducers.

Overload

Activating the "Overload" checkbox activates the diagnostics of the thermal monitoring of the output level. The "Overload" diagnostics is triggered when the maximum temperature is exceeded at the output and is detected channel by channel.

The maximum temperature may be exceeded for the following reasons:

- Ambient temperature is too high
- Output is being operated outside the specification

NOTE

Overload

Please note that overload exposes the modules to a high thermal load. This can affect the output channels. You should therefore avoid continuously running analog output modules in overload.

2.15 Value status

Value status

In case of a faulty analog value, the analog module outputs the error values 0x7FFF (error value for overflow and all other error states) or 0x8000 (error value for underflow) for the affected channel. The user program is now able to detect and evaluate a channel error. The user also has the option to evaluate the system diagnostics event-driven by means of diagnostics alarms.

In addition to the error values 0x7FFF or 0x8000 and the configured diagnostic types, analog input and output modules provide diagnostics information by means of the Process image input (PII). It is referred to as Value status and transferred synchronously with the user data. The value status (Quality Information = QI) provides a statement regarding the validity of the input signal. A distinction is made between the quality level "Good" (signal valid = 1) and "Bad" (signal invalid = 0).

NOTE

For analog input modules, the use of the value status is an alternative to the evaluation of the channels by the error values 0x7FFF or 0x8000. Compared to the error values, the binary evaluation of the value status (0 or 1) in the user program is simpler and more clearly arranged.

For analog output modules, the value status informs you as to whether the written value can be output by the respective channel. Using the value status you can respond to this information without having to evaluate the diagnostics of the module in the first place.

Example

Enabling the value status of an analog input module

To enable the value status of an analog input module, follow these steps:

- Select the required analog module in STEP 7.
- Select "AI configuration" in the "Properties" tab of the analog module.
- Click the "Value status" button.

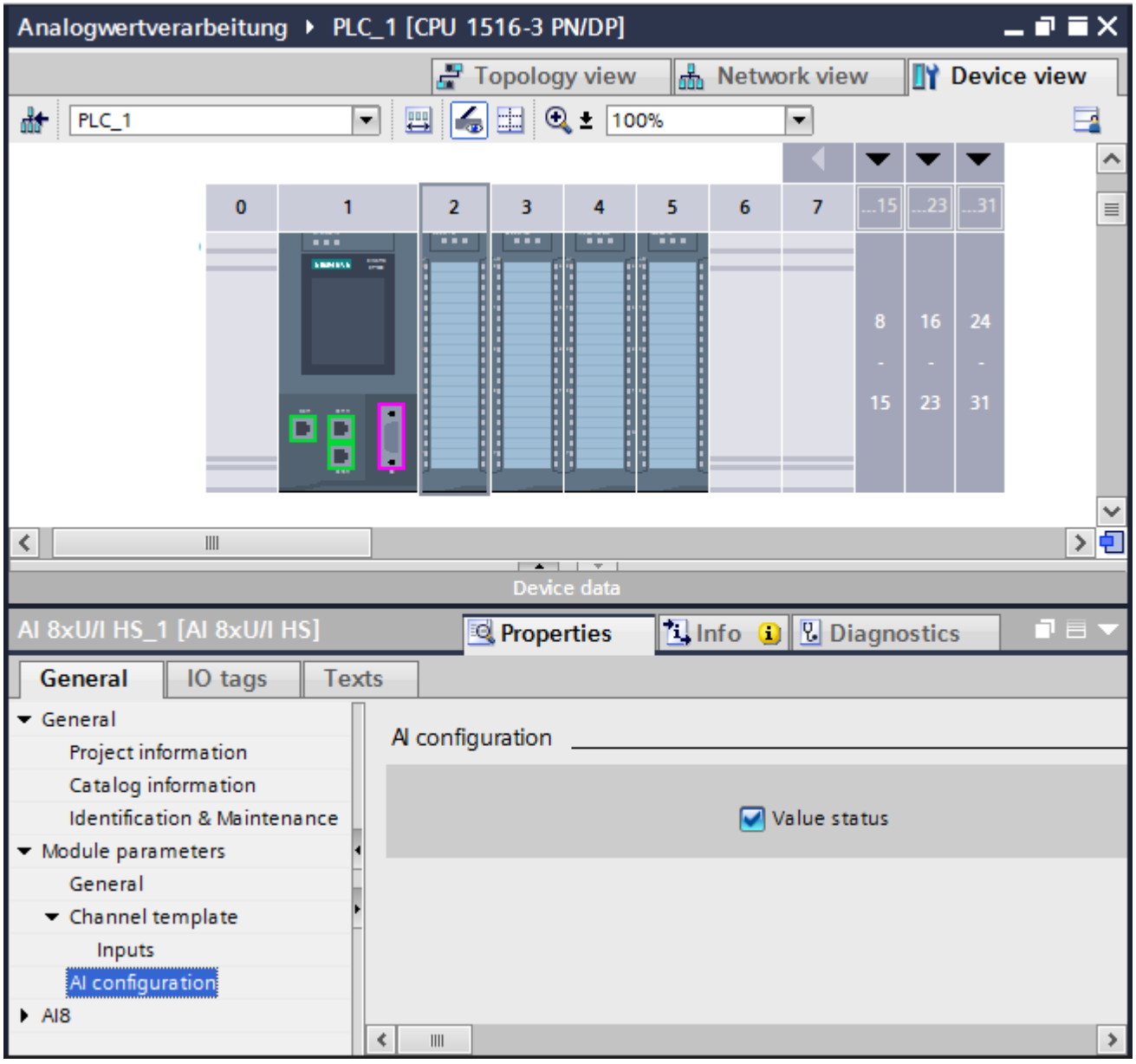


Figure 3-571 Enabling the value status in STEP 7

An additional byte is occupied in the input address space of the respective module when you enable the value status. Each bit in this byte is assigned to a channel and provides information on, for example, whether the output value specified by the user program is actually queued at the module terminal (0= value is invalid; 1= value is valid).

Error occurrence

If a wire break occurs at an analog input module, for example, the current signal state is entered in the process image and the value status of the signal is set to "invalid". To trigger an indicator light in case of an error, for example, evaluate the value status in the user program.

Diagnostics alarms and value status

If you configure analog modules in a third-party product with the help of a GSD file and the diagnostics alarms are not evaluated event-driven, it is best to use the value status.

NOTE

The Value status represents a group diagnostics which only gives the user a Good or Bad information. The Value status is not suitable for a more specific identification of the cause of the error (e.g., wire break, short circuit in the encoder cable or load voltage failure).

2.16 Conversion time of an analog module

Basic conversion time and conversion time of an analog input channel

The basic conversion time is the minimum time required by one single channel to convert analog values. The actual conversion time comprises both the basic conversion time and, depending on the analog input module used:

- Processing time for measuring resistance
- Processing time for wire break monitoring
- Processing time for overflow/underflow monitoring
- Processing time for checking common mode errors

Example

This example shows channel 6 of an analog input module for resistance measurement in the range of 6000 Ω, a configured integration time of 20 ms, and activated wire break monitoring.

The conversion time of the channel is derived from the total of the following measurement variables:

Measurement variable	Time in ms
Basic conversion time	27
Processing time for RTD/resistance (6000 Ω)	4
Processing time for wire break monitoring in the RTD/resistance and thermocouple areas	9
Conversion time of the channel	**40**

Conversion time of the analog output channels

The conversion time of an output channel starts with the transfer of the digital value from the internal memory of the module and ends with the digital-to-analog conversion.

The conversion time does not include the settling time for the analog signal at the module terminal. Detailed information on the settling time can be found in Settling and response times of analog output modules (Page 44).

NOTE

Relationship between diagnostics and conversion time

While some diagnostics run parallel to the conversion and do not extend the conversion time, other diagnostics types can lead to an extension of the conversion time, as demonstrated in the example above.

Conversion time for high-speed analog modules

High-Speed analog modules (HS modules) are designed for faster processing of signals. HS modules offer fewer diagnostics and measurement types than standard modules (ST modules). You can find more information on HS modules in the section High-Speed analog modules (Page 94).

2.17 Cycle time of an analog module

Definition

The cycle time of an analog module represents the time that the module needs to process all channels used. The cycle time depends on the form of measured value acquisition used, e.g. multiplex or parallel measured value acquisition.

Sequential measured value processing

This procedure processes the analog channels in the module one after another (sequentially). For analog inputs, the values are connected to a converter, for example using a multiplexer, and sequentially converted.

The cycle time of the analog module is derived from the total conversion time of all activated analog channels of the module. STEP 7 provides the option of deactivating unused analog channels. to reduce the cycle time.

The figure below gives an overview of the factors that determine the cycle time of an n-channel analog module.

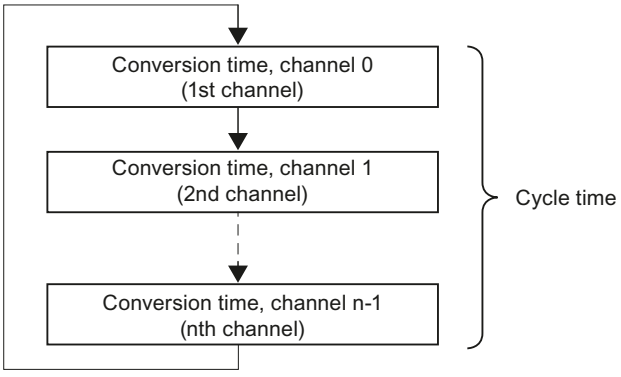


Figure 3-572 Cycle time of an analog module with multiplex conversion

Parallel measured value acquisition

This procedure processes the analog channels of a module at the same time (in parallel) rather than one after another. In parallel measured value processing, the cycle time of the module is usually constant and does not depend on the number of channels used. The goal of parallel measured value acquisition as it is applied by high-speed analog modules, for example, is a shorter cycle time. You can find more information on HS modules in the section High-Speed analog modules (Page 94).

2.18 Settling and response times of analog output modules

Settling and response times provide information on the delay of the output of a specified analog output variable and its availability to the process.

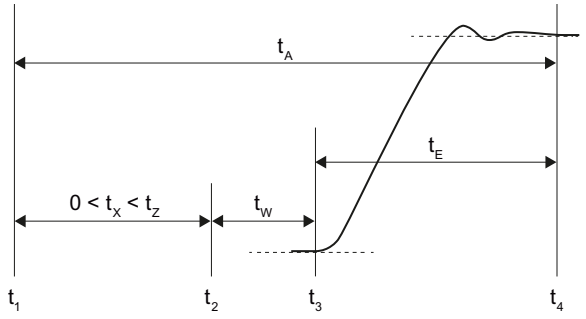
Response time

The response time for a new output value is defined as the time between the input of a digital output value to the internal memory of the module and the value to be output at the analog output being reached (with a residual error of 1 %).

The response time (t_A) is the sum of application time (t_X), conversion time (t_W) and settling time (t_E):

$t_A = t_X + t_W + t_E$

Settling and response times of analog output modules



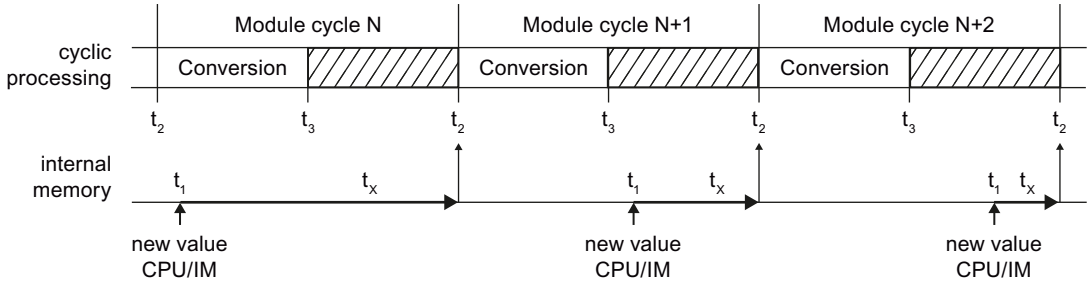
t_A	Response time
t_X	Application time
t_Z	Module cycle time
t_W	Conversion time
t_E	Settling time
t_1	New digital output value is available in the internal memory of the module
t_2	Module activates the digital output value and starts conversion
t_3	Module ends conversion at the terminal of the analog output channel and outputs the analog signal
t_4	Signal has settled and the specified analog output value has been reached (residual error 1 %)

Figure 3-573 Settling and response time of an output channel

Application time

The CPU/IM (interface module) writes new output values to the internal memory of the analog output module. The time required for this is not determined by the CPU/IM. These output values are converted asynchronously to their entry in buffer memory. The worst-case application time (t_X) may be equal to the cycle time (t_Z). This situation develops if the CPU writes a new value to the internal memory of the module immediately after the transfer of the value for conversion. This new value will not be processed until the next conversion.

The figure below shows acyclic access of the analog output module to output values from the internal memory in non-isochronous mode. You can find more information on isochronous mode in the paragraph on isochronous mode of the section High-Speed analog modules (Page 94).



t_X Application time

t_1 New digital output value is available in the internal memory of the module

t_2 Module activates the digital output value and starts conversion

t_3 Module ends conversion at the terminal of the analog output channel and outputs the analog signal

Figure 3-574 Application of the output values

Conversion time

The conversion time of an output channel starts with the transfer of the digital value from the internal memory of the module (t_2) and ends with the digital-to-analog conversion (t_3).

Settling time

The settling time starts when the analog signal is output to the module (t_3) terminals and ends when the output value (t_4) is reached. The output value is reached as soon as the output signal has settled at its final value, taking into account a residual error of 1%.

The settling time depends on the type of output for the module, and on the connected load. The load for the analog output consists of connecting line and connected actuator. When the output is "Current", the settling time increases with high ohmic resistance. Inductive loads cause subsequent fluctuation in the output value. When the output is "Voltage", the capacitive load causes subsequent fluctuation.

2.19 Smoothing

Using the smoothing functions

Most analog input modules allow you to configure smoothing for the measuring signal in STEP 7. Smoothing analog values reduces the effect of interference signals. Smoothing is useful with slow changes in measured values, for example in temperature measurements.

Smoothing principle

The measured values are smoothed by means of filtering. The module forms mean values from a specified number of converted (digitalized) analog values. Smoothing should not be confused with the integration of measured values over a defined period of time. It is therefore not possible to smooth measured signals to filter out a specific interference frequency. However, this smoothing returns more "stable" data values because it suppresses peaks which overlay the measured signal.

4 (none, weak, medium, strong) or more levels of smoothing can be configured by the user depending on the module used. The level determines the number of analog values from which the mean value is generated. The greater the smoothing factor, the better the filtering.

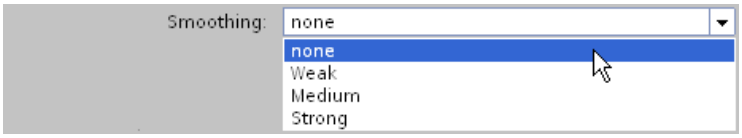


Figure 3-575 Selecting the smoothing level in STEP 7

Smoothing method

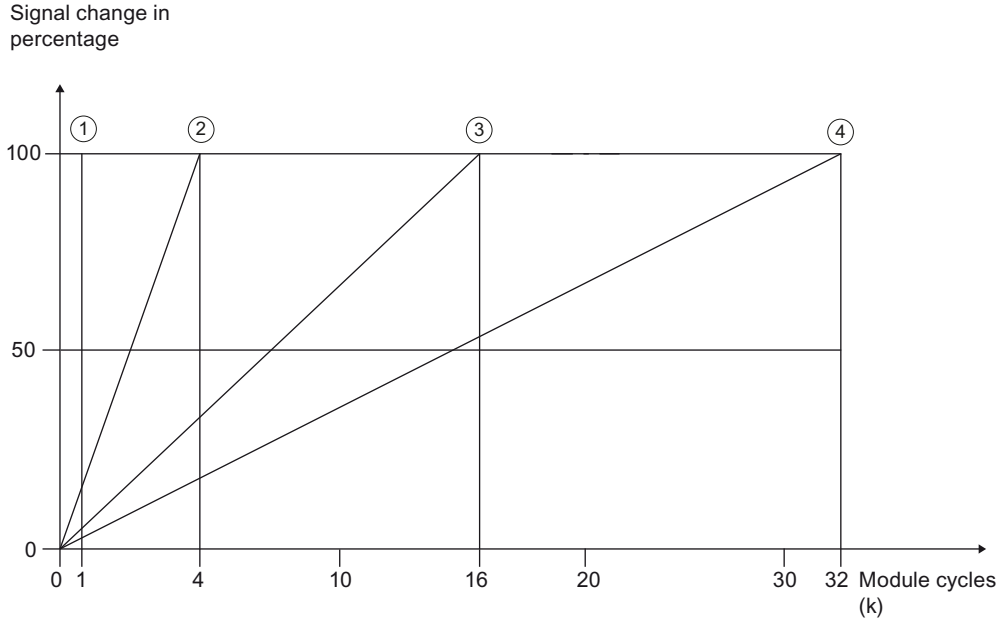
A smoothing algorithm is applied to a configurable number of measured values (e.g. 4, 8, 32) in line with the moving average. Each new measured value is factored in, and the oldest measured value then ignored. This mechanism suppresses interference peaks which overlay the measured signal. Utility signal jumps only become evident in the data after some time (see examples below).

The modules of the various product ranges use different smoothing algorithms. Smoothing is either linear or exponential. The differences are apparent particularly with strong smoothing and lead to a faster or slower rate of rise depending on the product used.

For information on whether or not a specific module supports customization of the smoothing function, please refer to the manual of the analog input module.

Example 1: Linear smoothing

The diagram below shows the number of module cycles (k) it takes for each smoothing level setting for the smoothed analog value to reach approximately 100 % after a step response. This specification is valid for all signal changes at the analog input.

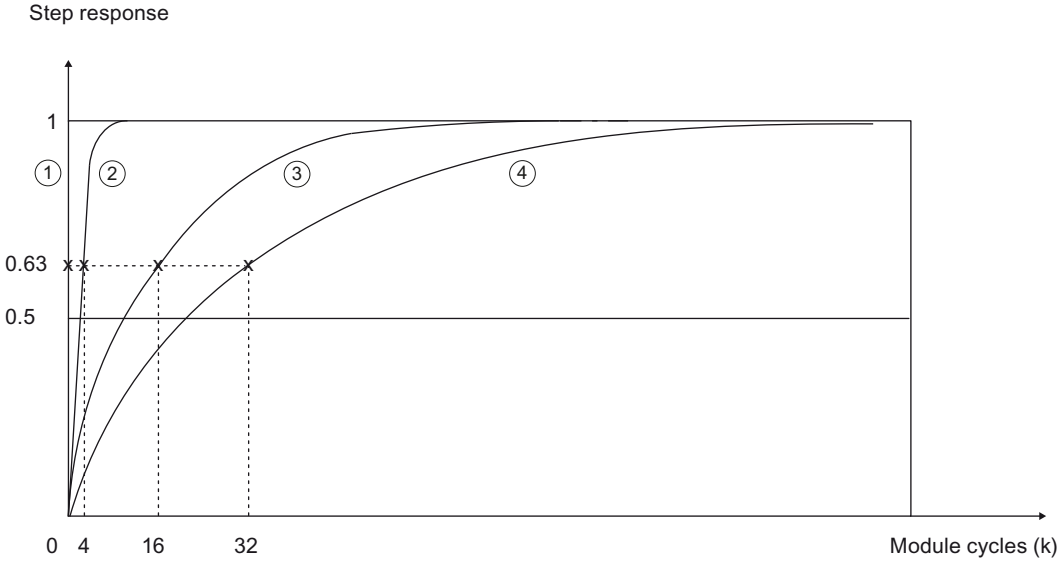


① No smoothing (k = 1)
② Weak smoothing (k = 4)
③ Medium smoothing (k = 16)
④ Strong smoothing (k = 32)

Figure 3-576 Linear smoothing with four smoothing levels

Example 2: Exponential smoothing

The diagram below shows the step response of the smoothing factor for different numbers of module cycles.



① No smoothing (k = 1)
② Weak smoothing (k = 4)
③ Medium smoothing (k = 16)
④ Strong smoothing (k = 32)

Figure 3-577 Exponential smoothing with four smoothing levels

2.20 Burden with 2-wire transducers

2-wire transducers

2-wire transducers are current transducers which convert the process variable into a current signal of between 4 and 20 mA. Two connection lines supply the transducer with an output current of at least 4 mA. Additional information on connecting 2-wire transducers to analog input modules can be found in the section Wiring current transducers (Page 59).

Burden

The burden indicates how great the external resistance in a current loop may be. If the external resistance is greater than the specified burden, the 2-wire transducer supply voltage is too low. The burden consists of the resistance of the transducer and all other resistances connected to the current loop.

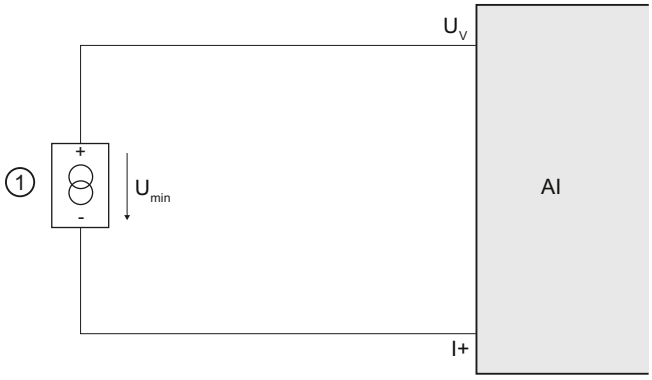
The maximum admissible burden of the transducer, e.g. 820 Ω, is specified in the technical data of the analog module.

Example 1: Connecting a transducer to the electrical circuit

In accordance with the technical data of the 2-wire transducer used, it requires a supply voltage (U_{min}) of at least 8.5 V. Using Ohm's Law, you can calculate the resistance of the transducer used (R_{2DMU}) for a current of 20 mA.

$$R_{2DMU} = \frac{U_{min}}{I} = \frac{8.5\ V}{0.020\ A} = 425\ \Omega$$

With a supply voltage of at least 8.5 V, the transducer has a resistance of 425 Ω. The resistance is less than 820 Ω. You can therefore connect the transducer to the analog input module (AI) without exceeding the maximum burden.



① 2-wire transducers
U_V Terminal for feed voltage at the channel
I+ Terminal for current input
U_{min} Voltage drop at 2-wire transducer

Figure 3-578 Connecting a transducer to the electrical circuit

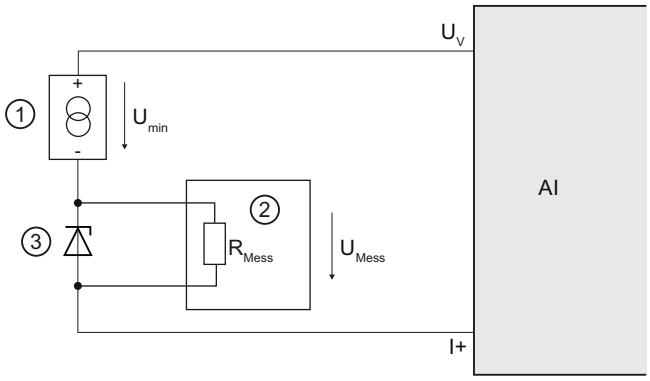
Example 2: Connecting a transducer and other devices

If multiple measuring devices are connected in series, the sum of all connected resistances may not exceed the value of the maximum burden.

If you have connected a 2-wire transducer to a supply voltage of 8.5 V, you will need to allow for the resistance of the measuring device connected ②.

Maximum transducer burden:	820 Ω
Transducer resistance upon a voltage drop of 8.5 V:	425 Ω
Maximum resistance of additional devices connected:	395 Ω

The resistance of the measuring instrument may therefore not exceed 395 Ω.



① 2-wire transducers
② Digital multimeter
③ Zener diode
U_V Terminal for feed voltage at the channel
I+ Terminal for current input
U_{min} Voltage drop at 2-wire transducer
R_{Mess} Resistance at measuring instrument
U_{Mess} Voltage drop at the measuring instrument

Figure 3-579 Connecting a transducer and other devices to the circuit

Calculating admissible voltage drop

The maximum additional resistance in the current loop may not exceed 395 Ω at a maximum current of 20 mA. You can calculate the voltage drop at the connected measuring instrument (U_{Mess}) as follows using Ohm's Law:

$U_{Mess} = R_{Mess} * I = 395\ \Omega * 0.020\ A = 7.9\ V$

The voltage drop at the measuring instrument should therefore not exceed 7.9 V.

Representation of analog values

3

3.1 Overview

Conversion of analog values

The CPU only processes analog values in digitalized format.

Analog input modules convert the analog signal into a digital value for further processing by the CPU.

Analog output modules convert the digital output value from the CPU into an analog signal.

Analog value representation at 16-bit resolution

The digitized analog value is the same for all I/O values at the same rated range. The analog values are represented as fixed point numbers in twos complement. This leads to the following conditions:

Table 3-95 Representation of analog values

Resolution	Analog value															
Bit number	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Significance of the bits	S	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

Sign

The sign (S) of the analog value is always set in bit 15:

- "0" → +
- "1" → -

Resolution less than 16 bits

The analog value is left-aligned in the memory of analog modules with a resolution of less than 16 bits. The unused least significant digits are padded with "0" values.

This reduces the number of measured values that can be represented. Modules occupy a range of values of between+32767 and -32768 regardless of the resolution. The scaling between two successive values depends on the resolution of the module.

Example

The following example shows how the least significant digits are padded with "0" values:

- The module with 16-bit resolution is capable of incrementing the values in steps of one unit ($2^0 = 1$).
- The module with 13-bit resolution is capable of incrementing the values in steps of 8 units ($2^3 = 8$).

Table 3-96 Example: Bit pattern of a 16-bit and 13-bit analog value

Resolution	Analog value															
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
16-bit	S	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
13-bit	S	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	0	0	0

S = sign

NOTE

For information on the resolution supported by each analog module, please refer to the technical data for the relevant module.

3.2 Representation of input ranges

The tables below set out the digitalized representation of the input ranges by bipolar and unipolar input ranges. The resolution is 16 bits.

Please see the device manuals for each analog input module for assignment of the values to the specific measured values in each measuring range.

Table 3-97 Bipolar input ranges

Dec. value	Measured value in %	Data word																Range
		2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
32767	>117.589	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Overflow
32511	117.589	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	Over range
27649	100.004	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	
27648	100.000	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	Rated range
1	0.003617	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
0	0.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
-1	-0.003617	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
-27648	-100.000	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	
-27649	-100.004	1	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	Under range
-32512	-117.593	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
-32768	<-117.593	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Underflow

Table 3-98 Unipolar input ranges

Dec. value	Measured value in %	Data word																Range
		2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
32767	>117.589	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Overflow

Dec. value	Measured value in %	Data word																Range
32511	117.589	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	Over range
27649	100.004	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	
27648	100.000	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	Rated range
1	0.003617	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
0	0.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
-1	-0.003617	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Under range
-4864	-17.593	1	1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	
-32768	<-17.593	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Underflow

3.3 Representation of output ranges

The tables below set out the digitalized representation of the output ranges by bipolar and unipolar range. The resolution is 16 bits.

Please see the device manuals for each analog output module for assignment of the values to the specific output values in each measuring range.

Table 3-99 Bipolar output ranges

Dec. value	Output value in %	Data word																Range
		2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}	
32511	117.589	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	Maximum output value*
32511	117.589	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	Over range
27649	100.004	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	
27648	100.000	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	Rated range
1	0.003617	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
0	0.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
-1	-0.003617	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
-27648	-100.000	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	
-27649	100.004	1	0	0	1	0	0	1	1	1	1	1	1	1	1	1	1	Under range
-32512	-117.593	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
-32512	-117.593	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	Minimum output value**

* When values > 32511 are specified, the output value is limited to 117.589 % or 0 % (0.0 V / 0.0 mA), depending on the module used.

** When values < -32512 are specified, the output value is limited to -117.593 % or 0 % (0.0 V / 0.0 mA), depending on the module used.

Table 3-100 Unipolar output ranges

Dec. value	Output value in %	Data word																Range
		2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}	
32511	117.589	0	1	1	1	1	1	1	1	x	x	x	x	x	x	x	x	Maximum output value*
32511	117.589	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	Over range
27649	100.004	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	
27648	100.000	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	Rated range
1	0.003617	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
0	0.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
0	0.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Minimum output value**

* When values > 32511 are specified, the output value is limited to 117.589 % or 0 % (0.0 V / 0.0 mA), depending on the module used.

** When values < 0 are specified, the output value is limited to 0% (0.0 V / 0.0 mA).

Connecting transducers

4

4.1 Overview

Introduction

This chapter describes the basic procedure for wiring transducers to analog inputs. Information on specific wiring options is available in the manual of each module.

For more information, e.g. on cable routing and shielding or potential equalization, etc., refer to the function manual for Configuring interference-free controllers (http://support.automation.siemens.com/WW/view/en/59193566).

Transducers that can be wired to analog inputs

You can wire the following transducers to the analog input modules, depending on the type of measurement:

- Voltage transducers
- Current transducers
  - 2-wire transducers
  - 4-wire transducers
- Resistance transducers
  - 4-wire connection
  - 3-wire connection
  - 2-wire connection
- Thermocouples

Isolated transducers and non-isolated transducers

Transducers are available in various models:

- Isolated transducers are **not connected** locally to the ground potential. Floating operation is possible.
- Non-isolated transducers are **connected** locally to the ground potential.

  Non-isolated transducer connections are connected to the conductive enclosure.

  Note: All non-isolated transducers must have a galvanic connection to each other and be locally connected to the ground potential.

Abbreviations used in the figures

Key to the abbreviations in the figures below:

AI	Analog input module
M	Ground connection
L+	Supply voltage connection
M_n+/M_n-	Measuring input, channel n
I_{Cn}+/I_{Cn}-	Current output to thermal resistor (RTD) channel n
U_n+/U_n-	Voltage input channel n
I_n+/I_n-	Current input channel n
COMP+/COMP-	Compensation input
I_{Comp}+/I_{Comp}-	Current output for compensation
U_V	Feed voltage at channel (the connection can be used for 2-wire transducer (2DMU) or with ET 200eco PN and ET 200pro for 2/4-wire transducer).
U_{CM}	Potential difference between the reference points of the measuring inputs / the analog ground M_{ANA}
U_{ISO}	Potential difference between the reference points of the measuring inputs and the central ground
M_{ANA}	Reference point of the analog ground

Lines for analog signals

Always use shielded twisted-pair cables to wire the analog signals. This improves immunity.

4.2 Wiring analog inputs with MANA connection

The reference potentials of the measuring inputs and the central ground are electrically isolated in analog input modules with M_{ANA} connection.

Limited potential difference U_{ISO} (insulation voltage)

Always verify that the admissible potential difference U_{ISO} between the reference point of the analog ground M_{ANA} and the central ground is not exceeded.

Potential difference U_{ISO} may be caused by: Maximum line lengths exceeded.

If you want to ensure that the permitted value U_{ISO} is not exceeded, install an equipotential bonding cable between the terminal M_{ANA} and the central grounding point.

Limited potential difference U_{CM} (common mode)

Always verify that the admissible potential difference U_{CM} between the reference point of the measuring inputs and the analog groundM_{ANA} is not exceeded.

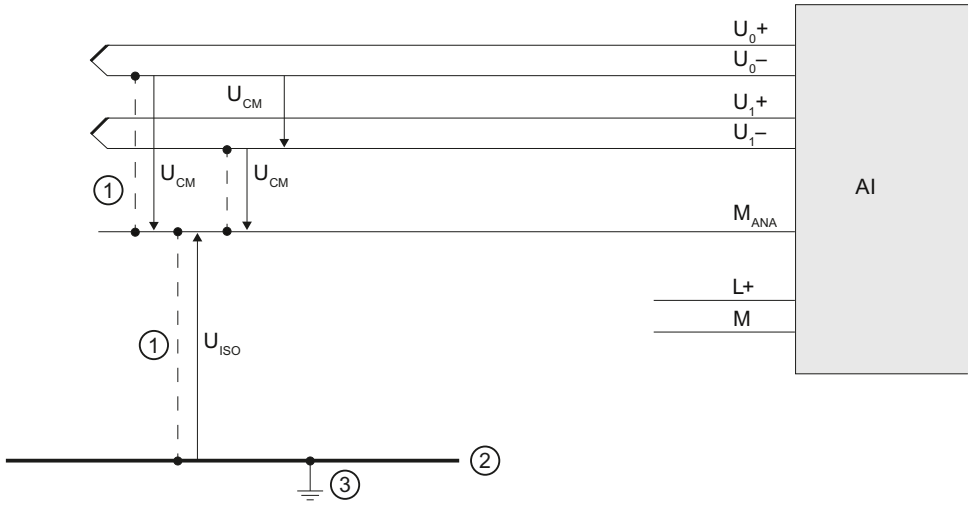
Potential differences U_{CM} may be caused by:

- Environments with EMC disturbance
- Use of grounded transducers
- Use of long cable lengths

Measuring errors / malfunctions can occur if the admissible potential difference U_{CM} is exceeded.

Some modules can detect an invalid potential difference U_{CM} and report this error with an entry in the diagnostics buffer of the CPU.

If you want to ensure that the maximum value U_{CM} is not exceeded, interconnect the reference points of the measuring inputs and the analog ground M_{ANA} with an equipotential bonding cable.



① Equipotential bonding cable
② Grounding bus cable
③ Central ground

Figure 3-580 Example: Reference potential for analog input modules with M_{ANA} connection

4.3 Wiring analog inputs without MANA connection

The reference potentials of the measuring inputs and the central ground are electrically isolated from each other in analog input modules without an M_{ANA} connection.

Limited potential difference U_{ISO} (insulation voltage)

Always verify that the maximum potential difference U_{ISO} between the reference points of the measuring inputs and central ground is not exceeded.

Potential difference U_{ISO} may be caused by: Maximum line lengths exceeded.

If you want to ensure that the permitted value U_{ISO} is not exceeded, install an equipotential bonding cable between the reference points of the measuring inputs and the central grounding point.

Limited potential difference U_{CM} (common mode)

Always ensure that the permitted potential difference U_{CM} between the reference points of the measuring inputs is not exceeded.

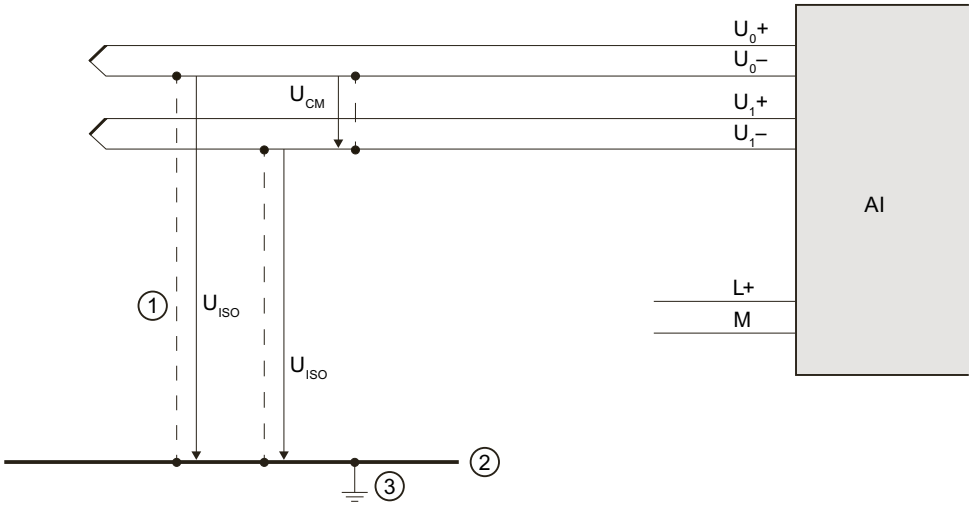
Potential differences U_{CM} may be caused by:

- Environments with EMC disturbance
- Use of grounded transducers
- Use of long cable lengths

Measuring errors / malfunctions can occur if the admissible potential difference U_{CM} is exceeded.

Some modules can detect an invalid potential difference U_{CM} and report this error with an entry in the diagnostics buffer of the CPU.

If you want to ensure that the permitted value U_{CM} is not exceeded, install equipotential bonding cables between the reference points of the measuring inputs or, with the ET 200eco PN and ET 200pro, between the reference points of the measuring inputs and ground.

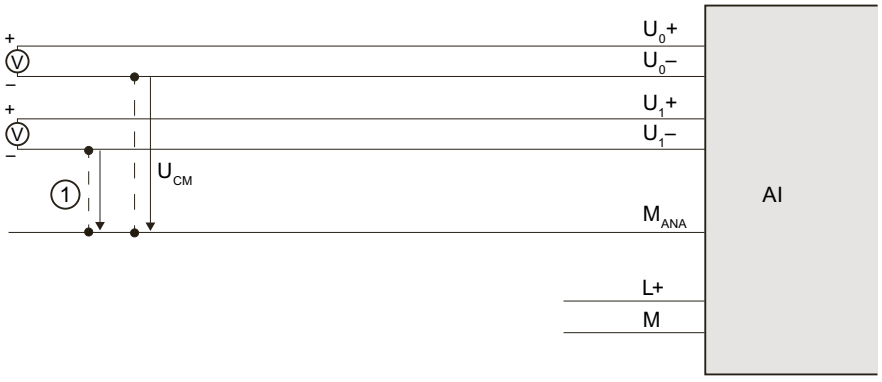


① Equipotential bonding cable (not for 2-wire and resistance transducers)
② Grounding bus cable
③ Central ground

Figure 3-581 Example: Reference potential for analog input modules without M_{ANA} connection

4.4 Wiring voltage transducers

The figure below shows how to connect voltage transducers. If you want to ensure that the permitted value U_{CM} is not exceeded, install equipotential bonding cables to connect the reference points of the measuring inputs to the analog ground M_{ANA}, or with ET 200eco PN and ET 200pro the reference points of the measuring inputs to the ground.



① Equipotential bonding cable (only relevant to modules with M_{ANA} connection)

Figure 3-582 Example: Wiring voltage transducers to an analog input module

4.5 Wiring current transducers

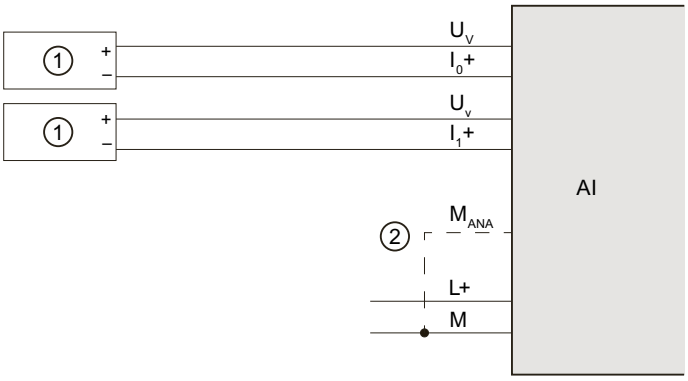
Current transducers are available as 2-wire transducers and 4-wire transducers. Below are a number of ways to supply current transducers with voltage.

Wiring 2-wire transducers with power supply from the module

The 2-wire transducer converts the process variable into a current. The 2-wire transducer is wired to the short circuit-proof supply voltage at the terminals of the analog input module. The transducer is therefore frequently also called a "passive transducer". Its simple wiring means that the 2-wire transducer is frequently used in industrial environments. If you use this type of connection, you will need to set the "Current (**2-wire transducer**)" measurement type in STEP 7.

NOTE

2-wire transducers must be electrically isolated.



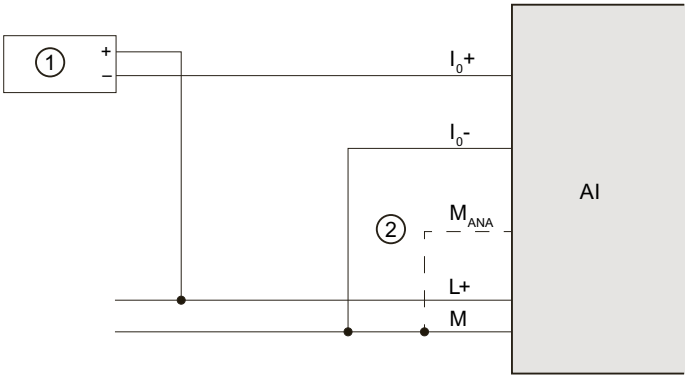
① 2-wire transducers (2WT)
② Equipotential bonding cable (only relevant to modules with M_{ANA} connection)

Figure 3-583 Example: Wiring 2-wire transducers to an analog input module

Wiring 2-wire transducers to an analog input for 4-wire transducers

The figure below shows an alternative to the above connection: supplying the 2-wire transducer from supply line L+ of the module. If you use this type of connection, you will need to set the "Current (**4-wire transducer**)" measurement type in STEP 7.

In this type of connection, galvanic isolation between the supply voltage L+ and the analog circuit will be removed.

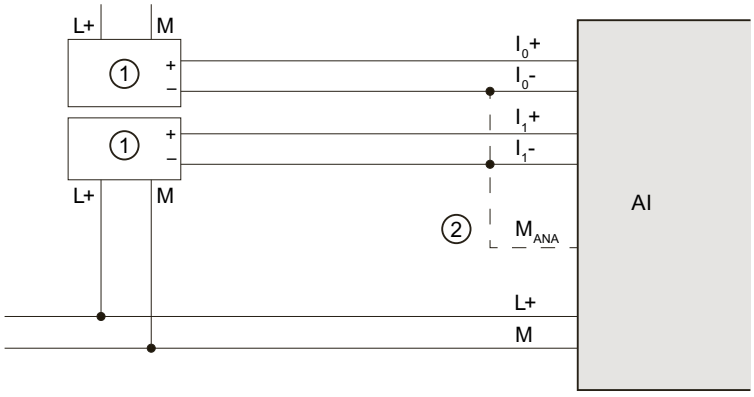


① 2-wire transducers (2WT)
② Equipotential bonding cable (only relevant to modules with M_{ANA} connection)

Figure 3-584 Example: Wiring 2-wire transducers to an analog input for 4-wire transducers

Wiring and connecting 4-wire transducers

4-wire transducers provide terminals for connecting a separate supply voltage. They are powered with an external supply and are frequently called "active transducers". If you use this type of connection, you will need to set the "Current (**4-wire transducer**)" measurement type in STEP 7.



① 4-wire transducers (4WT)

② Equipotential bonding cable (only relevant to modules with M_{ANA} connection)

Figure 3-585 Example: Wiring 4-wire transducers to an analog input module

4.6 Wiring thermal resistors and resistors

The module provides a constant current at terminals I_C+ and I_C- for resistance measurements. The constant current is fed to the resistance to be measured where it is measured as voltage drop. It is important to wire the connected constant current cables directly to the thermal resistor/resistor.

Measurements with 4-wire or 3-wire connection compensate for line resistance and therefore achieve greater accuracy compared to measurements with 2-wire connection.

Measurements with two-wire connection always acquire line resistance in addition to the actual resistance; you must therefore allow for a significant loss of precision in the measuring results.

The figures below give some connection examples.

4-wire connection of a thermal resistor

The voltage at the thermal resistor is acquired using high-impedance measurement via the M_0+ and M_0- terminals. Make sure the wiring is correctly poled (I_{C0}+ and M_0+, and I_{C0}- and M_0- at the thermal resistor).

Always wire the **I_{C0}+ and M_0+** lines, and the **I_{C0}- and M_0-** lines directly to the thermal resistor.

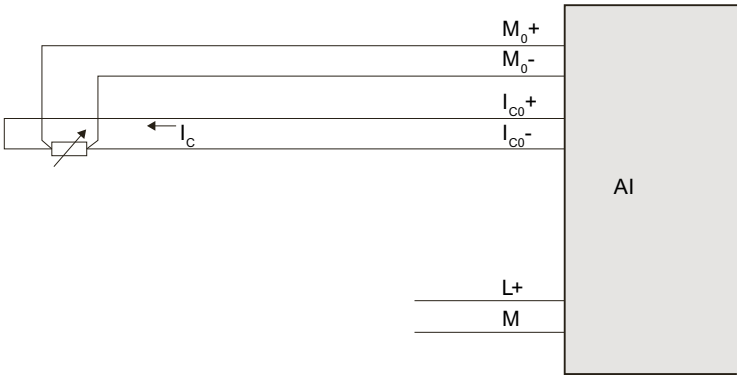


Figure 3-586 Example: 4-wire connection of thermal resistor to an analog input module

3-wire connection of a thermal resistor

Depending on the module, for a 3-wire connection to modules with 4 terminals (per channel), you may need to insert a bridge between **M_0- and I_{C0}-** (see figure below) or between **M_0+ and I_{C0}+**. Always wire the **I_{C0}+** and **M_0+** lines directly to the thermal resistor. Use cable with wires with identical cross-section.

For ET 200AL, ET 200eco PN and ET 200pro, no bridge is required as all necessary connections are implemented internally.

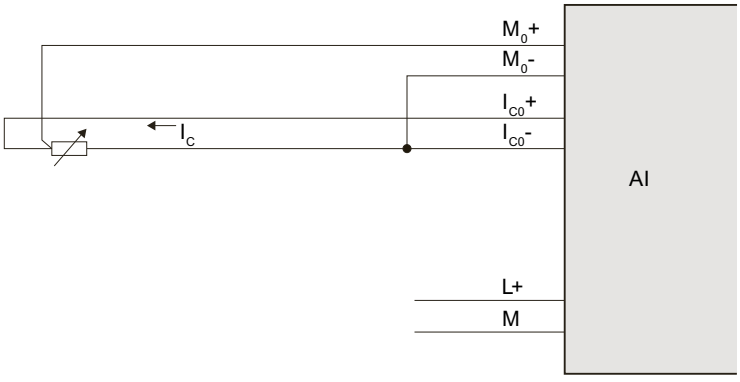


Figure 3-587 Example: 3-wire connection of thermal resistor to an analog input module

2-wire connection of a thermal resistor

When installing a 2-wire device on modules with 4 terminals (per channel), you will need to insert bridges at the module between **M_0+ and I_{C0}+** and between **M_0- and I_{C0}-** as shown in the figure below. The line resistance is measured, but not compensated. As a result of physical limitations, this measurement type is less accurate than measurement with 3-wire or 4-wire connections. The wiring for this type of measurement is, however, simple as the bridges required can be wired in the plug, saving line.

For ET 200AL, ET 200eco PN and ET 200pro, no bridge is required as all necessary connections are implemented internally.

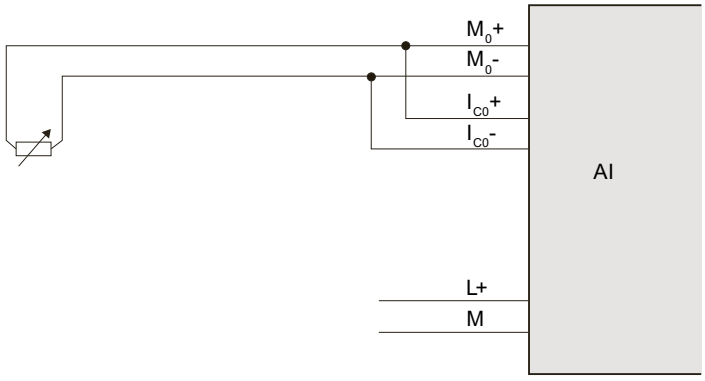


Figure 3-588 Example: 2-wire connection of thermal resistor to an analog input module

4.7 Wiring thermocouples

Introduction

Thermocouples are generally supplied ready-to-use. Protective casing prevents the thermocouples from being destroyed by mechanical force, for example.

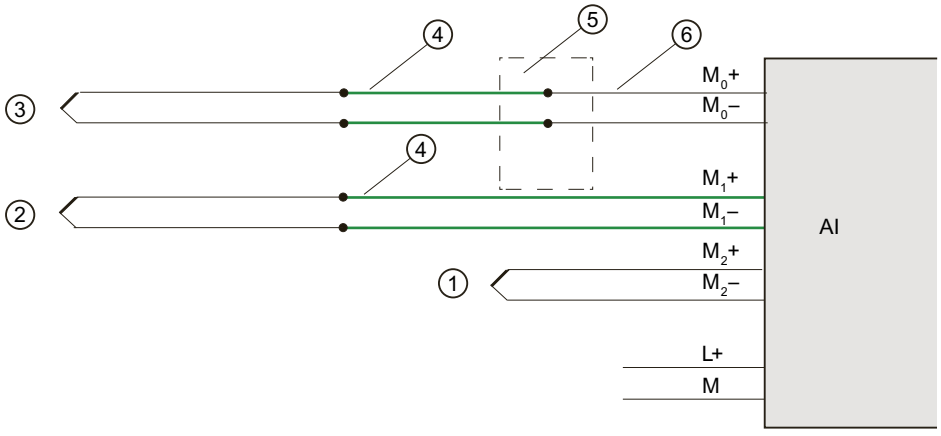
Compensating lines

The compensating lines belonging to the respective thermocouples are identified by a special color code, because only the compensating line that is made of the material matching the thermocouple may be used. The standardized compensating lines are specified in DIN EN 60584. Observe the maximum temperatures in the manufacturer's specifications.

Thermocouple connection options

There are various different ways to wire thermocouples to an analog input module:

- Directly ①.
- Using compensating lines ②.
- With a compensating line to the reference junction, connected with a supply line, e.g. copper ③.



① Thermocouple without compensating line
② Thermocouple with compensating line
③ Thermocouple with compensating line and supply line
④ Compensating line (same material as thermocouple)
⑤ External reference junction
⑥ Copper supply cable, for example

Figure 3-589 Example: Wiring thermocouples to an analog input module

Further information

Further information, such as the selection of thermocouples and how they operate, can be found in the section Thermocouples (Page 65).

Thermocouples

5

5.1 Selecting thermocouples

Introduction

Thermocouples are electrical devices for precise temperature measurement. They consist of two different metals connected at one point. Temperature affecting this point generates a voltage difference from which the temperature can be calculated.

Thermocouples can measure a wide range of temperatures and come in extremely robust models. They are therefore frequently used in industrial applications. Below are some of the criteria to consider when selecting the right thermocouple:

- Temperature range
- Atmospheric conditions
- Price

Grounded thermocouples

In grounded thermocouples, a conductive thermocouple wire is attached to the inside of the sensor housing. This results in good heat transfer from the sensor housing to the thermocouple measuring tip.

Non-grounded thermocouples

In non-grounded thermocouples, the thermocouple is not connected to the sensor housing. The response time following temperature changes is longer than with grounded thermocouples. The measuring point is galvanically isolated.

Type and temperature range

The different thermocouple types are derived from different material compositions.

NOTE

Due to physical conditions, thermocouples are extremely inaccurate outside the specified temperature range. Only use thermocouple in the temperature range specified by the manufacturer.

The following table lists the types and material compositions, as well as the temperature measuring range of different thermocouples:

Type	Material composition	Temperature range
B	PtRh-PtRh	250 to 1820 °C
C	W-Re	0 to 2315 °C
E	NiCr-CuNi	-270 to 1000 °C
J	Fe-CuNi	-210 to 1200 °C
K	NiCr-Ni	-270 to 1372 °C
L	Fe-CuNi	-200 to 900 °C
N	NiCrSi-NiSi	-270 to 1300 °C
R	PtRh-Pt (Pt 13%)	- 50 to 1769 °C
S	PtRh-Pt (Pt 10%)	-50 to 1769 °C
T	Cu-CuNi	-270 to 400 °C
U	Cu-CuNi	-200 to 600 °C
TXK/XKL	NiCr-CuCr	-200 to 800 °C

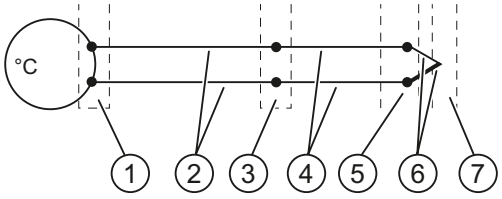
5.2 Structure and operating principle of thermocouples

Thermocouple structure

A thermocouple consists of a pair of thermal sensors and the respective installation and wiring elements. Two wires made of different metals/alloys are welded together at their ends (hot end). The welding point forms the so-called measuring point, while the free ends of the thermocouple form the reference junction.

The free ends are interconnected with the evaluation device (e.g. analog input module) via insulated wires or cables.

The different thermocouple types, e.g. K/J/N, are derived from different material composition; the same measuring principle is applied to all thermocouples, independent on their type.



① Thermal voltage acquisition point
② Copper supply cable, for example
③ Reference junction
④ Compensating line (same material as thermocouple)
⑤ Connection point
⑥ Thermocouple with positive and negative thermal elements
⑦ Measurement point

Figure 3-590 Thermocouple

Operating principle of thermocouples

Temperature differences between the measuring point and the free ends of the pair of thermal sensors (connection point) generate a thermal voltage at the reference junction. The value of the thermal voltage is determined by the temperature difference between the measuring point and the free ends, as well as by the material composition of the pair of thermal sensors.

Thermocouples always acquire a differential temperature, which means that the temperature at their free ends (reference junction) must be known to determine the temperature at the measuring point.

The thermocouple can be extended with compensating lines from the connection point. This allows the reference junction to be located at a specific point, for example, where the temperature can be kept constant or the temperature sensor is easy to install. The compensating lines and thermocouple wires are made of the same material. Copper cables are used to connect the reference junction to the module.

NOTE

Always observe the polarity, as incorrect wiring will result in unacceptable measuring errors.

5.3 Compensation for the reference junction temperature

5.3.1 Overview

Introduction

You have several options for measuring the reference junction temperature in order to obtain a correct temperature value as a function of the temperature difference between the reference junction and the measuring point.

You have various compensation options to suit requirements at the location of the reference junction.

The compensation options supported by the analog module used are specified in the manual of the respective module.

Options of compensating for the reference junction temperature

Table 3-101 Compensation options: Explanation and use case

Compensation options	Explanation	Use case / special feature
Internal reference junction	**Function principle** With this type of compensation, the temperature of the reference junction is measured using an integrated sensor in the analog module. **Procedure** Connect the thermocouple to the I/O module directly, or with compensating lines; see chapter Compensation with internal reference junction (Page 70).	• For the connection, use compensating lines that match the thermocouple material. • If the reference junction temperature and the module temperature are identical in your system, you may also use lines made from a different material. • Advantages: – Inexpensive – No external reference junction required – No additional wiring required
Reference channel of the module	**Properties** With this type of compensation, the reference junction temperature is determined using an external thermal resistor (RTD). **Procedure** Connect the thermocouple to the supply lines directly at the reference junction, or indirectly using compensating lines. Wire the supply lines to the corresponding terminals of the module. Wire the thermal resistor (RTD) to the reference channel of the module. The thermal resistor (RTD) must be positioned in the area of the reference junction; see chapter Compensation with reference channel of the module (Page 71).	• They acquire the temperature directly at the reference junction. • The measured temperatures of all channels that you have configured for this compensation type will be corrected automatically by the temperature value of the reference junction. • Advantages: – More precise compared to compensation with internal reference junction; however, you need to install and wire an additional thermal resistor.
Reference channel of group 0	**Properties** With the "TC" (thermocouple...) setting, the channel acts as receiver for the reference junction temperature of group 0. The associated transmitter of group 0 is set up to for the RTD channel. **Procedure** Connect the thermocouple to the supply lines directly at the reference junction, or indirectly using compensating lines. Wire the supply lines to the corresponding terminals of the module. Wire the thermal resistor (RTD) to the configured reference channel for group 0 of the module. The thermal resistor (RTD) must be positioned in the area of the reference junction; see chapter Compensation, reference channel of Group 0 (Page 73).	• They acquire the temperature directly at the reference junction. • The measured temperatures of all channels that you have configured for this compensation type will be corrected automatically by the temperature value of the reference junction (transmitter).

Compensation options	Explanation	Use case / special feature
Fixed reference temperature	**Properties** With this type of compensation, the reference junction temperature is stored in the module as fixed value. **Procedure** Connect the thermocouple to the supply lines directly at the reference junction, or indirectly using compensating lines. Wire the supply lines to the corresponding terminals of the module. Depending on the module, you can enter a fixed reference junction temperature in the configuration data (e.g. 20 °C), or use the fixed reference junction temperature of the module (0 °C); see chapter Compensation with fixed reference temperature (Page 75).	• You keep the reference junction temperature constant and know the temperature value. • To ensure high precision, you must ensure that the temperature remains constant (this can be complicated, depending on the application).
Dynamic reference temperature	**Properties** With this type of compensation, the reference junction temperature is determined using a module. Transfer this temperature value to other modules in the user program by means of a data record. **Procedure** Wire the thermal resistor (RTD) for the reference junction to any channel. The reference junction temperature is transferred with a function block by means of data records from the CPU or IM to the module, see section Compensation by means of dynamic reference temperature (Page 77).	• You are using multiple modules at the reference junction and can therefore compensate for all channels using a common temperature value. • You only need a thermal resistor (RTD) or a thermocouple to measure the temperature value.
No/external compensation	**Properties** With this type of compensation, the reference junction temperature is measured outside the analog input module. You can, for example, connect a compensating box to the thermocouple for this purpose. **Procedure** Connect the compensating box with the connection module of the analog input module with copper cables, see section "None" or external compensation (Page 80).	• The temperature of the reference junction for this type of compensation is specified as 0 °C. This can be achieved by using a compensating box. A separate compensating box is required for each thermocouple. • Thermocouples of type B do not require a compensating box.
RTD (0)	**Properties** This compensation is based on a measurement of the resistance value of a Pt1000 at the clamping unit of a compensation connector or of an external resistance value Pt1000. **Procedure** Additional information about the connection options with and without compensation connector is available in the section Type of compensation RTD (0) (Page 82).	• The reference junction temperature is determined with resistance value of the Pt1000. • All channels of the analog input module that you select for this type of compensation receive the same reference junction temperature.

5.3.2 Compensation with internal reference junction

Function principle

The reference junction for compensation via internal reference junction is at the terminals of the analog input module. Wire the thermocouples or compensating lines directly to the module inputs. The internal temperature sensor acquires the module temperature and returns a compensating voltage.

Note that compensation via internal reference junction will not always reach the precision of external compensation!

Procedure

Configuration steps:

1. Open the project in STEP 7.
2. In the device view, select the required analog module and the corresponding channel.
3. Select the "General" tab in the Inspector window of the selected module.
4. Select the "Inputs/Measuring" area.
5. Select the "Thermocouple" value as "Measurement type".
6. As "Reference junction", select the value "Internal reference junction".

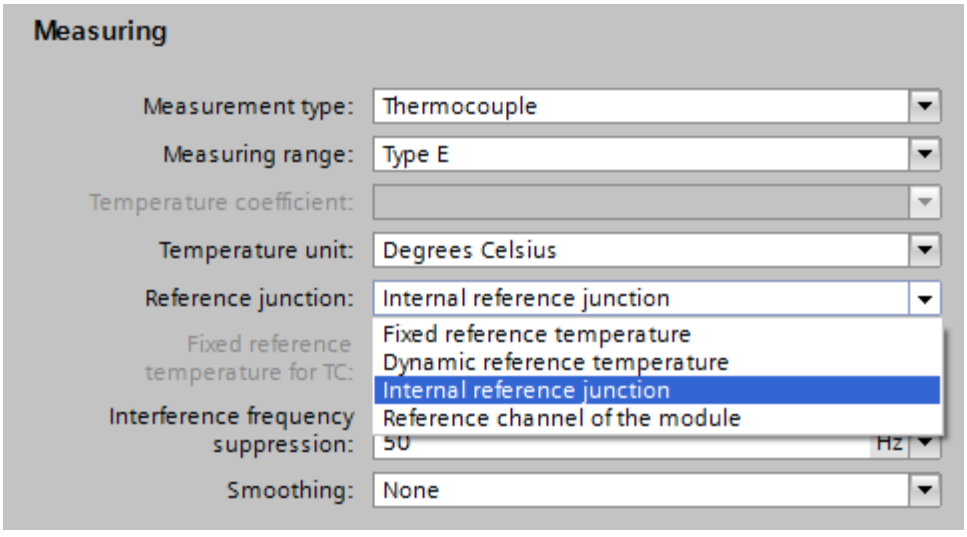
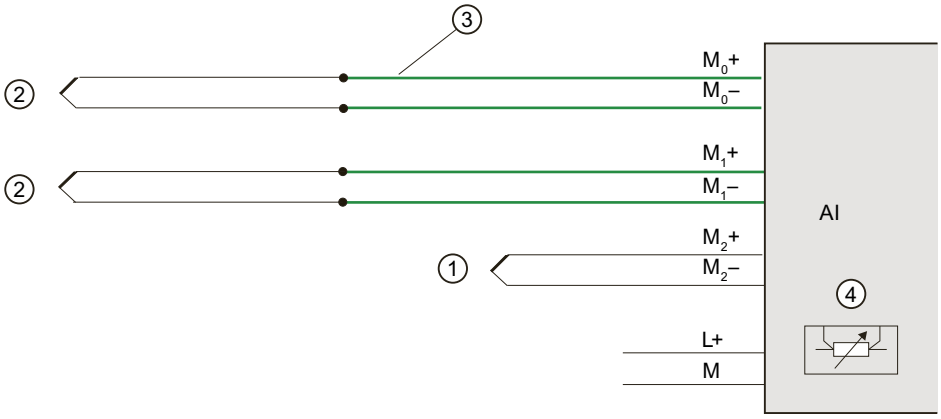


Figure 3-591 Internal reference junction

Wiring thermocouples

Wire the thermocouples directly or indirectly via compensating lines to the module inputs.



① Thermocouple without compensating line
② Thermocouple with compensating line
③ Compensating line (same material as thermocouple)
④ Internal reference junction

Figure 3-592 Example: Wiring thermocouples for compensation via internal reference junction

5.3.3 Compensation with reference channel of the module

Function principle

With this type of compensation, the reference junction temperature is determined using an external thermal resistor (RTD). Certain modules provide an internal reference channel.

Procedure

Configuration steps:

1. Open the project in STEP 7.
2. In the device view, select the required analog module and the corresponding channel.
3. Select the "General" tab in the Inspector window of the selected module.
4. Select the "Inputs/Measuring" area.
5. Select the "Thermocouple" value as "Measurement type".

6. As "Reference junction", select the value "Reference channel of the module"".

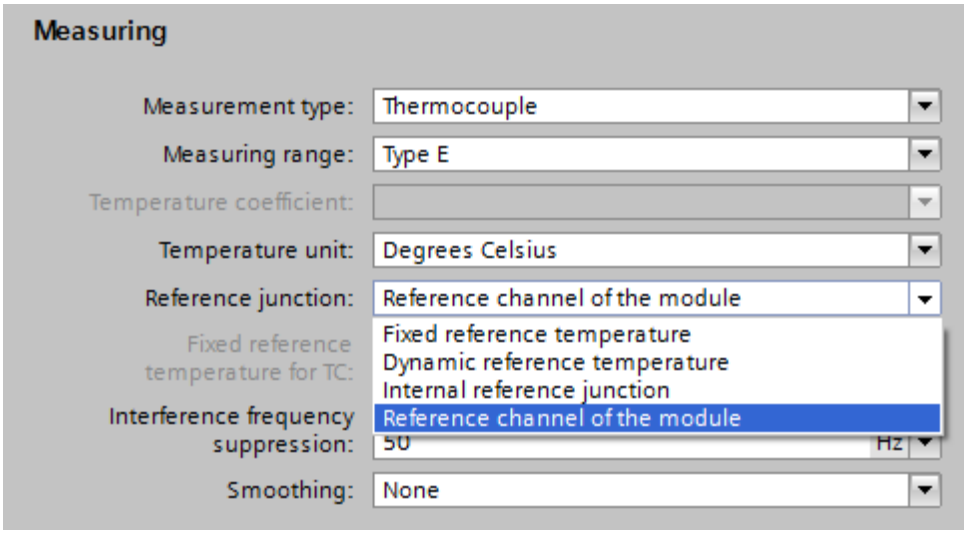
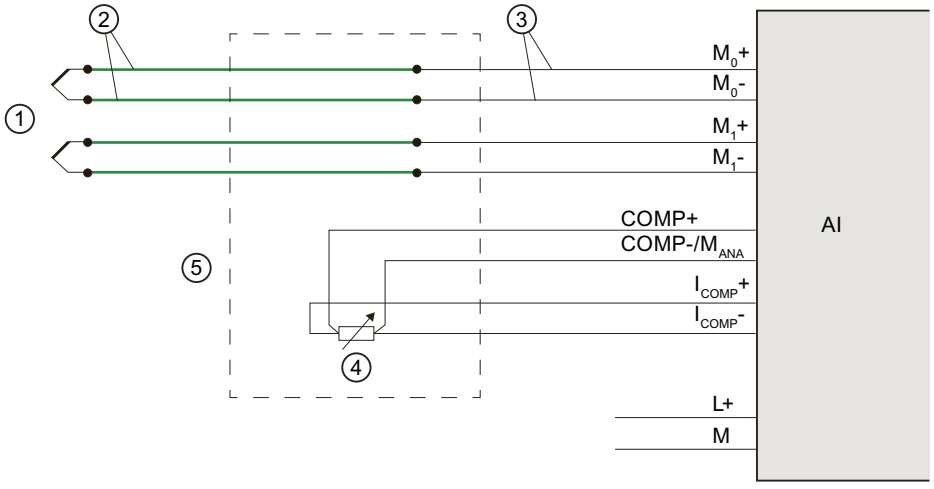


Figure 3-593 Reference channel of the module

Wiring thermocouples and thermal resistors

Connect the thermocouple to the supply lines directly at the reference junction, or indirectly using compensating lines. Wire the supply lines to the corresponding terminals of the module.

You may use cables made of any material to wire the thermal resistor to the module terminals.



① Thermocouple
② Compensating line (same material as thermocouple)
③ Copper supply cable, for example
④ Thermal resistor (RTD)
⑤ Reference junction

Figure 3-594 Example: Wiring thermocouples/thermal resistors for compensation by means of reference channel of the module

5.3.4 Compensation, reference channel of Group 0

Function principle

For this compensation, a module channel with a connected thermal resistor (RTD) acts as "Reference temperature transmitter". Other channels (reference temperature receivers) with connected thermocouples can be compensated using this reference temperature. The measured temperatures of all channels (receivers) that you have configured for this compensation type will be compensated automatically by the temperature value of the reference junction (transmitter).

The reference junction temperature is determined by means of an external thermal resistor (RTD).

Procedure

Configuration steps:

1. Open the project in STEP 7.
2. In the device view, select the required analog module and the corresponding channel.
3. Select the "General" tab in the Inspector window of the selected module.
4. Select the area "Inputs/measurement".
5. For the channel of the relevant module, specify as transmitter:
   As "Measurement type" select, for example, "Thermal resistor (4-wire connection)".
   As "Reference junction", select the value "Reference channel of group 0".

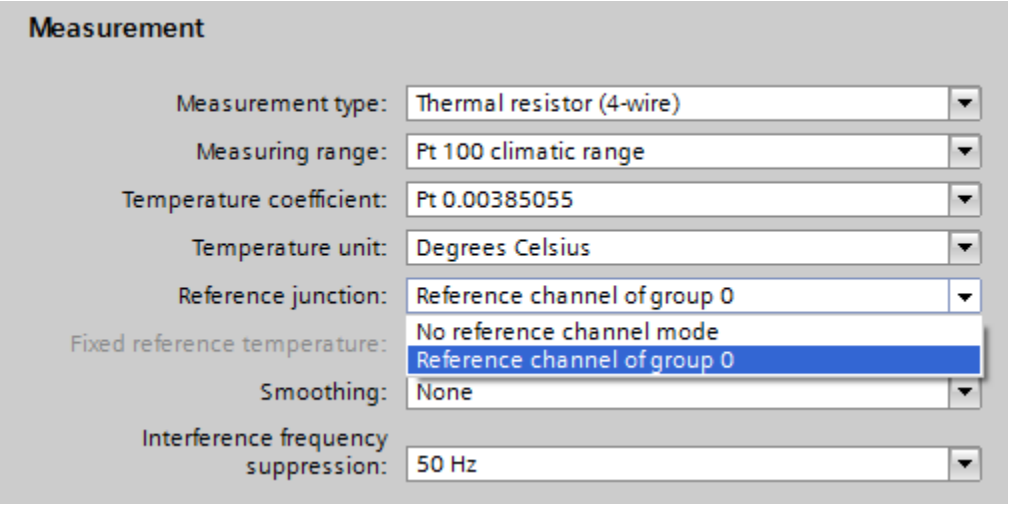


Figure 3-595 Transmitter: Reference channel of group 0

6. For the channels you specify as receivers:
   Select the "Thermocouple" value as "Measurement type".
   As "Reference junction", select the value "Reference channel of group 0".

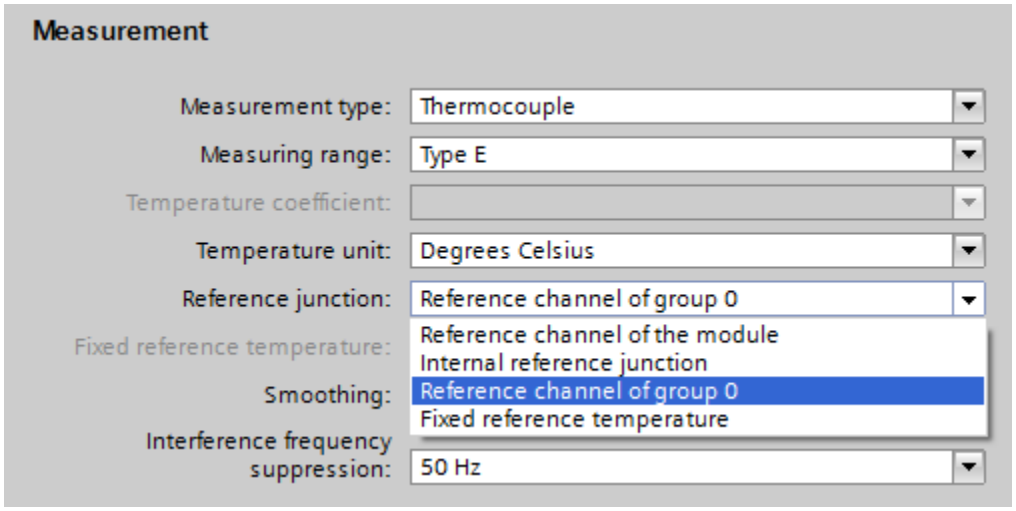


Figure 3-596 Receivers: Reference channel of group 0

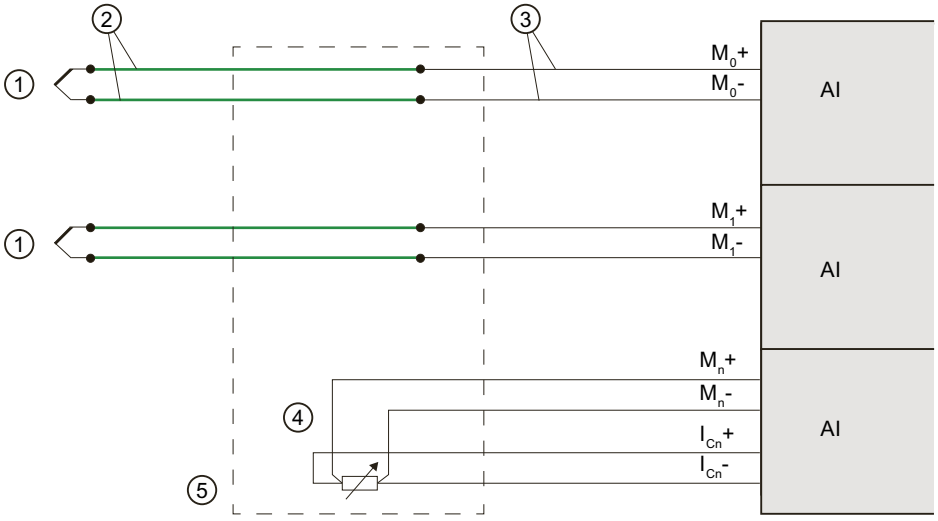
Connecting thermocouples and thermal resistors

The example below shows:

- An analog module with thermal resistor as reference temperature transmitter and
- Two analog modules with thermocouple as reference temperature receivers.

Connect the thermocouples to the supply lines at the reference junction, either directly or with compensating lines. Wire the supply lines to the corresponding terminals of the module.

You may use cables made of any material to wire the thermal resistor to the module terminals.



① Thermocouple
② Compensating line (same material as thermocouple)
③ Copper supply cable, for example
④ Thermal resistor (RTD)
⑤ Reference junction

Figure 3-597 Example: Connecting thermocouples/thermal resistors for group 0 compensation

5.3.5 Compensation with fixed reference temperature

Function principle

With this type of compensation, the reference junction temperature is stored in the module as fixed value.

Procedure

Configuration steps:

1. Open the project in STEP 7.
2. Select the required analog module in the Device view.
3. Select the "General" tab in the Inspector window of the selected module.
4. Select the "Inputs/Measuring" area.
5. Select the "Thermocouple" value as "Measurement type".
6. As "Reference junction", select the value "Fixed reference temperature".

7. Specify the temperature of the reference junction in the "Fixed reference temperature" area, for example, 20 °C.

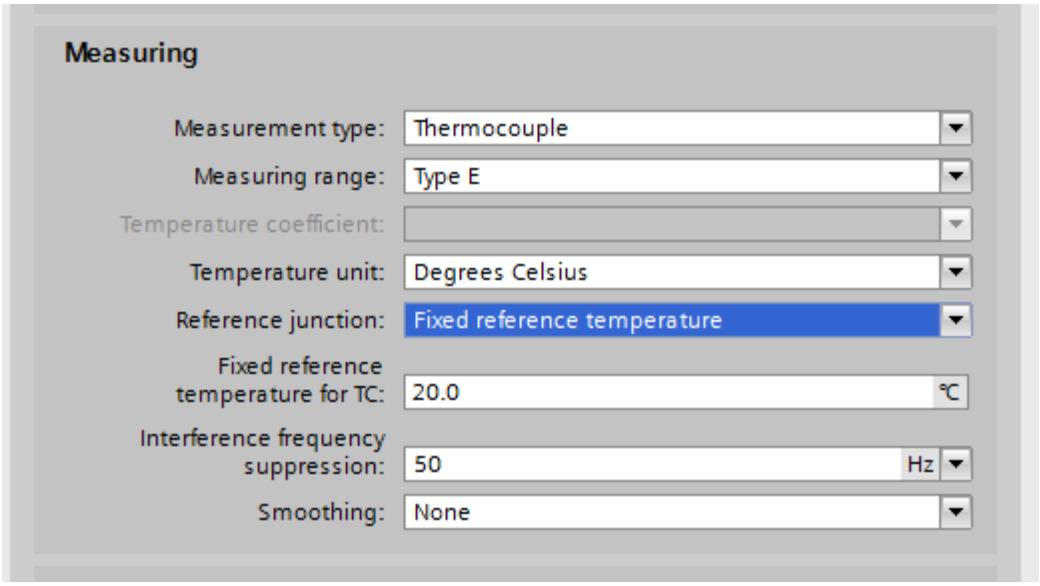
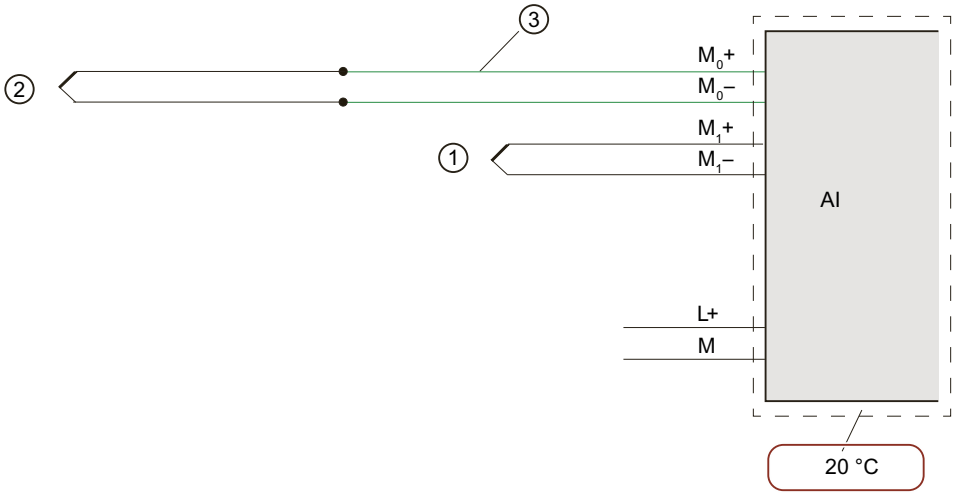


Figure 3-598 Fixed reference temperature

Temperature condition with "Fixed reference temperature" setting

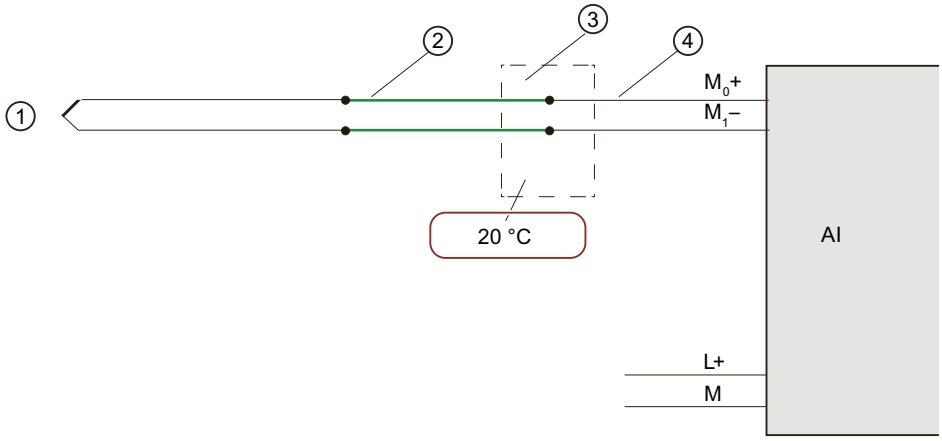
The figure below shows the connection options for thermocouples provided the temperature of the module is kept at a fixed reference temperature (20 °C), for example by installing it in an air-conditioned switch cabinet. The reference junction is in the module.



① Thermocouple without compensating line
② Thermocouple via compensating line
③ Compensating line (same material as thermocouple)

Figure 3-599 Example 1: Connecting a thermocouple to an analog module for compensation with "fixed reference temperature"

The figure below shows the connection options for thermocouples provided the temperature of the reference junction (outside the module) is kept at a fixed reference temperature (20 °C).



① Thermocouple with compensating line and supply line
② Compensating line (same material as thermocouple)
③ Reference junction
④ Copper supply cable, for example

Figure 3-600 Example 2: Connecting a thermocouple to an analog module for compensation with "fixed reference temperature"

5.3.6 Compensation by means of dynamic reference temperature

Function principle

This compensation type allows you to handle the reference junction temperature for temperature compensation in the user program. You can derive the temperature value from any other module of the station. The reference junction temperature is transferred via data records using the instruction **WRREC** (SFB 53).

The structure of the data records is detailed in the device manual for each module.

Requirement

STEP 7 project with the following contents:

- User program with WRREC (SFB 53) instruction for transferring the data records with reference temperature
- Analog module for acquisition of the process temperature using thermocouple (TC)
- Analog module for measuring the process temperature using thermal resistor (RTD)

Analog module for acquisition of the process temperature using thermocouple (TC)

Configuration steps:

1. Open the project in STEP 7.
2. In the device view, select the required analog module and the corresponding channel.
3. Select the "General" tab in the Inspector window of the selected module.
4. Select the "Inputs/Measuring" area.
5. Select the "Thermocouple" value as "Measurement type".
6. As "Reference junction", select the value "Dynamic reference temperature".

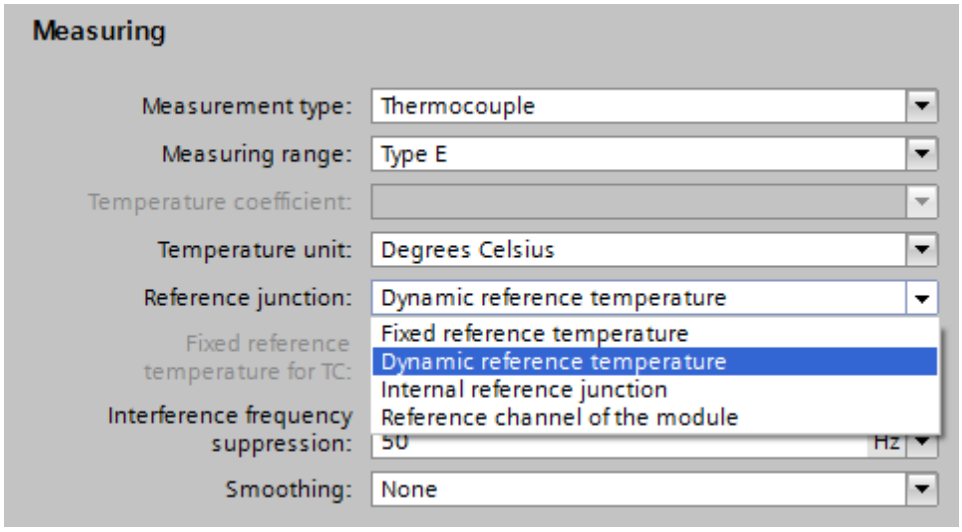


Figure 3-601 Dynamic reference temperature

Analog module for measuring the process temperature using thermal resistor (RTD)

Configuration steps:

1. Open the project in STEP 7.
2. In the device view, select the required analog module and the corresponding channel.
3. Select the "General" tab in the Inspector window of the selected module.
4. Select the "Inputs/Measuring" area.

5. Select the "Thermal resistor (4-wire connection)" value as "Measurement type".

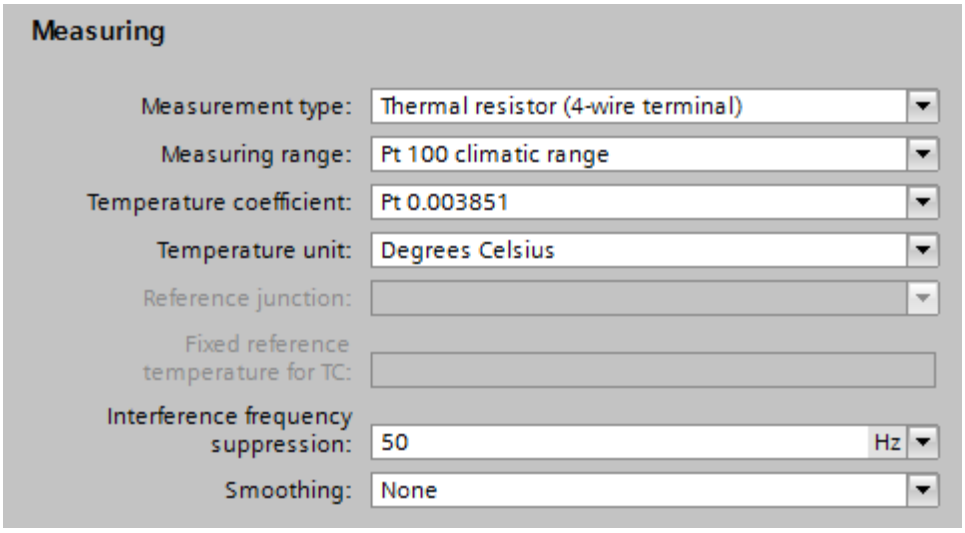
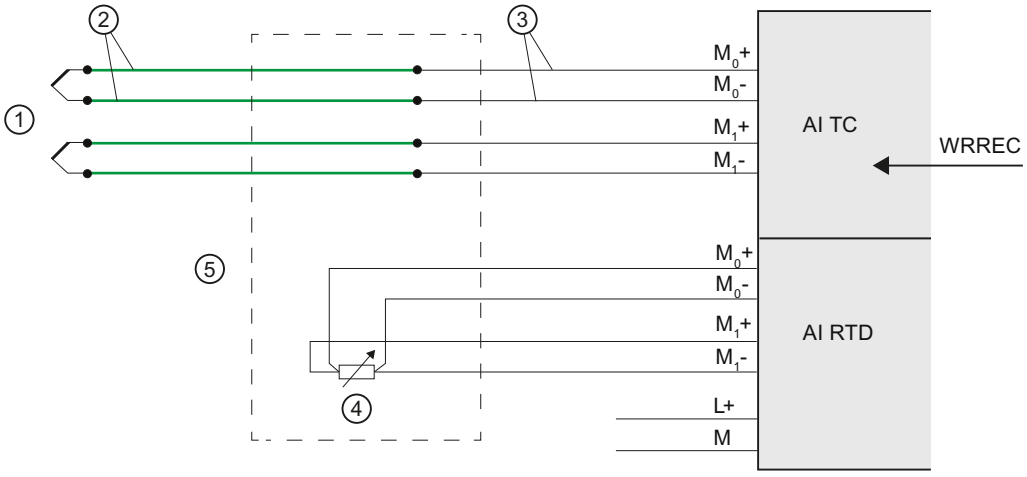


Figure 3-602 Settings for thermal resistor (RTD) type of measurement

Connecting thermocouples and thermal resistors

Connect the thermocouples, for example, to the module inputs using supply lines for temperature compensation with dynamic reference temperature. In this case, the temperature is acquired at the reference junction by means of a thermal resistor (RTD). This reference junction temperature determined in this way is transferred to the analog module with thermocouple via data records with the WRREC instruction.



① Thermocouple
② Compensating line (same material as thermocouple)
③ Copper supply cable, for example
④ Thermal resistor (RTD)
⑤ Reference junction

Figure 3-603 Example: Connecting thermocouples/thermal resistors for compensation by means of dynamic reference temperature

5.3.7 "None" or external compensation

Function principle

The reference junction temperature of the thermocouples is measured outside the analog input module, e.g., by means of a compensating box on the thermocouple. The temperature of the reference junction for this type of compensation is specified as 0° C.

The compensating box includes a bridge circuit that is calibrated for a specific reference junction temperature (compensation temperature). The connectors for the ends of the compensating line of the thermocouple form the reference junction. If the actual comparison temperature deviates from the compensation temperature, the temperature-dependent bridge resistor changes. A positive or negative compensation voltage is generated and added to the thermal voltage.

NOTE

Thermocouples of type B do not require a compensating box.

Procedure

Configuration steps:

1. Open the project in STEP 7.
2. Select the required analog module in the Device view.
3. Select the "Inputs" tab in the Inspector window of the selected module and the respective channel.
4. Select the "Thermocouple" value as "Measurement type" in the "Measuring" area.
5. As "Reference junction", select the value "None" or "External compensation" depending on the used module.

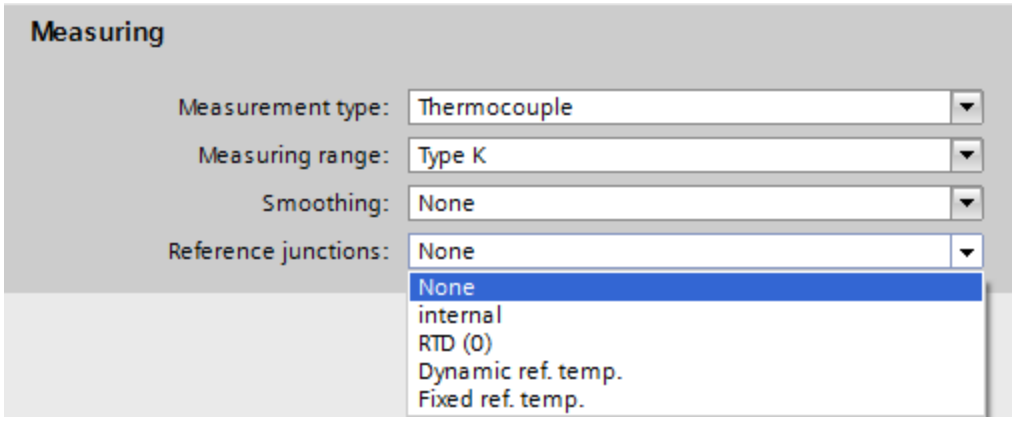


Figure 3-604 No reference junction

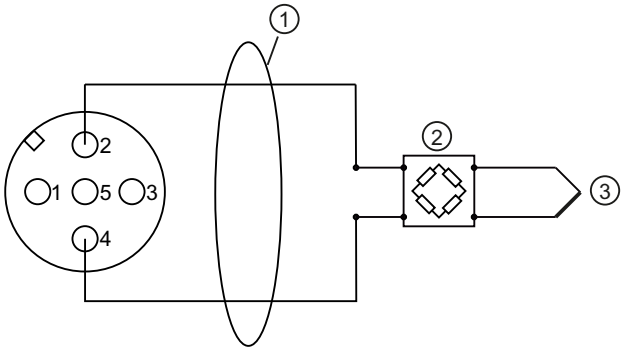
Connection of the compensating box

The compensating box is looped into the supply lines of an individual thermocouple. The compensating box must be supplied isolated. The power supply unit must have a sufficient noise filter, e.g., by means of a grounded shielding winding.

Each channel can use its own thermocouple type supported by the analog module regardless of the other channels. A separate compensating box is required for each channel.

Connection example "None" or external compensation

Connect the compensating box with the connection module of the analog input module using copper cables.



① Copper cables
② Compensating box (per channel), for example; thermocouple type B does not require a compensating box
③ Thermocouple

Figure 3-605 Connection example "No" compensation as reference junction

5.3.8 Compensation type RTD (0)

Function principle

The reference junction temperature is determined by means of the resistance value of a Pt 1000 at the clamping unit of the M12 compensation connector. The resistance measurement is only permitted at the X1 circular socket (channel 0). All of the module's channels with this type of compensation receive the same reference junction temperature.

Procedure

Configuration steps:

1. Open the project in STEP 7.
2. Select the required analog module in the Device view.
3. Select the "Inputs" tab in the Inspector window of the selected module.
4. Select the "Thermocouple" value as "Measurement type" in the "Measuring" area.

5. As "Reference junction", select the value "RTD (0)".

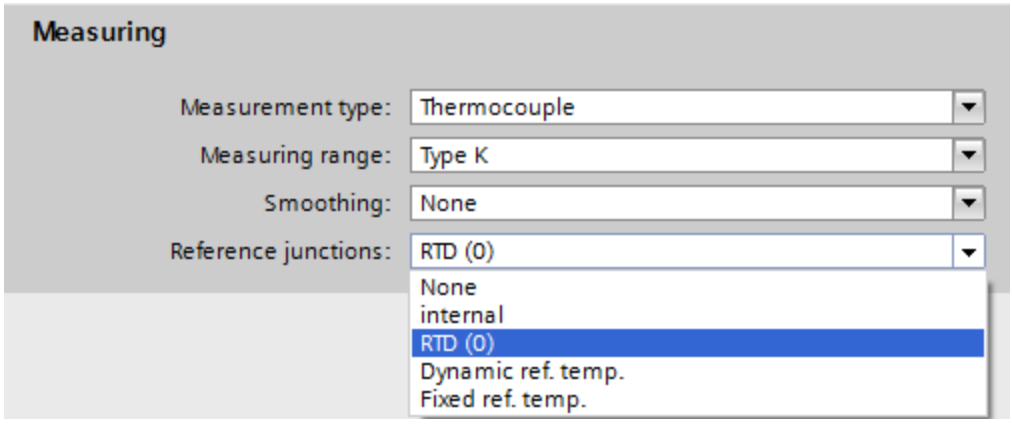


Figure 3-606 Compensation type RTD (0)

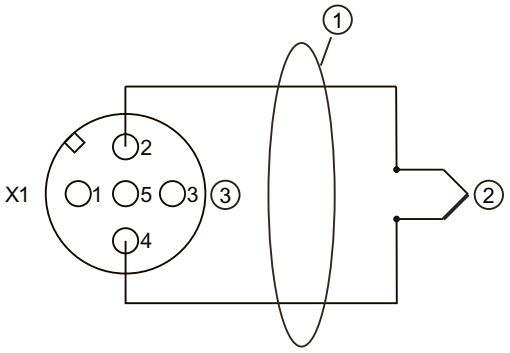
Connection example

Connection with M12 compensation connector
Connect the thermocouple to the M12 compensation connector directly or with compensating lines. Install the M12 compensation connector to the X1 circular socket (channel 0) of the CM IO 4 x M12 at the 4 AI TC High Feature.

Connection without M12 compensation connector
To measure the referent junction temperature, connect an external Pt1000 (with α = 003851) to terminals 1 and 3 using copper cables. The thermal resistor Pt1000 must be positioned in the area of the reference junction. Connect the thermocouples to terminals 2 and 4 from the reference junction with copper cables.

Connecting additional thermocouples
You can connect additional thermocouples to the circular sockets X2 to X4 on the CM IO 4 x M12 of the 4 AI TC High Feature. The temperature of reference junction collected by measuring the resistance value at the X1 circular socket applies to all channels of the module that you have selected for this type of compensation.

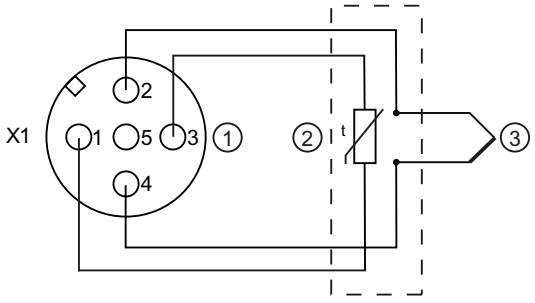
The figure below shows a connection example "RTD (0)" as reference junction with M12 compensation connector and integrated thermal resistor Pt1000:



① Direct connection of the thermocouple or with compensating lines
② Thermocouple
③ M12 compensation connector (terminals 1 and 3 with internal Pt1000) only at X1 circular socket. The comparison value of the M12 compensation connector at circular socket X1 also applies to thermocouples at X2, X3 and X4.

Figure 3-607 Connection example "RTD (0)" as reference junction in the M12 compensation connector

The figure below shows a connection example "RTD (0)" as reference junction with external thermal resistor Pt1000:



① M12 connector only at X1 circular socket
② External Pt1000 (α = 0.003851) in the area of the reference junction with copper cables at terminals 1 and 3. The comparison value of the external Pt1000 at circular socket X1 also applies to thermocouples at X2, X3 and X4.
③ Thermocouple

Figure 3-608 Connection example "RTD (0)" as reference junction with external Pt1000

Wiring loads/actuators

6

6.1 Overview

Introduction

This chapter describes the basic procedure for wiring loads/actuators to analog outputs. Information on specific wiring options is available in the manual of each module.

For detailed information on cable routing and shielding, potential equalization, etc. please refer to the function manual Configuring interference-free controllers (http://support.automation.siemens.com/WW/view/en/59193566).

Abbreviations used in the figures

Key to the abbreviations in the figures below:

AQ	Analog output module
M	Ground connection
L+	Supply voltage connection
S_n+/S_n-	Sense line channel n
QV_n+/QV_n-	Voltage output channel n
QI_n+/QI_n-	Current output channel n
M_{ANA}	Reference point of the analog ground
U_{ISO}	Insulation voltage

Lines for analog signals

Always use shielded twisted-pair cables to wire the analog signals. This improves immunity.

6.2 Wiring loads/actuators

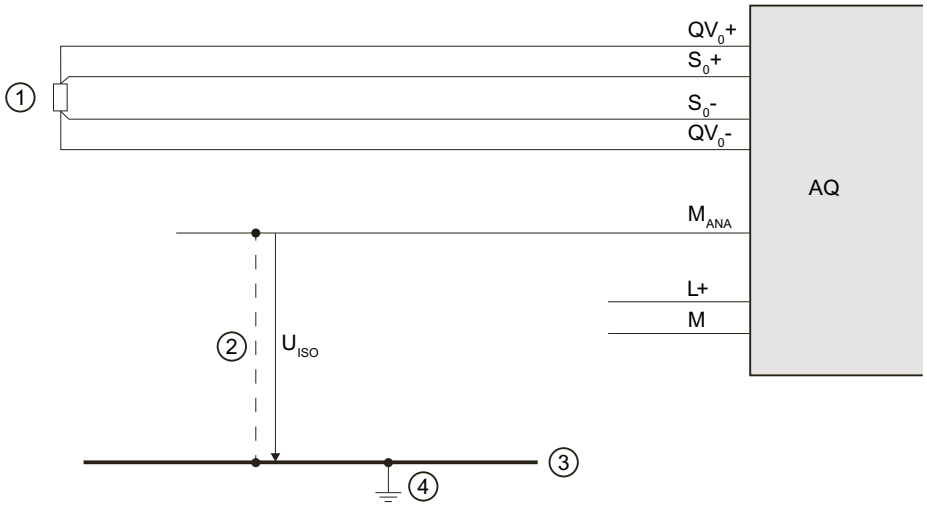
Reference potential for analog output modules with M_{ANA} connection

Analog output modules have no galvanic connection between the reference point of the analog ground M_{ANA} and the central ground.

Always verify that the admissible potential difference U_{ISO} between the reference point of the analog ground M_{ANA} and the central ground is not exceeded.

Potential difference U_{ISO} may be caused by: Maximum line lengths exceeded.

If you want to ensure the maximum value U_{ISO} is not exceeded, wire terminal M_{ANA} and the central ground with an equipotential bonding cable.



① Load on the voltage output
② Equipotential bonding cable
③ Grounding bus cable
④ Central ground

Figure 3-609 Example: Reference potential for an analog output module with M_{ANA} connection

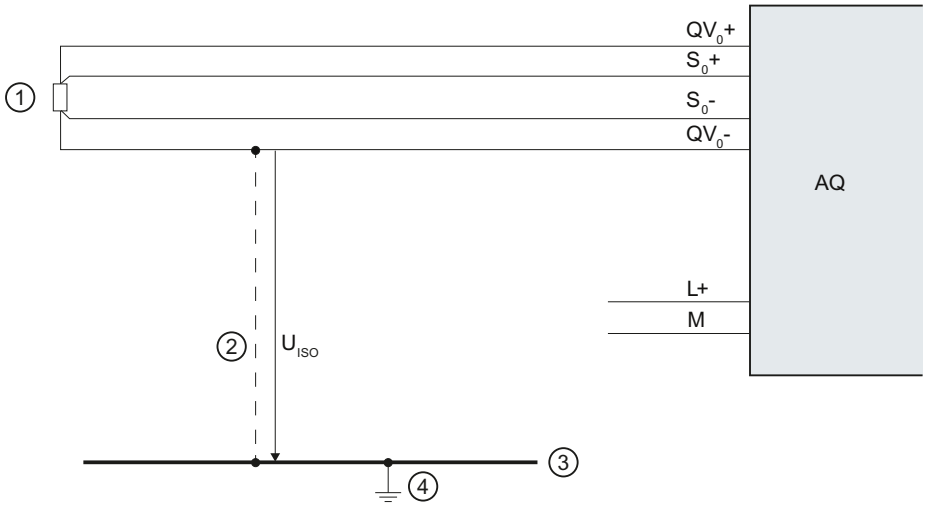
Reference potential for analog output modules without M_{ANA} connection

Analog output modules have no galvanic connection between the reference potential of the analog output circuits and central ground.

Always verify that the maximum potential difference U_{ISO} between the reference points of the analog output circuits and the central ground is not exceeded.

Potential difference U_{ISO} may be caused by: Maximum line lengths exceeded.

f you want to ensure the maximum value U_{ISO} is not exceeded, interconnect each analog output circuit with the central ground using an equipotential bonding cable.



① Load on the voltage output
② Equipotential bonding cable
③ Grounding bus cable
④ Central ground

Figure 3-610 Example: Reference potential for an analog output module without M_{ANA} connection

Supported functions

7

7.1 Calibrating analog modules

7.1.1 Overview

Calibration

A calibration checks the process values measured by the analog input module and the process values output by the analog output module, determines the deviation from the actual values and compensates for any measurement and output errors.

Calibrating analog modules

The SIMATIC analog modules were calibrated before being shipped and have excellent long-term stability; calibration is therefore not required during runtime.

But certain regulations and directives, for example from the Food and Drug Administration (FDA), require regular calibration for all components in a measuring circuit. These components include analog input and output modules.

A calibration makes sense especially for plants in which sensors detect and process relatively small voltages or currents. The calibration compensates for influences on the measuring result by cables and/or temperature.

The calibration collects the new values and saves them retentively on the module. But the calibration values determined prior to delivery at the plant are not lost. You can return to these original calibration values at any time.

NOTE

The calibration saves the calibration values of each channel for the specific measuring range retentively on the module, which means the values apply to the same measuring range in which the user calibration took place.

If you reconfigure a channel with effective user calibration values to another type of measuring mode, the calibration values saved at the plant for this channel and for this measuring range will become effective.

But the user calibration values are not deleted. They are not overwritten until there is a new user calibration of the channel. If you set the original measuring range for this channel once again without new user calibration, the previously determined user calibration values will become effective.

The respective manual will include information whether or not your analog module supports the "Calibration" functionality.

Scope of functions

The "Calibration" group offers the following functions:

- Specifying the current calibration of all channels
- Calibrating a channel
- Canceling a running calibration
- Resetting the calibration of a channel to the factory settings

7.1.2 Calibrating analog modules

Manual calibration

The following requirements must be met to start manual calibration:

- An online connection exists between STEP 7, the respective CPU and the analog module to be calibrated.
- You have opened the "Online & Diagnostics" view for the selected analog module from the shortcut menu of the project and you are now in the "Functions > Calibration" area.
- The configuration reflects the actual structure of the station.
- No calibration process is busy on the module (if you want to launch calibration).
- A 24 V load voltage must be present at each module for the calibration.
- The last step was successfully completed (if you want to continue or conclude calibration).

Procedure

The basic mask for calibration opens once you start the "Calibration" function. The module reads the following general information data and calibration values after each new selection of a channel:

- **Calibration:** Indicates whether or not the currently effective calibration values are factory calibration values or user calibration values.
- **Measurement type:** Information about the selected measurement type
- **Measuring range:** Currently configured measuring range of the selected channel
- **Gain:** Currently effective gain correction of the analog-digital converter
- **Offset:** Currently effective offset correction of the analog-digital converter

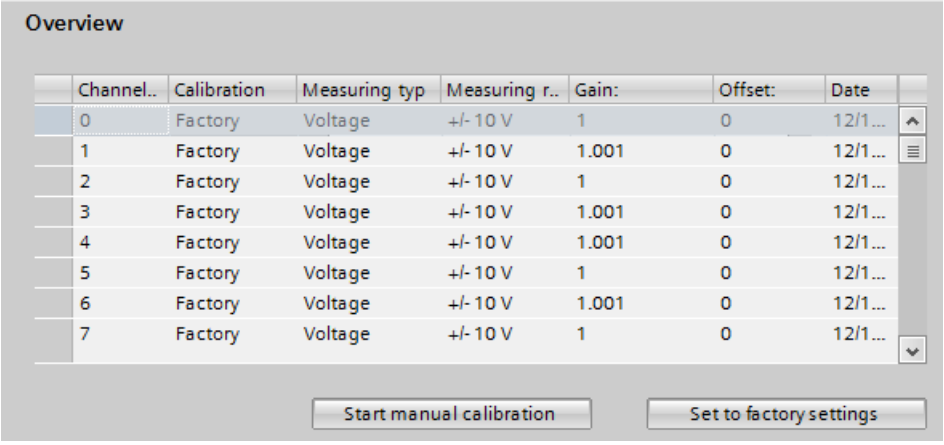


Figure 3-611 Calibration table

To start the calibration, follow these steps:

1. Select the line associated with the channel to be calibrated in the overview table.
2. Click the "Start manual calibration" button.
3. Now go through the steps in the "Manual calibration" section.
4. Follow the instructions in the "Command" field.
5. Click ""Next".

The required calibration values of the selected channel according to the measuring range configured for this channel are specified once again during the user calibration.

NOTE

The calibration can take place in RUN mode as well as STOP mode of the CPU. If the CPU is in RUN, the calibration value that was last collected prior to the start of the calibration is supplied for the duration of the calibration.
The module channel to be calibrated cannot process any new process values during the user calibration. All analog input values of the module are set to 0x7FFF ("Invalid analog value") until the end of the calibration. When the value status is enabled, the value status of the signal is set to "invalid" for the duration of the calibration.

You must provide a voltage and/or temperature during a user calibration. To do so, use the corresponding external wiring and an external voltage/temperature transducer. The field "Command" includes numbers of pins to which you can connect the calibration stimulus. The first pin number identifies the positive connector, the second pin number the negative connector. The accuracy of the calibration depends on the accuracy of the provided voltage/temperature.

NOTE

To ensure that the module retains the specified measuring accuracy after the user calibration, the provided voltage/temperature must be twice as accurate as specified for the module. Inaccurate voltages or temperature result in a faulty calibration.

The figure below shows an example of channel calibration with "Voltage" measurement, measuring range "+/- 10 V".

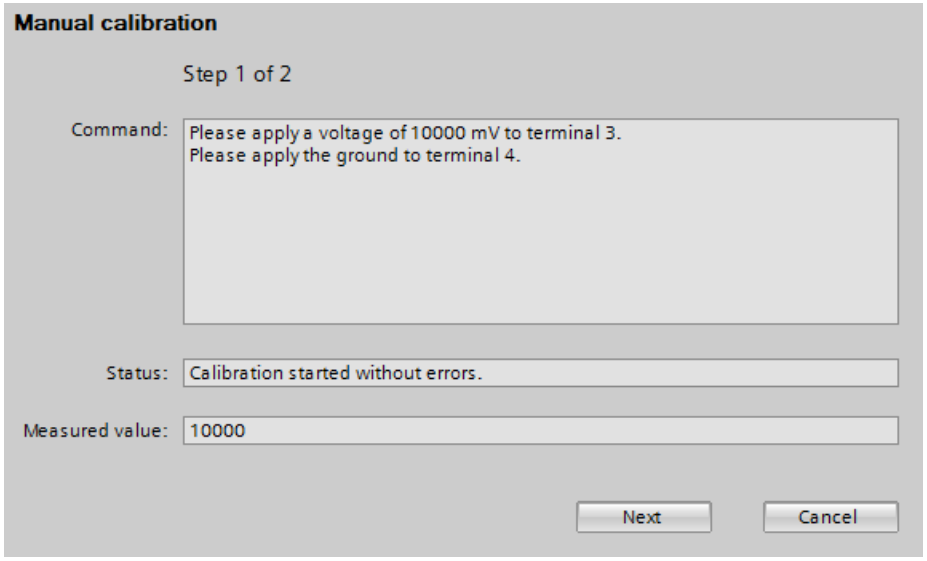


Figure 3-612 Manual calibration

- **Command:** The field "Command" indicates which actions the user has to execute during the current calibration step. Here you execute the specified actions and confirm them with the "Next" button. The module now executes all actions required for the current calibration step. If the calibration step was error-free, the next calibration step takes place. The instructions in the "Command" field are to be performed additively. For example, after you have applied the voltage/ground to the terminals 3/4, these connections must remain in place during the execution of the next calibration step.
- **Status:** Depending on the set type of measurement, several calibration steps are required for calibration of a channel. The field "Status" indicates whether or not the last calibration step included errors. If an error occurs during processing of a calibration step, the error is displayed here and calibration of the channel is aborted. All calibration values recorded up to this point are deleted. The calibration values that were in effect prior to the start of the user calibration are effective once again.

NOTE

Calibrators

If the "Wire break" diagnostics is activated for analog input modules, a test current is applied to the line for the measuring types "Resistance", "Thermistor" and "Thermocouple". This applied test current can result in inaccurate measured values in some calibrators. The wire break monitoring is therefore automatically disabled in some analog modules during the calibration.

To avoid the risk of inaccurate measured values, we recommend you disable the "Wire break" diagnostics during the calibration of analog input modules.

Result

Calibration sets new settings for the channel.

Error occurrence

If an error occurs during the calibration, the module cancels the calibration. All calibration values recorded up to this point are lost. The channel to be calibrated will then have the same settings as before the start of calibration.

7.1.3 Canceling a calibration

Requirement

- You have opened the "Online & Diagnostics" view for the selected analog module from the shortcut menu of the project and you are now in the "Functions > Calibration" area.
- The associated CPU is online.
- A calibration is currently running on the analog module.

Procedure

Click the "Cancel" button to cancel an ongoing calibration.

Result

The active calibration is canceled. The channel to be calibrated will then have the same settings as before the start of calibration.

7.1.4 Resetting analog modules to factory settings

Requirement

- You have opened the "Online & Diagnostics" view for the selected analog module from the shortcut menu of the project and you are now in the "Functions > Calibration" area.
- The associated CPU is online.

Procedure

Proceed as follows to reset the channel of an analog module to factory settings:

1. In the overview table, select the line of the channel to be calibrated.
2. Click the "Set to factory settings" button.

Result

The factory settings of the channel are restored.

NOTE

When you reset the current channel to the factory settings, the original calibration values that were saved in the delivery state of the module become effective once again. Any existing user calibration values of this channel are lost. You cannot restore these user calibration values.

High-speed analog modules

8

8.1 Basics

High-Speed analog modules (HS) are available for users with high demands regarding performance and speed. The main characteristics of these HS analog modules compared to Standard analog modules (ST) is their shorter cycle times. To achieve this goal, the input and output modules are equipped with components with extremely short throughput and conversion times. In addition, the entire architecture of the modules is designed for faster signal processing.

HS analog modules convert the output of measured values and output values at the same time. Each channel within the module has its own A/D or D/A converter. This means the cycle time is basically the conversion time and independent of the number of activated channels. This is true for analog input modules as well as analog output modules. This means HS modules can be used in fast isochronous mode.

Apart from isochronous mode, the HS analog modules also provide benefits in non-isochronous (free-running) mode. Due to the fast processing of the process signals, HS analog modules are able to detect changes in the process values more quickly and to respond to these events with the appropriate program blocks (for example, hardware interrupt or cyclic interrupt organization blocks). Additional information on the various organizational blocks can be found in the STEP 7 online help.

Isochronous mode

Isochronous mode refers to synchronous coupling:

- Of signal acquisition and output via the distributed I/O
- Of signal transmission via PROFIBUS or PROFINET
- Of program processing with the constant bus cycle time of PROFIBUS or PROFINET.

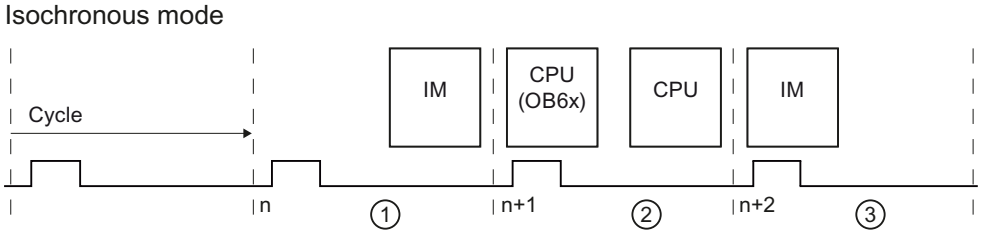
The result is a system that acquires its input signals in constant time intervals, processes them and outputs the output signals. Isochronous mode guarantees reproducible and defined process reaction times as well as equidistant and synchronous signal processing with distributed I/O.

The bus system and the I/O modules work synchronously with configured isochronous mode. The transmitted input and output data are linked to an "isochronous task" in the CPU. As a result, the data of a cycle are always consistent. All data of a process image belong together logically and in time. Jitter in the user program caused by the acquisition of outdated values is therefore almost impossible.

Even fast processes can be perfectly controlled by the exact timing reproducibility of all processes. Isochronous mode thus contributes to high control quality and hence to greater manufacturing precision. While possible fluctuations of the process reaction times are drastically reduced. The time-assured processing can be utilized to improve machine cycle times. Shorter cycle times increase the processing speed and help to lower production costs.

Send clocks

When you configure isochronous mode, the input and output data is synchronized within a send clock (cycle). The data of the input modules is acquired in cycle n and simultaneously transferred to the IM. The data is available in cycle n+1 in the CPU and can be processed. The CPU copies the data to the IM in the next cycle n+2. The output modules then output the data simultaneously in the same send clock. The acquisition – processing – output therefore takes place in three cycles. You can find more information on the configuration of isochronous mode in the STEP 7 online help.



① Measured values of the input modules are acquired and copied to the IM
② Measured values are processed and output values determined
③ Output values are copied to the IM and output by output modules

Figure 3-613 3-cycle model

Oversampling

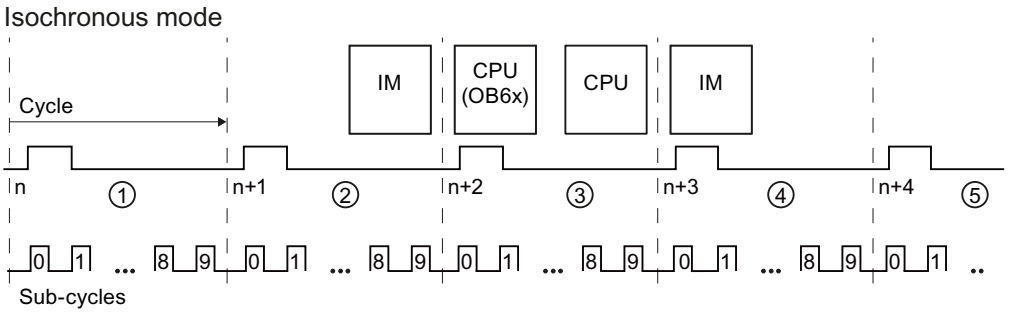
The use of the oversampling function in analog input or analog output modules requires an isochronous configuration.

With analog input modules, the set send clock is divided into time-equidistant sub-cycles. The send clocks can be subdivided into 2 to 16 sub-cycles. Each sub-cycle reads in a measured value. The read-in measured values of a data cycle are copied to the IM in the next send clock and are then available to the processing CPU one send clock later.

With analog output modules, the set send clock is also divided into time-equidistant sub-cycles. The send clocks can be subdivided into 2 to 16 sub-cycles. Each sub-cycle returns an output value. The output values are copied to the IM by the CPU within the same send clock and are written to the process one send clock later.

The read-in and output values are transmitted in the user data of the analog module. This way, the address space of the module is extended from 2 bytes of user data per channel to 16 x 2 bytes of user data per channel. If you subdivide the send clock into less than 16 sub-cycles, the unused addresses are assigned the error value 0x7FFF during input. For output, the values of the unused addresses are ignored.

Because the sub-cycles have to be within a send clock, oversampling needs an additional send clock to copy the data to the IM, unlike the 3-cycle model of isochronous mode. The result is a 5-cycle model.



① Send clock is divided into sub-cycles which record the measured value
② Measured values are copied to the IM
③ Measured values are processed and output values determined
④ Output values are copied by the CPU to the IM
⑤ Output values are written to the process

Figure 3-614 5-cycle model

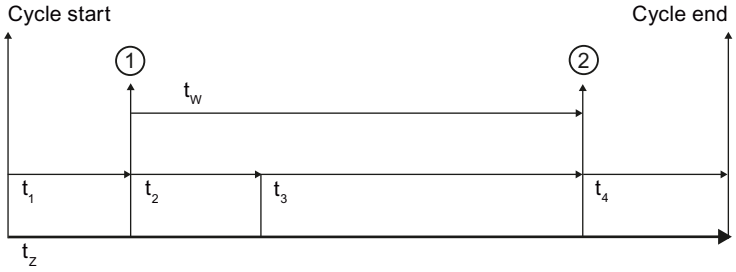
Due to the configured modules, the send clock of an IO device has a minimum possible update time, which means the time interval within which an IO device/IO controller of the PROFINET IO system is supplied with new data. Modules with oversampling functionality, however, offer the option of further reducing the update time for their channels without having to shorten the send clock for the entire S7 station at the same time. The subdivision of the send clock into time-equidistant sub-cycles therefore enables an even faster signal processing speed.

Example
In practice, the use of oversampling makes sense when the isochronous system works with only one specific specific send clock (for example, 1 ms) due to the modules used and when faster sampling of the process values is required. By using oversampling and a subdivision of the send clock into 4 sub-cycles, for example, you can sample the process values in intervals of 250 µs.

Configuring oversampling
Enable the option "Isochronous mode" in the IO device used and set the corresponding parameters ("Send clock", etc.). You define the number of sub-cycles in the relevant distributed analog module with the "Sampling rate" parameter for analog input modules and the "Output rate" parameter for analog output modules. If, for example, you configure a "Sampling rate" of 4 "Values/cycle" for a "Send clock" of 1 ms, the send clock is subdivided into 4 sub-cycles and the process values are sampled in intervals of 250 µs.

Cycle time of an analog input module

If you have configured the system property "Isochronous mode" for HS modules, all analog input modules are synchronized to a shared time within the send clock (cycle) ①. The cycle time is made up of the following time intervals: $t_Z = t_1 + t_2 + t_3 + t_4$



① Synchronization time for all analog input modules in isochronous mode and simultaneously time of the converted input signal at the terminal in this cycle

② Digitalized input signal is transferred to the backplane bus

t_Z Cycle time

t_1 Time between cycle start and synchronization

t_2 Hardware-related runtime up to the analog-digital converter

t_3 Processing time of digitalized input data in the module

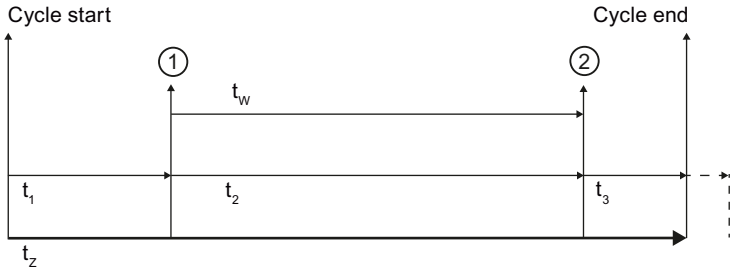
t_4 Transfer time of the backplane bus

t_W Conversion time of the module

Figure 3-615 Cycle time of the analog input module

Cycle time of an analog output module

The synchronization time for analog output modules refers to the output of the digital-analog converter ②. Because the impedance of the connected actuator including connection cable is unknown in output modules but has a significant impact on the signal run time, the settling time cannot be added as a fixed value. The respective manuals of the output modules specify the typical load settling times as reference point. But in practice, a measurement with an oscilloscope is required for a precise measurement of the settling time. The settling time may exceed the actual end of the cycle due to very short cycle times and very high capacitive loads. The cycle time is made up of the following time intervals: $t_Z = t_1 + t_2 + t_3$



① Output data is available in digital form in the module

② Synchronization time for all analog output modules in isochronous mode and simultaneously output time of data in the digital-analog converter

t_Z Cycle time

t_1 Transfer time of the backplane bus

t_2 Processing time of data in the module until output at digital-analog converter

t_3 Settling time of hardware until setpoint of output value

t_W Conversion time of the module

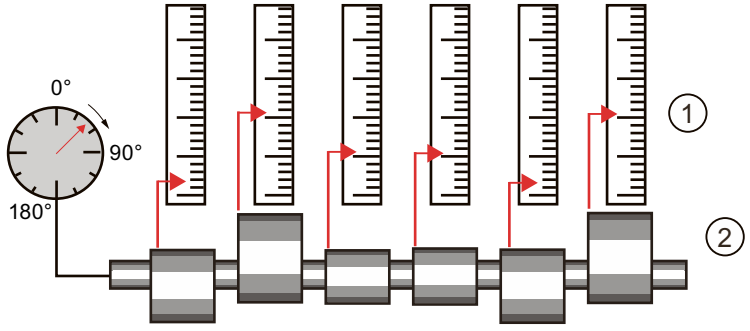
Figure 3-616 Cycle time of the analog output module

Typical applications

In principle, isochronous mode is worthwhile whenever measured values must be acquired synchronously, movements must be coordinated, and process reactions must be defined and executed at the same time. There are thus numerous areas in which isochronous mode can be used.

Typical applications include, for example, the acquisition of binary signals for quality assurance at specific times and positions. But hydraulic applications with position and pressure control can benefit as well from the equidistant and isochronous data transmission.

The following example shows the use of isochronous mode within the production process of camshafts. Precise measurements must be made at several measuring points for quality assurance.



① Measured values
② Camshaft

Figure 3-617 Measuring of camshafts

By using the system property "isochronous mode" and the associated simultaneous measured value acquisition, measurement can be performed continuously. The time required for measurement is reduced. Resultant workflow:

- Continuous machining of the camshaft
- During the continuous turning, measure the positions and cam excursion synchronously
- Process the next cam shaft

All camshaft positions and the corresponding measured values are measured synchronously within a single rotation of the camshaft. This increases machine output and maintains or enhances precision of the measurement.

8.2 ST modules vs HS modules

This section gives you an overview of other important distinctions between standard and high-speed analog modules. The specified numerical values are examples of selected modules. Keep in mind that the information can vary from module to module. The exact information of specific used analog module is available in the corresponding manual.

Conversion method

Instantaneous value conversion

Instantaneous value conversion if often used to convert analog signal into digital information in HS modules. In this type of conversion a very short sample is taken from the measured signal and converted into digital data. This digital information therefore represents an instantaneous value of the measured signal. Instantaneous value conversion is used to acquire fast changes of process values, such as in the area of motion control. The quickly changing physical quantities in this case must be acquired and processed quickly in cooperation with suitable transducers. Input areas are primarily voltage, current and resistance, the latter especially for position potentiometers.

Because the measured signal is converted within a short time, there is a risk of incorrect measurements in case of faulty signals. The analog inputs working with the instantaneous value conversion method cannot detect if the sampled signal value is the target signal or an overlaying disturbing pulse. They always convert the "instantaneously" detected value. This

means the pending measurement task should be carefully examined with regard to time constraints.

Integrating conversion
ST modules usually work according to the integrating conversion principle. The integrating conversion involves the sampling of a measured signal across a specified time period (integration time). Although this method is slower than instantaneous value conversion, it returns a conversion with higher immunity to interference. When you select the time interval for the conversion so that it corresponds to one or several periods of the surrounding network frequency, the omnipresent interference that is possibly also overlaying the signal is basically suppressed. SIMATIC modules give you the option to set the network frequency at which the plant is operated by means of parameter assignment. The resolution and conversion times may change depending on the interference frequency suppression that is set. The technical specifications of the respective module define these dependencies.

Analog inputs with integrating methods can be used universally. Even though the cabling must also be carefully designed with these analog inputs, the requirements are much less than those for analog inputs with instantaneous value conversion due to their slower signal acquisition that is basically immune to interference.

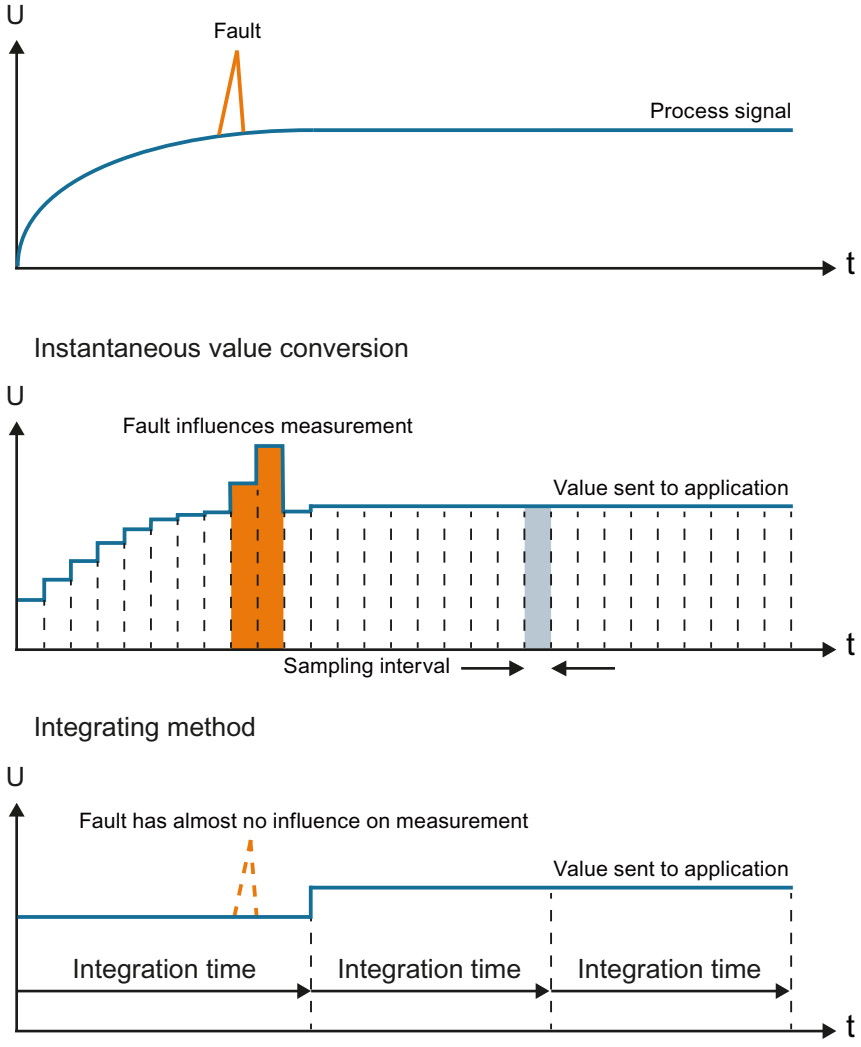


Figure 3-618 While an interference directly influences the value that is supplied to the application with instantaneous value encryption, its influence is negligible for the integrating method.

Electromagnetic compatibility

The entire architecture of HS modules is designed for fast processing of the signals. An interference-free design is therefore critical when using HS modules.

The following rules apply to the wiring of HS modules with sensors and actuators:

- Keep the cables as short as possible
- Use shielded and twisted pair cables
- Low-impedance connection of the cable shield at the respective shield supports
- Short cable loop between shield support and terminal connection

NOTE

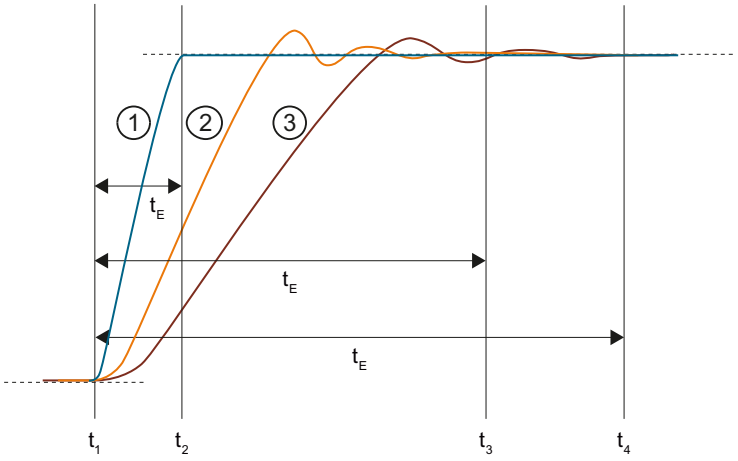
Interference-free design

Make sure that you pay close attention to the notes listed in the function manual Configuring interference-free controllers (http://support.automation.siemens.com/WW/view/en/59193566) when using HS modules.

Effect of load on the settling time

The settling times to the setpoint achieved with analog output modules depend on the applied load, among other things. To take advantage of the faster conversion times, only small loads (e.g., max. 47 nF) are permitted in HS modules as specified in the technical specifications.

The type of load has an effect on the form of settling to the setpoint when using output modules. Capacitive loads reduce the rise time due to the charging process and can cause the output signal to overshoot. Inductive loads result in a delayed current increase due to remagnetization and therefore also a shorter rise time. The figure below shows the output signal with no/small ①, medium ② and high ③ capacitive load.



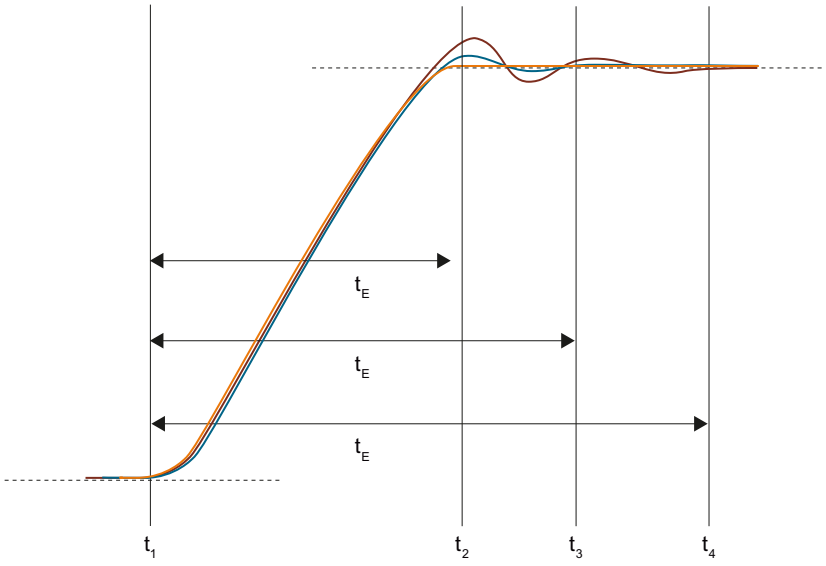
① Reference curve of a signal with no/small load capacity
② Signal with a load capacity of 47 nF
③ Signal with a load capacity of 100 nF
t_E Settling time
t_1 Module ends conversion at the terminal of the analog output channel and outputs the analog signal
t_2 Signal ① has settled and the specified analog output value has been reached (residual error 1 %)
t_3 Signal ② has settled and the specified analog output value has been reached (residual error 1 %)
t_4 Signal ③ has settled and the specified analog output value has been reached (residual error 1 %)

Figure 3-619 Effect of different loads on the settling time

Effect of the cable length on the settling time

Long cables between signal source and module are a target for interferences. You should therefore keep the cables as short as possible especially for HS modules. Cables have a capacitive and inductive component and therefore have an effect on the settling behavior of the signal.

The example below shows the jump of the output voltage of an HS output module with small, medium and long cable length. The overshoot of the input signal increases with the length of the cable and therefore the time until it reaches the setpoint.



t_E Settling time

t_1 Module ends conversion at the terminal of the analog output channel and outputs the analog signal

t_2 The signal running through a cable with short length has settled and the specified analog output value has been reached (residual error 1 %)

t_3 The signal running through a 20 m cable has settled and the specified analog output value has been reached (residual error 1 %)

t_4 The signal running through a 200 m cable has settled and the specified analog output value has been reached (residual error 1 %)

Figure 3-620 Effect of different cable lengths on the settling time

Effect of the value jump on the settling time

The figure below shows the effect of the height of the value jump between different output values on the settling time for analog output modules. The dotted line indicates the time when the signal has reached the setpoint. The higher the value jump, the later the signal reaches the setpoint.

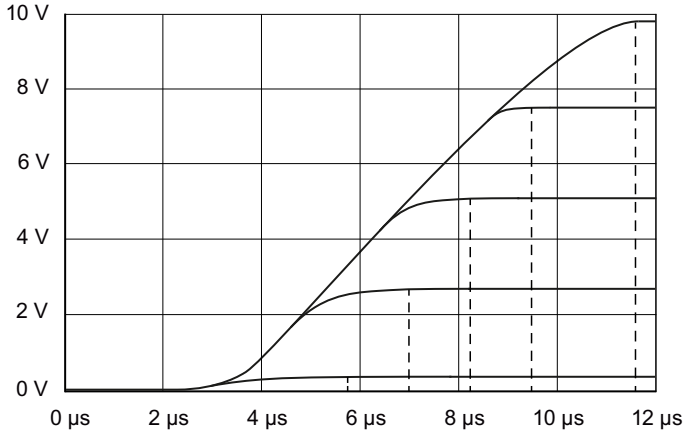


Figure 3-621 Settling time of five different analog signals with different value jumps

SIEMENS

Function Manuals Documentation Guide 1

Time-based IO basics 2

Configuring and parameter assignment 3

Programming 4

SIMATIC

S7-1500, ET 200MP, ET 200SP High-precision input/output with Time-based IO

Function Manual

12/2024

A5E33454822-AD

Preface

Purpose of the documentation

This function manual will support you when you use "Time-based IO" technology with the S7-1500, ET 200MP, and ET 200SP systems.

The documentation deals with the following topics:

- Using "Time-based IO" technology
- Functions of the "Time-based IO" technology
- Hardware and software requirements for "Time-based IO"
- Configuring the "Time-based IO" function with STEP 7 (TIA Portal)

Basic knowledge required

The following knowledge is required in order to understand the Function manual:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Proficiency with STEP 7 (TIA Portal)
- Knowledge about isochronous mode

Scope of the documentation

The following documentation is valid for all components of the S7-1500, ET 200MP and ET 200SP systems that support the "Time-based IO" technology.

Conventions

The following terms are used as synonyms in this documentation:

- **TIO module**: This term is used as synonym for I/O modules of the type:
  - ET 200MP TM Timer DIDQ 24x24V
  - ET 200SP TM Timer DIDQ 10x24V
- **TIO_Time**: This term is used as synonym for the shared time base (relative time) of the TIO modules.
- **Jitter**: This is a general term that includes various time influences affecting accuracy. This means that:
  - for input data: Deviation of the measured time from the actual event.
  - for output data: Deviation of the actual switching time from the specified time.

You should also pay particular attention to notes such as the one shown below:

NOTE
The notes contain important information on the product, handling the product or on part of the documentation to which particular attention should be paid.

Additional support

The range of technical documentation for the individual SIMATIC products and systems can be found on the Internet (http://www.siemens.com/simatic-tech-doku-portal).

For more information about configuration of Time-based IO, see the following FAQs in the Siemens Industry Online Support:

- Entry ID 109738186 (https://support.industry.siemens.com/cs/ww/en/view/109738186)
- Entry ID 109736374 (https://support.industry.siemens.com/cs/ww/en/view/109736374)

Additional information on isochronous mode is available in the Isochronous mode (http://support.automation.siemens.com/WW/view/en/49948856) and PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/109755401) manuals.

Industry Mall

The Industry Mall is the catalog and order system of Siemens AG for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).

You can find catalogs for all automation and drive products on the Internet (https://mall.industry.siemens.com) and in the Information and Download Center (https://www.siemens.com/automation/infocenter).

Security information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens products and solutions form one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For more information on industrial cybersecurity measures, please visit (http://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed here (http://www.siemens.com/industrialsecurity).

Table of contents

1 Function Manuals Documentation Guide 6

1.1 Function Manuals Documentation Guide 6

1.2 SIMATIC Technical Documentation 8

1.3 Tool support 10

2 Time-based IO basics 11

2.1 Using Time-based IO 11

2.2 Time behavior of Time-based IO 12

2.2.1 Time behavior of standard technology 12

2.2.2 Time-based IO properties 13

2.3 System environment 14

2.4 Hardware requirements 15

2.5 Configuration software requirements 15

2.6 Technical implementation 16

3 Configuring and parameter assignment 20

3.1 Requirements 20

3.2 Settings for Time-based IO 20

4 Programming 22

4.1 Overview of instructions 22

4.2 Programming of Time-based IO 23

4.3 Time-based IO 25

4.3.1 TIO_SYNC: Synchronizing TIO modules 25

4.3.2 TIO_DI: Reading in edges at digital input and associated time stamps 30

4.3.3 TIO_DI_ONCE: Reading in edges once at the digital input and associated time stamps 34

4.3.4 TIO_DQ: Output edges time-controlled at the digital output 40

4.3.5 UDT TIO_SYNC_Data 45

Function Manuals Documentation Guide

1

1.1 Function Manuals Documentation Guide



The documentation for the SIMATIC S7-1500 automation system, for the 1513/1516pro-2 PN, SIMATIC Drive Controller CPUs based on SIMATIC S7-1500 and the SIMATIC ET 200MP, ET 200SP, ET 200AL and ET 200eco PN distributed I/O systems is arranged into three areas.

This arrangement enables you to access the specific content you require.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742705).

Basic information



The system manuals and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500, SIMATIC Drive Controller, ET 200MP, ET 200SP, ET 200AL and ET 200eco PN systems. Use the corresponding operating instructions for 1513/1516pro-2 PN CPUs.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- Getting Started S7-1500
- System manuals
- Operating instructions ET 200pro and 1516pro-2 PN CPU
- Online help TIA Portal

Device information



Equipment manuals contain a compact description of the module-specific information, such as properties, wiring diagrams, characteristics and technical specifications.

Examples:

- Equipment manuals for CPUs
- Equipment manuals for interface modules
- Equipment manuals for digital modules
- Equipment manuals for analog modules
- Equipment manuals for communication modules
- Equipment manuals for technology modules
- Equipment manuals for power supply modules
- Equipment manuals for BaseUnits

General information



The function manuals contain detailed descriptions on general topics relating to the SIMATIC Drive Controller and the S7-1500 automation system.

Examples:

- Function Manual Diagnostics
- Function Manual Communication
- Function Manuals Motion Control
- Function Manual Web Server
- Function Manual Cycle and Response Times
- PROFINET Function Manual
- PROFIBUS Function Manual

Product Information

Changes and supplements to the manuals are documented in a Product Information. The Product Information takes precedence over the device and system manuals.

You will find the latest Product Information on the Internet:

- S7-1500/ET 200MP (https://support.industry.siemens.com/cs/de/en/view/68052815)
- SIMATIC Drive Controller (https://support.industry.siemens.com/cs/de/en/view/109772684/en)
- Motion Control (https://support.industry.siemens.com/cs/de/en/view/109794046/en)
- ET 200SP (https://support.industry.siemens.com/cs/de/en/view/73021864)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109765611)

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- S7-1500/ET 200MP/SIMATIC Drive Controller (https://support.industry.siemens.com/cs/ww/en/view/86140384)
- ET 200SP (https://support.industry.siemens.com/cs/ww/en/view/84133942)
- ET 200AL (https://support.industry.siemens.com/cs/ww/en/view/95242965)
- ET 200eco PN (https://support.industry.siemens.com/cs/ww/en/view/109781058)

1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
   - Industry Online Support International: (https://support.industry.siemens.com)

     The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
   - ID link:

     Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.
(https://support.industry.siemens.com/cs/ww/en/ps/ae)

1.3 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single tool.

With the TIA Selection Tool , you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet.
(https://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. This helps to prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet
(https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

See also

PRONETA Professional (https://support.industry.siemens.com/cs/ww/en/view/109781283)

Time-based IO basics

2

2.1 Using Time-based IO

Many processes in a plant require a relatively precise reproducibility as far as time is concerned. The reproducibility can be optimized to a limited extent by shorter CPU cycle times. The use of high-precision input/output with Time-based IO provides a more accurate reproducibility than the one that can be achieved by optimizing the CPU cycle time. An additional advantage of Time-based IO is the independence from the time scale of the application cycle.

Below is a selection of typical areas of application that can benefit from this technology.

Defined response times

An output signal that responds with a precise delay time that is independent of the application cycle can be output by adding a specified time to the time stamp of an edge at the digital input.

Length measurement

The length of a product passing by can be determined by the difference between two input time stamps and an associated travel speed.

Cam controller

The ongoing movement can be extrapolated from a synchronous position information (for example, from a counter module or an axis). Based on this result, the time of a switching position (cam position) is calculated and transferred to the TIO module (output). This way the switch event takes place at the required position.

Dosing

By specifying a switch-on and a switch-off edge to a time-controlled digital output, a valve can be opened for a specific time and the amount of liquid can be dosed accordingly.

2.2 Time behavior of Time-based IO

2.2.1 Time behavior of standard technology

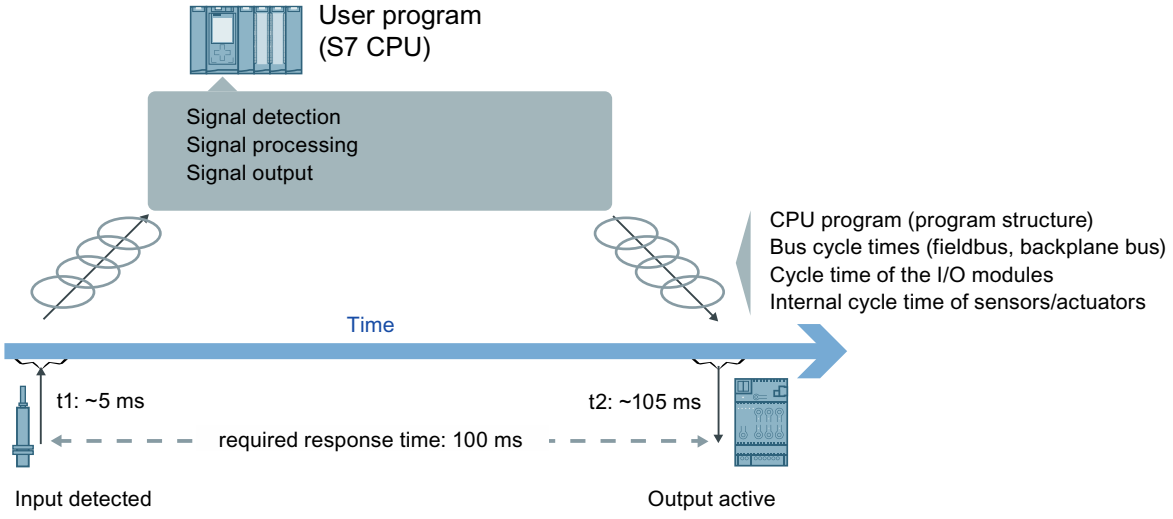
The time behavior of the inputs/outputs depends on the following factors for standard technology:

- CPU program (program structure)
- Bus cycle times (fieldbus, backplane bus)
- Cycle time of the I/O modules
- Internal cycle time of sensors/actuators

A deterministic statement as to

- when an input event (e.g., sensor signal) has taken place
- when the output event has an effect on the input event (e.g., output switches)

will become inaccurate due to the time factors listed above.

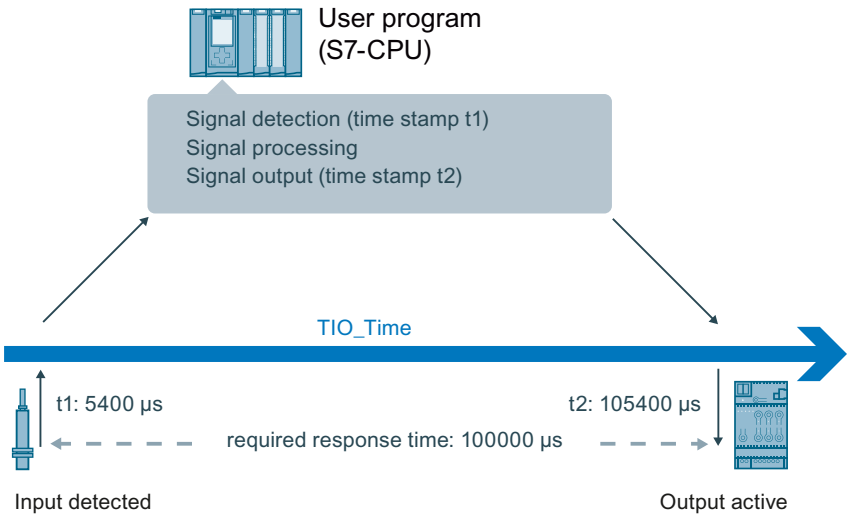


2.2.2 Time-based IO properties

Time-controlled I/O functionality

Time-based IO stands for time-based processing of I/O signals. All input signals are referred to one time (TIO_Time). The input signals receive the time stamp t1. After signal processing, the output event can also be linked with the TIO_Time and output at the required time. Output takes place at time t2.

Here an example for Time-based IO:



Independence and focus of Time-based IO

The shared time basis (TIO_Time) of all components involved is the basis for Time-based IO. By using TIO_Time, the accuracy of the output with Time-based IO does not depend on:

- CPU program (program structure)
- Bus cycle times (fieldbus, backplane bus)
- Cycle time of the I/O modules

The focus of Time-based IO is not on the I/O response time but on the predictability (determinism) of I/O signals. With Time-based IO, it is possible to respond to an input signal with an output signal within a defined time. Keep in mind the system-dependent minimum response time when using Time-based IO.

Time-based IO stands for:

- I/O functionalities executed with high precision
- I/O processes with time stamp

Accuracy

Accuracy is crucial for the performance capability of Time-based IO.

The accuracy is a property of the TIO modules and indicates the deviation with which the required response is achieved. For Time-based IO, the accuracy and reproducibility of the response is in the millisecond range.

Response time

In addition to a very high accuracy, a minimum response time to an input event can result depending on the configuration.

The response time is the time between the input event and the required output event.

For the minimum response time:

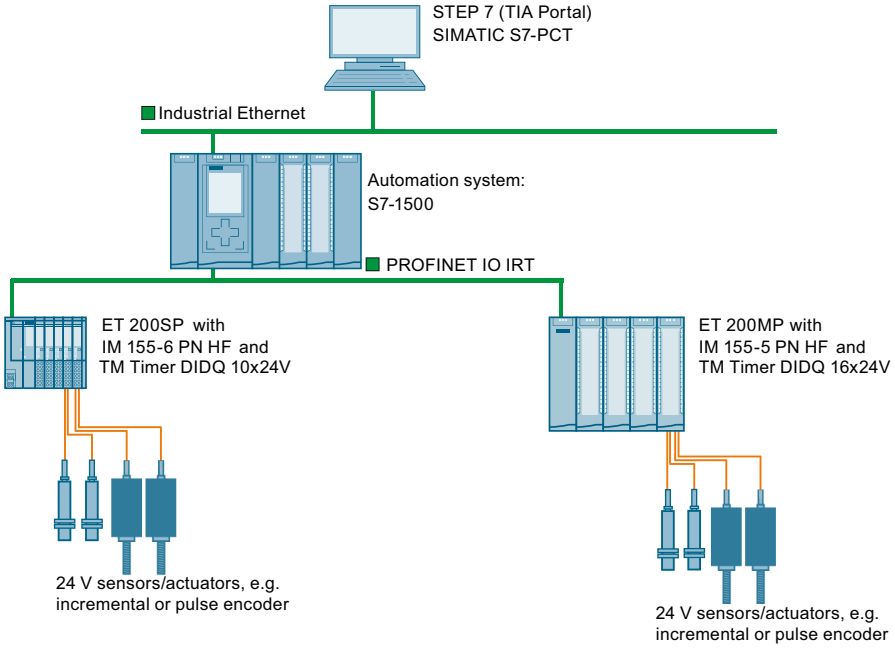
3 × application cycle T_{APP}

2.3 System environment

Introduction

Possible system configurations with PROFINET for the use of Time-based IO are shown below.

Use with STEP 7 (TIA Portal)



2.4 Hardware requirements

Introduction

The properties of the hardware components required for Time-based IO are listed below. You will also find specific modules as an example.

Requirements

Component	Properties	Examples
CPU	Isochronous mode/ PROFINET IO IRT: provides defines response time and high-precision plant behavior.	• CPU 1511-1 PN
ET 200 interface module	Supports isochronous mode	• ET 200SP with IM 155-6 PN HF (as of firmware V2.1) • ET 200MP with IM 155-5 PN HF
I/O module	TIO module	• ET 200SP: TM Timer DIDQ 10x24V • ET 200MP: TM Timer DIDQ 24x24V

See also

Requirements (Page 20)

2.5 Configuration software requirements

Introduction

Below is a list of the software versions which support the "Time-based IO" function.

Requirements

Configuration software	Requirements	Supported hardware components	Additional information
STEP 7 (TIA Portal) V16 and above	PROFINET IO IRT or isochronous mode on the backplane bus	• S7-1500 automation system • ET 200SP and ET 200MP distributed I/O systems • TM Timer DIDQ 24x24V • TM Timer DIDQ 10x24V	STEP 7 (TIA Portal) online help

Additional information on isochronous mode is available in the Isochronous mode (http://support.automation.siemens.com/WW/view/en/49948856) and PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/109755401) manuals.

TIO instructions

The TIO instructions are specific function blocks for use of Time-based IO. The following TIO instructions are available:

- TIO_SYNC
- TIO_DI
- TIO_DI_ONCE
- TIO_DQ

2.6 Technical implementation

Introduction

The information below will help you better understand the core aspects of Time-based IO and find out which SIMATIC functions are used to implement the described aspects.

Synchronization of involved modules (shared time basis)

The Time-based IO technology uses isochronous mode for all involved stations.

Isochronous mode enables multiple TIO modules to be synchronized to a shared time basis. The basis of the shared time basis for the TIO modules is the relative time TIO_Time.

Additional information on isochronous mode is available in the Isochronous mode (http://support.automation.siemens.com/WW/view/en/49948856) and PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/109755401) manuals.

TIO_Time

The TIO_Time is the central time basis to which all time stamps refer.

TIO_Time has the following properties:

- Shared time basis for all TIO modules which are synchronized with the TIO instruction TIO_SYNC.
- The time starts counting again with each CPU startup.
- The TIO_Time has data type LTime (e.g. LT#14s830ms652us315ns).
- All valid time stamps refer to TIO_Time:
  - Input time stamps of the TIO modules are converted to the TIO_Time in the TIO instructions TIO_DI and TIO_DI_ONCE.
  - In the TIO instruction TIO_DQ, output time stamps are converted to the output time stamp of the TIO modules.
- The value of TIO_TIME corresponds to the current time with respect to TIO instructions and is updated with the call of TIO_SYNC. If you want an output to relate not to a previous input time stamp but to the current time, you can use the value of TIO_TIME as basis for the output time stamp. Example: Output of an edge in 20 ms: TIO_DQ.TimeStampRE=TIO_SYNC_DATA.TIO_TIME+LT#20ms)

TIO instructions in the isochronous OB

The TIO instructions must be called in a "Synchronous Cycle" or "MC-PostServo" OB.

You can find additional information in the chapter Programming.

NOTE

The TIO instructions also support geared down isochronous mode. With a clock reduction ratio, the application cycle is longer than the send clock.

NOTE

The TIO instructions must be called in an "MC-PreServo" OB.
If you use an OB of the "MC-PostServo" type, you can decide separately for each TIO model whether it is used with Motion Control technology objects or with TIO instructions.
If you call the TIO instructions in an "MC-PostServo" type OB, you need to use the IPO model and also cannot use any reduction ratio.
Calling TIO instructions in an OB of the type "MC-PostServo" with reduction ratio "MC-Servo" can result in incorrect calculation of time stamps.

Modes for updating the process image

In isochronous mode, you can influence the order of the update of the process image partition of the input and output data. In doing so, you can select the following program execution models:

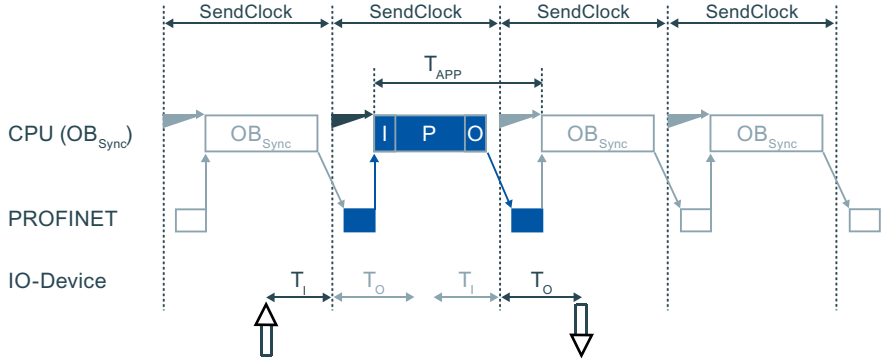
- IPO model (application cycle factor = 1)
- OIP model (application cycle factor >= 1)

The abbreviations I, P, O stand for the following processes: I = Input, P= Processing, O = Output.

Additional information on the application cycle factor is available in the PROFINET with STEP 7 (http://support.automation.siemens.com/WW/view/en/49948856) Manual.

IPO model (application cycle factor = 1)

The user program is started after the delay time. Start by updating the corresponding process image partition of the inputs in the user program by calling the SYNC_PI system instruction. Processing is started next (for example, calculation of the time stamps). The corresponding process image partition of the outputs is updated at the end of the user program in the CPU by SYNC_PO.



Transfer of inputs/outputs

Delay time

T_{APP} Application cycle

SYNC_PI SYNC_PO

SendClock Send clock

T_I Time for reading the input data

T_O Time until output of the output data

Time of read-in of the input data

Time of output of the output data

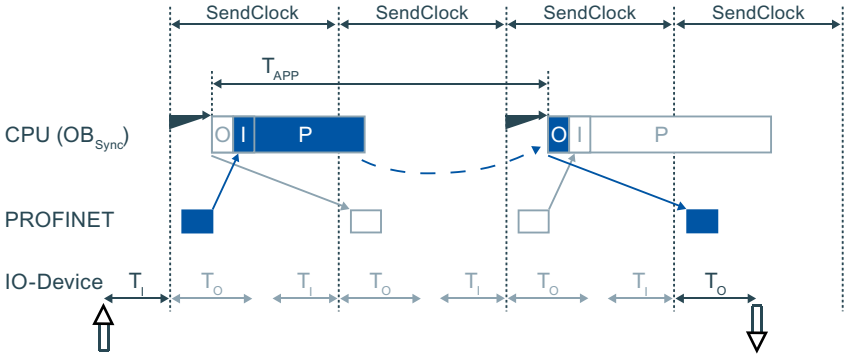
OB_{Sync} OB of type "Synchronous Cycle", "MC-PreServo" or "MC-PostServo"

Properties of the IPO model:

- Supports shorter response times
- The application cycle must not be greater than the send clock.
  This gives the application less time than with the OIP model.

OIP model (application cycle factor >= 1)

The user program is started after the delay time. In PIP_Mode 0, the TIO_SYNC instruction updates the process image. In the other modes, you start by updating the corresponding process image partition of the outputs in the user program by calling the SYNC_PO system instruction. As a result, the output data that was calculated in the previous network cycle will become active during the next network cycle (T_O). Next the corresponding process image partition of the inputs is updated in the CPU by SYNC_PI. Processing starts after the data is transmitted (for example, calculation of the time stamps).



Transfer of inputs/outputs

T_{APP} Application cycle

Delay time

SYNC_PI SYNC_PO

SendClock Send clock

T_I Time for reading the input data

T_O Time until output of the output data

Time of read-in of the input data

Time of output of the output data

OB_{Sync} OB of type "Synchronous Cycle", "MC-PreServo" or "MC-PostServo"

Properties of the OIP model:

- The response time is longer than with the IPO model.
- It is one application cycle longer than permitted by the send clock.
  This gives the application more time than with the IPO model.

Influence of accuracy

To estimate the accuracy you need the accuracy of

- TIO module
- Sensor/ actuator

Consult the data sheets of the respective module regarding the accuracy value.

You have to add the individual jitters of the TIO modules and the sensors/actuators. You can neglect any other influencing factors.

Configuring and parameter assignment 3

3.1 Requirements

Introduction

You need additional software components to use Time-based IO. You must also have created the standard configuration for your project.

Below you will learn more about the standard configuration for Time-based IO.

Requirements

In STEP 7 (TIA Portal):

- The project has been created.
- The CPU has been created and the parameters are assigned.
- Automation system and modules have been created and the parameters have been assigned.
- When using an ET 200 station: The connection has been created and the parameters are assigned via PROFINET.
- A "Synchronous Cycle" or "MC-PostServo" type OB has been created.

See also

System environment (Page 14)
Configuration software requirements (Page 15)

3.2 Settings for Time-based IO

Below you will find an overview of which settings have to be made for which components of Time-based IO.

Table 3-102 Overview of settings for Time-based IO

Component	Where adjustable[1]	Properties to be set	Additional information
When using an ET 200 station: PROFINET subnet	Properties of the PROFINET subnet > sync domain	Create sync domain or edit properties of sync domain	• PROFINET function manual (http://support.automation.siemens.com/WW/view/en/49948856) • Online help in the STEP 7 (TIA Portal) information system
		Specify devices of the sync domain: • Specify CPU as sync master. • Specify ET 200 interface module as sync slave with RT class "IRT".	

Component	Where adjustable[1]	Properties to be set	Additional information
S7-1500 station ET 200 station	Properties of the PROFINET interface > isochronous communication	Enable isochronous mode	• Function Manual Isochronous Mode (https://support.industry.siemens.com/cs/ww/en/view/10975540-1) • PROFINET function manual (http://support.automation.siemens.com/WW/view/en/49948856) • Manual Technology Module TM Timer DIDQ 24x24V (https://support.industry.siemens.com/cs/ww/en/view/10997430-9) • Manual Technology Module TM Timer DIDQ 10x24V (https://support.industry.siemens.com/cs/ww/en/view/95153951) • Online help in the STEP 7 (TIA Portal) information system
TIO module	Properties of the TIO module > I/O addresses	Enable isochronous mode	
	Properties of the TIO module > I/O addresses	Assign or create a "Synchronous Cycle" or "MC-PostServo" type OB	
	Properties of the TIO module > I/O addresses	Assignment of I/O addresses to the process image partition (e.g., PIP1)	
	Properties of the TIO module > Basic parameters	Configure "Module use from the user program"	
	Properties of the TIO module > Basic parameters/Channel parameters	For TM Timer DIDQ 10x24V: If required, assign parameters for Configuration "Use input/output individually"	
		Parameter assignment for use of Timer DI and Timer DQ	
Isochronous OB (Synchronous Cycle or MC-PostServo)	Properties of the Isochronous OB > Isochronous mode	Adjust application cycle, if necessary	

[1] Describes the topic area in the configuration software.

Setting for Time-based IO

If you have no special response time requirements, the following setting is suitable as a starting point:

- Send clock: 2 ms
- Application cycle: 4 ms
- Assignment to the process image partition: PIP1
- PIP_Mode: 0 (OIP model)

FAQ

For more information, see the following FAQs in the Siemens Industry Online Support:

- Entry ID 109738186 (https://support.industry.siemens.com/cs/ww/en/view/109738186)
- Entry ID 109736374 (https://support.industry.siemens.com/cs/ww/en/view/109736374)

Programming

4

4.1 Overview of instructions

Introduction

Time-based IO is used with special instructions (TIO instructions). The TIO_SYNC TIO instruction is responsible for synchronizing all involved TIO modules and creates a unique time basis (TIO_Time) to which all actions are referenced.

Additional instructions undertake the reading in of process input signals with associated time stamps and/or the time-controlled output of process output signals.

NOTE

The TIO instructions are helpful for general time-based IO applications. For special applications, such as cam controllers, there are also separate technology objects, for example, TO_CamOutput.

NOTE

The TIO instructions use the time stamp functions of the TIO modules. The other functions of the TIO modules can be used independently of the TIO instructions in applications.

TIO instructions

Instruction	Short description
TIO_SYNC	Synchronizes the TIO modules and provides the time basis for Time-based IO
TIO_DI	Detects the edges at the digital input (Timer DI) and supplies the associated time stamp
TIO_DI_ONCE	• Detects the edges at the digital input (timer DI) once and provides the associated time stamp • Controls a timer DI channel which is configured as an edge-triggered enable for another channel.
TIO_DQ	Outputs time-controlled edges at the digital output (Timer DQ)

4.2 Programming of Time-based IO

Introduction

To use Time-based IO, the TIO instructions must be called in an isochronous OB. The application can also run in another OB. This allows you to shorten the runtime of the isochronous OB.

You need the following TIO instructions according to the required task:

TIO module	TIO instructions
• TM Timer DIDQ 24x24V • TM Timer DIDQ 10x24V	• Per digital input, one TIO_DI or TIO_DI_ONCE for read-in • Per digital output, one TIO_DQ for output • One TIO_SYNC (for up to eight TIO modules)

This section below describes the programming of the CPU for Time-based IO.

Requirements

Hardware configuration in STEP 7 (TIA Portal):

- The TIO modules are assigned to an isochronous network.
- The TIO modules are assigned to a shared process image partition.
- The process image partition is assigned to an isochronous OB.
- The TIO modules are configured for use with instructions from the "Time-based IO" library.

Additional information on configuration of Time-based IO is available in the section Settings for Time-based IO (Page 20).

Procedure

1. Create a TIO instruction, TIO_SYNC, in the isochronous OB.
2. Connect all TIO modules to be synchronized at the TIO_SYNC TIO instruction using parameters HWID_1 to HWID_8.

   The HWID can be found in the hardware configuration under "Properties > System constants".

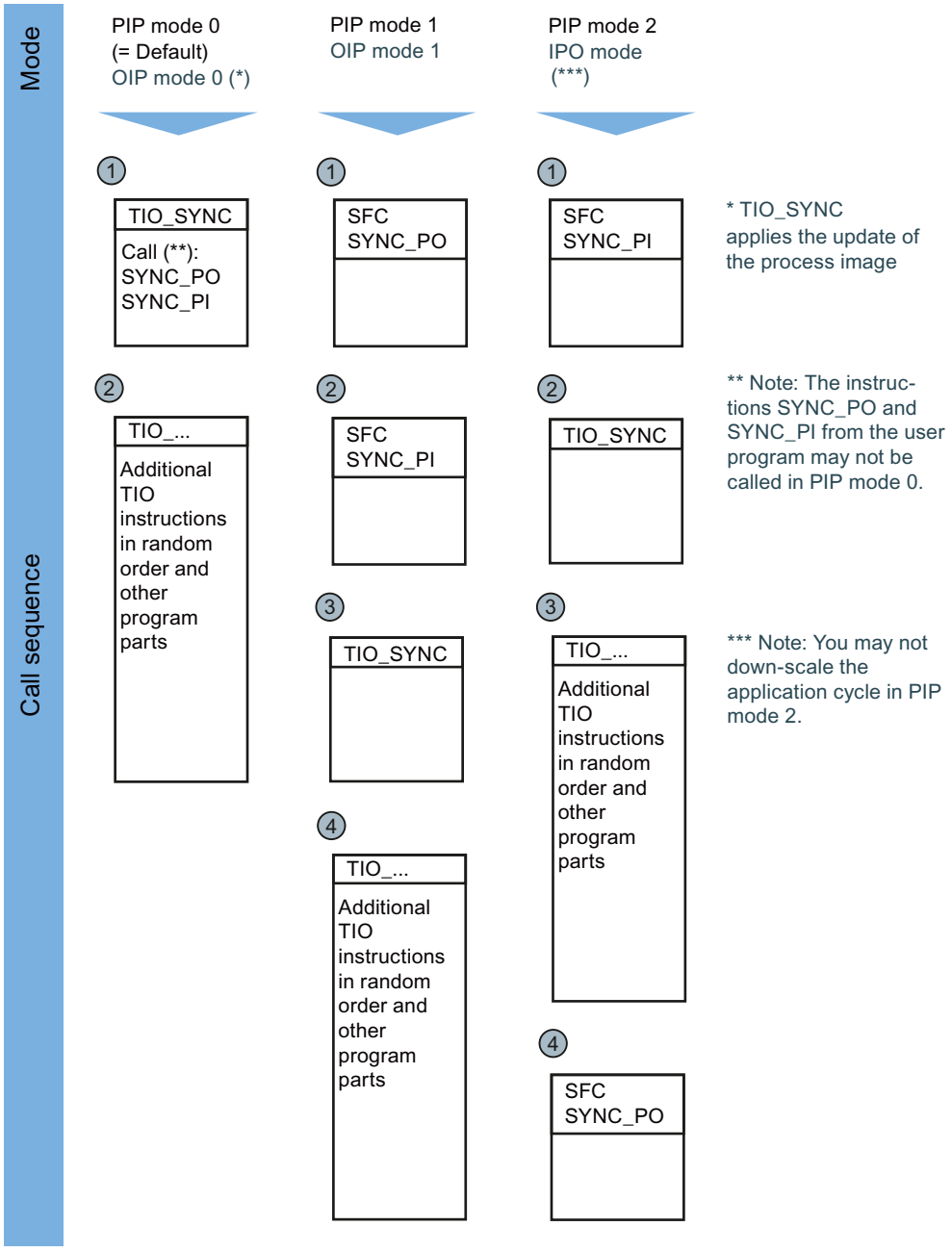
   NOTE
   Use of symbolic constants is generally preferred instead of absolute numerical values when interconnecting.

3. Set the data update mode at the TIO_SYNC instruction at the PIP_Mode input parameter.

   The description of the modes is available in the chapter Technical implementation (Page 16).

   The parameter assignment of the TIO_SYNC TIO instruction is complete.

4. For the following instructions, note the call sequence depending on the selected value for PIP_Mode:



5. Add the TIO instructions for read-in/output required for your application in the isochronous OB.
6. At the TIO instructions for read-in/output, interconnect in each case the input/output TIO_SYNC_Data with the same name output at the TIO_SYNC.
7. At the TIO instructions for read-in/output, assign parameters for the input parameters HWID (see "Properties > System constants" in hardware configuration) and Channel.
   The Time-based IO functionality is successfully programmed.
8. Interconnect the Time-based IO functionality with your application, such as evaluating the read-in time stamp in a step sequencer in another OB.

9. If TIO_SYNC does not automatically read out the send clock: Define the send clock manually, e.g. in OB100.
10. Compile and download the entire project to the CPU.

Result

You have completed programming the use of Time-based IO.

FAQ

For more information, see the following FAQs in the Siemens Industry Online Support:

- Entry ID 109738186 (https://support.industry.siemens.com/cs/ww/en/view/109738186)
- Entry ID 109736374 (https://support.industry.siemens.com/cs/ww/en/view/109736374)

4.3 Time-based IO

4.3.1 TIO_SYNC: Synchronizing TIO modules

Description

TIO_SYNC is the basis for all other TIO instructions. TIO_SYNC synchronizes TIO modules to a shared time basis TIO_Time.

You can synchronize up to 8 TIO modules with TIO_SYNC. All TIO modules must be assigned to the same process image partition (PIP). If you select "0" for the input parameter PIP_Mode, you assign the number of the process image partition at the PIP_PART input parameter.

Additional information on configuration of Time-based IO is available in the Configuration and parameter assignment section.

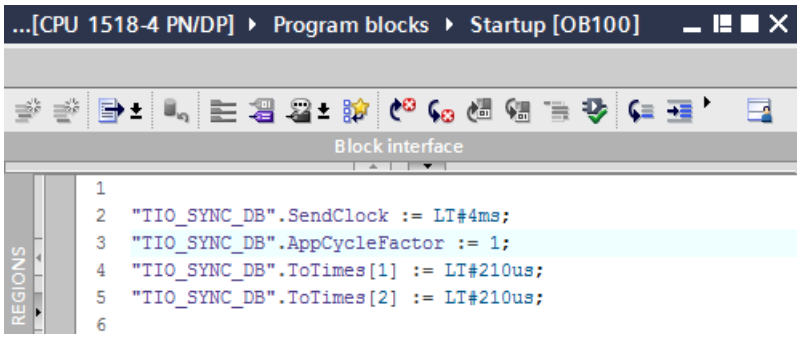
Startup characteristics

At the startup of the CPU, the TIO_SYNC instruction receives and checks the input parameters once and initializes the TIO_Time.

You have several options for handling the optional parameters SendClock, AppCycleFactor and ToTimes:

- SendClock, AppCycleFactor and ToTimes can be read in automatically each time the system is started. This results in a time delay during startup, but the values are always consistent.
- Automatically read in SendClock, AppCycleFactor and ToTimes at each startup and apply the read-in values as set values during commissioning. This results in fast subsequent startups, but is inconsistent after changes in the hardware configuration (repeat commissioning necessary).

- Manually define SendClock, AppCycleFactor and ToTimes before the first call of the instruction, for example, in OB100:



This results in a fast startup, but you need to manually update the values after changes to the hardware configuration.

You will find information about the parameters in the table below.

NOTE

Automatic reading of SendClock, AppCycleFactor and ToTimes is recommended
The automatic reading of SendClock, AppCycleFactor and ToTimes is recommended to ensure the consistency of the parameters even with subsequent changes in the hardware configuration. You activate the automatic reading via the parameter value AppCycleFactor = 0.

If startup takes place without errors, the instruction changes to normal operation. In the event of an error, the instruction does not change to normal operation and generates an error message.

Operating principle

In normal operation, the instruction ensures synchronization of all TIO modules configured at the HWID input.

The calculated TIO_Time for the instructions of the TIO modules is provided at the TIO_SYNC_Data output.

Reaction to error

The Error output indicates if the instruction was processed correctly. In the event of an error, the cause of the error is displayed at the Status output.

Parameter

The table below shows the parameters of the TIO_SYNC instruction.

Parameter	Declaration in library version		Data type	Default	Description
	< V2.0	≥ V2.0	S7-1500		
HWID_1 ... HWID_8*	Input		HW_IO	65535	Hardware identifier for TIO module from hardware configuration
PIP_Mode*	Input		PIP	0	Mode for the data update**: • 0: OIP model with internal update of the process image by SYNC_PO and SYNC_PI. • 1: OIP model without internal update of the process image • 2: IPO model without internal update of the process image
PIP_PART*	Input		USInt	1	Only relevant if PIP_Mode = 0 Number of the process image partition which is to be updated isochronously.
TIO_SYNC_ Data	Output		"TIO_ SYNC_ Data"		Calculated system time for the TIO instructions of the TIO modules and internal data used for synchronization. See UDT TIO_SYNC_Data (Page 45).
Status	Output		DWord	16#0	Status of the instruction: see description of Status parameter
Error	Output		Bool	False	Error = True: An error has occurred. For detailed information see Status parameter. Error is reset as soon as the error is corrected.
OperatingState		Static	Int	0	Internal operating state of the instruction: • 0: Input parameters are checked • 1: Optional parameters are read out • 2: Read-out parameters are checked • 3: Normal operation (all parameters OK, TIO modules synchronized) As soon as operating state 3 is reached, time stamps can be read in and edges can be output. If you want to repeat the synchronization of the TIO modules and the readout of the optional parameters, you can set the operating state to 0.
SendClock	Input	Static	LTime	LT#0ns	Send clock of the sync domain. Apply the send clock from the PROFINET configuration. Note: If you use the parameter value AppCycleFactor = 0, SendClock can be left as the default (automatic reading of the parameters).
AppCycleFactor		Static	UInt	0	Application cycle factor: • Range of values: 0 <= AppCycleFactor <= 85 • 0: SendClock, AppCycleFactor and ToTimes are read in automatically The application cycle T_{APP} is calculated as follows: T_{APP} = AppCycleFactor × SendClock
ToTimes		Static	LTime array [1...8]	LT#0ns	T_o for each TIO module: Time for output of isochronous output data. Note: If you use the parameter value AppCycleFactor = 0, ToTimes can be left as the default (automatic reading of the parameters).

* Checked once at startup of the CPU

** The IPO model (PIP_Mode = 2) provides the shortest response times, but it also places the highest demands on system performance. Processing of all TIO instructions and other program sections must be completed within one send clock.
Select the OIP model (PIP_Mode = 0) only if you use only *one* instance of the TIO_SYNC instruction per process image partition so that the SYNC_PI and SYNC_PO instructions are not called more than once in the isochronous OB. In addition, do not call SYNC_PI and SYNC_PO in the other program sections in the OIP model.

NOTE

The TIO instructions must be called in an "MC-PreServo" OB.

If you use an OB of the "MC-PostServo" type, you can decide separately for each TIO model whether it is used with Motion Control technology objects or with TIO instructions.

If you call TIO_SYNC in an "MC-PostServo" type OB, you need to use PIP_Mode = 2 and also cannot use any reduction ratio.

Status parameter

Error codes or status information is output as double word at the Status output.

The double word is divided as follows:

Error code (DW#16#...)	Meaning
z0yywwww	Error of a system function: • during startup (z = 1) • during normal operation (z = 0) System functions with subordinate use are coded in yy: See table with error codes. wwww specifies the RET_VAL of the system function. The error information is available in the help for the system function.
z0yy0000	An error that does not originate in a system function. This error receives a consecutive error number yy. The error can occur: • during startup (z = 1) • during normal operation (z = 0)

Table with error codes

Error code (DW#16#...)	Meaning	Solution
00000000	No error.	—
1001xxxx	An error has occurred with system function RD_SINFO. The low word xxxx displays the error information of the RET_VAL return value from RD_SINFO.	• Read the description of the RD_SINFO in the STEP 7 (TIA Portal) information system. • Make sure that TIO_SYNC is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10020000	The read cycle time of the isochronous OB is invalid (LT#0ms or negative). The instruction can only be used without errors in an isochronous OB.	• Correct the value of the cycle time. • Make sure that TIO_SYNC is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10030000	The TIO_SYNC instruction is not called in an isochronous OB. The instruction can only be used without errors in an isochronous OB.	Make sure that TIO_SYNC is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10040000	The assigned value at the PIP_Mode input parameter is outside the valid range of 0 to 2.	Correct the value at the PIP_Mode input parameter.
10050000	The configured send clock is outside the permitted range of 0 < SendClock <= 4 ms.	Correct the value of the send clock.
0006xxxx*	An error has occurred during execution of the SYNC_PI system function. The low word xxxx displays the error information of the RET_VAL return value from SYNC_PI.	Read the description of the SYNC_PI in the STEP 7 (TIA Portal) information system.
0007xxxx*	An error has occurred during execution of the SYNC_PO system function. The low word xxxx displays the error information of the return value RET_VAL from SYNC_PO.	Read the description of the SYNC_PO in the STEP 7 (TIA Portal) information system.

* Available only when "0" is selected for the input parameter PIP_Mode.

Error code (DW#16#...)	Meaning	Solution
10080000	At least one of the hardware identifiers does not belong to a TIO module.	Check the values of input parameters HWID_1 to HWID_8. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration.
10090000	HWID_1 is not a valid hardware identifier. Possible causes: • No module with this hardware identifier available. • The CPU went to RUN mode before the module was supplied with voltage.	Check the value of the respective input parameter. In each case, specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.
100A0000	HWID_2 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
100B0000	HWID_3 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
100C0000	HWID_4 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
100D0000	HWID_5 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
100E0000	HWID_6 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
100F0000	HWID_7 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
10100000	HWID_8 is not a valid hardware identifier. Possible cause: No module with this hardware identifier available.	
10110000	The value at input parameter PIP_PART is outside the valid range of 1 ... 31.	Correct the value at the PIP_PART input parameter.
10120000	The value "2" is configured at the input parameter PIP_Mode, while the value > 1 (reduction ratio) is configured at the static parameter AppCycleFactor.	Correct the value at the PIP_Mode input parameter. PIP_Mode with the value "2" does not allow a reduction ratio.
x0130000	MC-Servo (OB91) is not isochronous to the bus cycle time.	Correct the value of the cycle time of the MC-Servo to the value of the bus cycle time. Note: Calling TIO instructions in an OB of the type "MC-PostServo" with reduction ratio "MC-Servo" can result in incorrect calculation of time stamps.
x014xxxx	An error has occurred when reading the data record. The low word xxxx indicates the error information of the instruction RDREC.	Read the description of the instruction RDREC in the STEP 7 (TIA Portal) information system.
x0FF0000	General internal error.	—

* Available only when "0" is selected for the input parameter PIP_Mode.

4.3.2 TIO_DI: Reading in edges at digital input and associated time stamps

Description

TIO_DI continuously detects the edges at a digital input of a TIO module and returns the associated time stamps.

Startup characteristics

During startup of the CPU, the instruction TIO_DI applies the input parameters once and checks the following:

- Checking HWID
- Checking to see if the number of the digital input (Channel) is in the permitted range (depending on addressed module and channel configuration)
- Checking TIO_SYNC_Data.ERROR: Is an error present at TIO_SYNC?
- Checking TIO_SYNC_Data.TO_TIMES for plausibility (0 ms to 4 ms)
- Checking to see whether the OB is isochronous

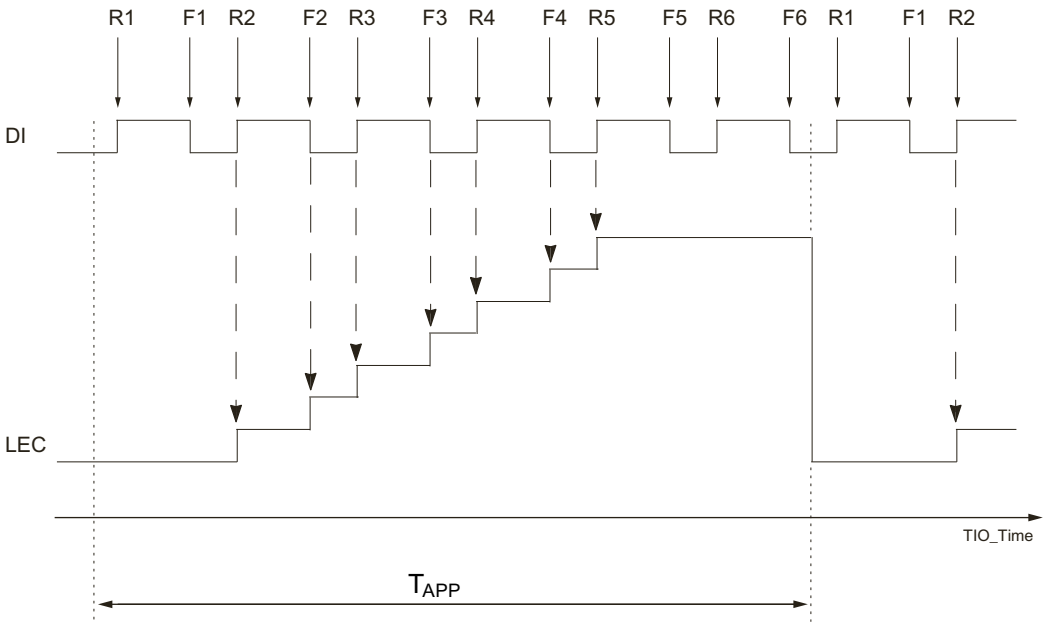
If startup takes place without errors, the instruction changes to normal operation. In the event of an error, the instruction does not change to normal operation and generates an error message.

Functional description

In normal operation, the instruction detects the edges at a digital input and the associated time stamps of the last valid, defined edge pair from the preceding isochronous cycle. Use the input parameter EdgeSel to determine the edges for which time stamps are detected.

You connect the input TIO_SYNC_Data with the output of the same name of the TIO_SYNC instruction. This ensures a shared time basis.

The following figure shows an example of the behavior of LEC when a read-in job is started with EdgeSel = 3 (rising and falling edge, order depending on occurrence).



T_{APP} Application cycle
Rn Specified times of a positive DI edge
Fn Specified times of a falling DI edge

The module can count a maximum of seven edges per application cycle. LEC = 7 means therefore that seven or more edges have been counted.

Reaction to error

The Error output indicates if the instruction was processed correctly. In the event of an error, the cause of the error is displayed at the Status output.

Parameter

The table below shows the parameters of the TIO_DI instruction.

Parameter	Declaration in library version		Data type	Default	Description
	< V2.0	≥ V2.0	S7-1500		
HWID*	Input		HW_IO	0	Hardware identifier for TIO module from hardware configuration
Channel*	Input		UInt	0	Number (0 ... m) of the digital input of the connected TIO module
EdgeSel	Input		UInt	3	Specify the edges for which time stamps are detected: 0_D: Invalid 1: Two rising edges 2: Two falling edges 3: Rising and falling edge (order depending on occurrence) 4: First rising, then falling edge 5: First falling, then rising edge 6 to 255: Invalid

* Checked once at startup of the CPU

Parameter	Declaration in library version		Data type	Default	Description
	< V2.0	≥ V2.0	S7-1500		
					EdgeSel can be changed during normal operation.
DI	Output		Bool	False	Status of digital input. If an inversion of the digital input is configured, this parameter is inverted as well.
TimeStampRE	Output		LTime	LT#0ns	Time stamp: Time at which a positive edge was detected. Exception: EdgeSel = 2: Time at which a falling edge has been detected (if *multiple* falling edges have occurred during the application cycle).
TimeStampFE	Output		LTime	LT#0ns	Time stamp: Time at which a falling edge was detected. Exception: EdgeSel = 1: Time at which a rising edge has been detected (if *multiple* rising edges have occurred during the application cycle).
EventCountRE	Output		UInt	0	Counter: Is incremented with each new, valid time stamp at a positive edge. The counter is reset with each CPU startup.
EventCountFE	Output		UInt	0	Counter: Is incremented with each new, valid time stamp at a falling edge. The counter is reset with each CPU startup.
LEC	Output		UInt	0	Counter: Number of edges for which no time stamp could be saved. The module can count a maximum of seven edges per application cycle. The counter is reset with each new application cycle.
Status	Output		DWord	16#0	Status of the instruction: see description of Status parameter
Error	Output		Bool	False	Error = True: An error has occurred. For detailed information see Status parameter. Error is reset as soon as the error is corrected.
TIO_SYNC_Data*	Input	InOut	"TIO_SYNC_Data"		System time provided for the TIO instructions of the TIO modules by the TIO_SYNC instruction. See UDT TIO_SYNC_Data (Page 45). Connect this input parameter with the "TIO_SYNC_Data" output parameter of the TIO_SYNC instruction.

* Checked once at startup of the CPU

Status parameter

Error codes or status information is output as double word at the Status output.

The double word is divided as follows:

Error code (DW#16#...)	Meaning
z0yywwww	Error of a system function: • during startup (z = 1) • during normal operation (z = 0) System functions with subordinate use are coded in yy: See table with error codes. wwww specifies the RET_VAL of the system function. The error information is available in the help for the system function.
z0yy0000	An error that does not originate in a system function. This error receives a consecutive error number yy. The error can occur: • during startup (z = 1) • during normal operation (z = 0)

Table with error codes

Error code (DW#16#...)	Meaning	Solution
00000000	No error.	—
10010000	The assigned number of the digital input at the Channel input parameter is outside the permitted range (depending on addressed module and channel configuration).	Correct the value at the Channel input parameter.
10020000	The TIO_DI instruction is not called in an isochronous OB. The instruction can only be used without errors in an isochronous OB.	Make sure that TIO_DI is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10030000	An error occurred when reading the HWID input parameter.	Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.
x0040000	The data in TIO_SYNC_Data is invalid/incorrect.	Check the TIO_SYNC instruction and the interconnection of its TIO_SYNC_Data output.
1005xxxx	An error has occurred during execution of the RD_SINFO system function. The low word xxxx displays the error information of the RET_VAL return value from RD_SINFO.	• Read the description of the RD_SINFO in the STEP 7 (TIA Portal) information system. • Make sure that TIO_DI is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10060000	No TIO module found. Possible cause: The module configured using the hardware identifier is not a TIO module.	• Make sure that the configured module is a TIO module. • Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration.
10070000	An internal error occurred during the address calculation.	Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.
00080000	TIO module is not synchronized using the TIO_SYNC instruction. The error code can also indicate that: • A job was already present before the first run of the instruction. • The assigned number at the Channel input parameter is not a digital input.	Check the instruction TIO_SYNC.
10090000	The read cycle time of the isochronous OB is outside the permitted range of $0 < T_{APP} <= 16$ ms and is therefore invalid. The instruction can only be used without errors in an isochronous OB.	• Correct the cycle time. • Make sure that TIO_DI is called in a "Synchronous Cycle" or "MC-PostServo" OB.
100A0000	The time T_O of the TIO model stored in TIO_SYNC_Data is outside the permissible range of $0 < T_o <= 4$ ms.	Check the instruction TIO_SYNC.
100Bxxxx	An error has occurred during execution of the RD_ADDR system function. The low word xxxx displays the error information of the RET_VAL return value from RD_ADDR.	Read the description of the RD_ADDR in the STEP 7 (TIA Portal) information system.
000C0000	The converted time stamp is invalid. Possible cause: Communication error	Check the communication with the TIO module.

Error code (DW#16#...)	Meaning	Solution
000D0000	The Quality Information of the digital input indicates that an error has occurred at the digital input.	Check the supply voltage L+/1L+/2L+.
000E0000	The assigned number at the Channel input parameter is not a digital input configured as Timer DI.	• Check the channel configuration (only for TM Timer DIDQ 24x24V). • Check the operating mode of the digital input.
000F0000	The assigned value at the EdgeSel input parameter is outside the valid range of 1 to 5.	Correct the value at the EdgeSel input parameter.
10100000	The send clock is outside the permitted range of 0 < SendClock <= 4 ms and is therefore invalid. The error code can also indicate that • The data in TIO_SYNC_Data is invalid or does not exist. • The TIO_DI instruction is not called in an isochronous OB.	Correct the send clock.
x0130000	MC-Servo (OB91) is not isochronous to the bus cycle time.	Correct the value of the cycle time of the MC-Servo to the value of the bus cycle time. Note: Calling TIO instructions in an OB of the type "MC-PostServo" with reduction ratio "MC-Servo" can result in incorrect calculation of time stamps.
10140000	The configured value at the HWID input parameter is not present in the structure at the TIO_SYNC_Data parameter. The HWID and TIO_SYNC_Data parameters are not consistent.	Correct the value at the HWID input parameter or the structure at the TIO_SYNC_Data parameter.
x0FF0000	General internal error.	—

4.3.3 TIO_DI_ONCE: Reading in edges once at the digital input and associated time stamps

Description

TIO_DI_ONCE detects the edges at a digital input of a TIO module **once** and returns the associated time stamps. Alternatively, you can use this instruction to control a timer DI channel that is configured as an edge-triggered enable for another channel.

Startup characteristics

During startup of the CPU, the instruction TIO_DI_ONCE applies the input parameters once and checks the following:

- Checking HWID
- Checking to see if the number of the digital input (Channel) is in the permitted range (depending on addressed module and channel configuration)
- Checking TIO_SYNC_Data.ERROR: Is an error present at TIO_SYNC?
- Checking TIO_SYNC_Data.TO_TIMES for plausibility (0 ms to 4 ms)
- Checking to see whether the OB is isochronous

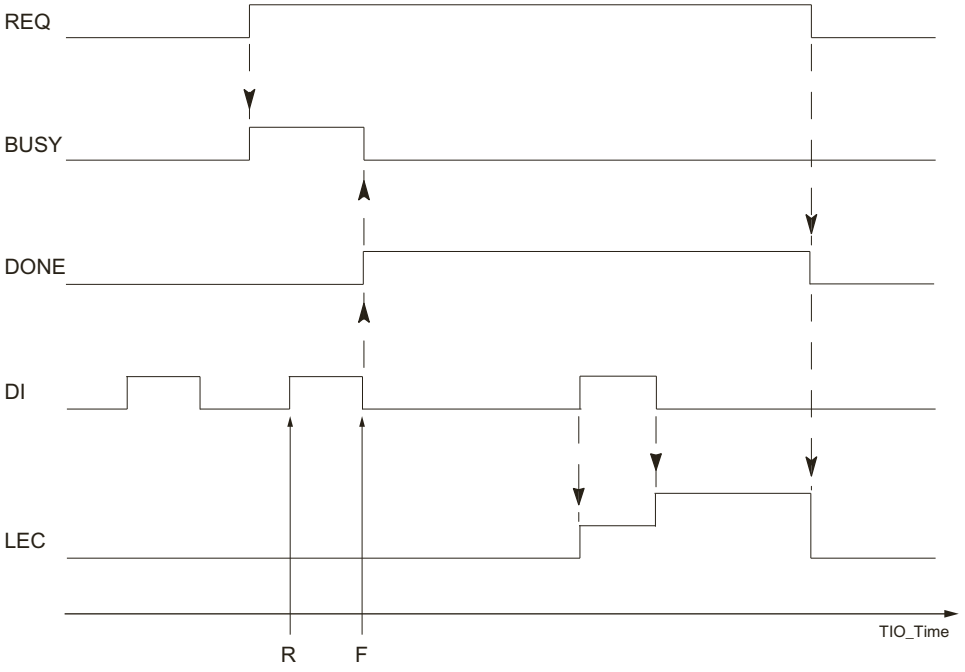
If startup takes place without errors, the instruction changes to normal operation. In the event of an error, the instruction does not change to normal operation and generates an error message.

Functional description: Time stamp detection

In normal operation, the instruction detects the edges at a digital input and the associated time stamps of the **first** valid, defined edge pair after the start of a read-in job. Use the input parameter EdgeSel to determine the edges for which time stamps are detected. To detect a new edge pair, a new positive edge is required at the REQ input parameter of the instruction.

You connect the input TIO_SYNC_Data with the output of the same name of the TIO_SYNC instruction. This ensures a shared time basis.

The figure below shows an example for the reaction of the bits DONE and BUSY at the start of a read-in job (EdgeSel = 4).



R Read-in time of the positive DI edge

F Read-in time of the falling DI edge

Functional description: edge-triggered enable

You can use this instruction to control a timer DI channel that is configured as an edge-triggered enable for another channel.

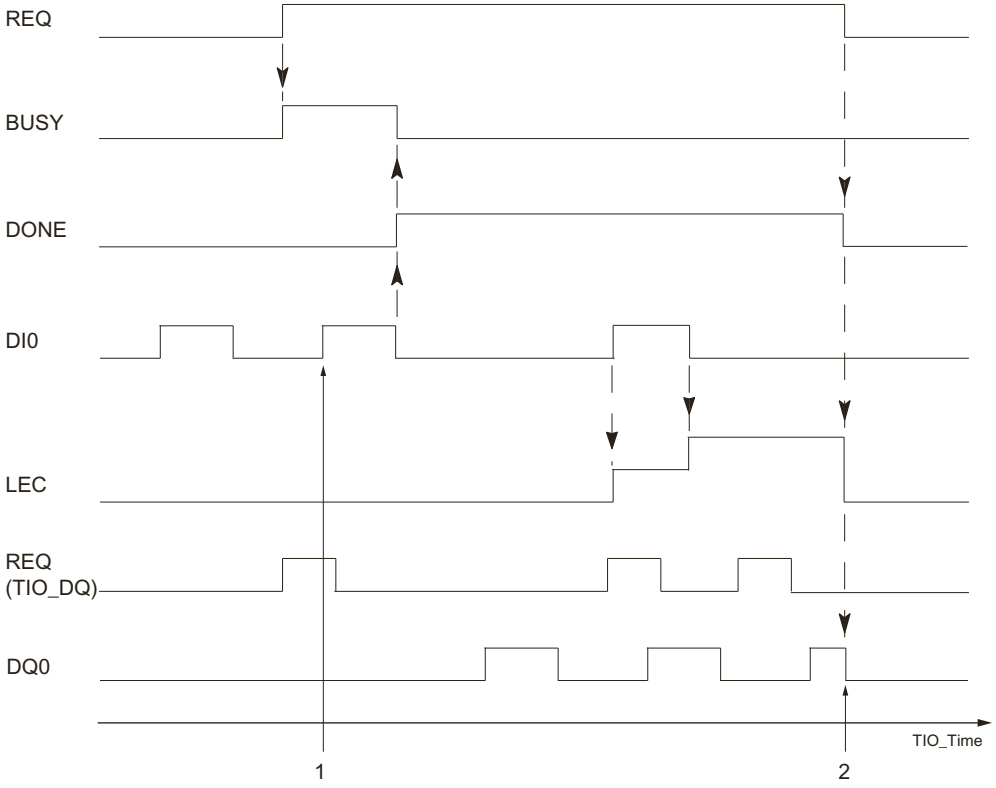
Example:

For a TIO module TM Timer DIDQ 10x24V, the following is configured in the hardware configuration for DQ0/DI0:

- Configuration DQ/DI group = timer DQ with enable
- HW enable by DI0 = edge-triggered
- DQ0 is not inverted

In this case, use the instruction TIO_DQ for DQ0 and the instruction TIO_DI_ONCE for DI0. You can control the enable by means of the input parameters REQ and EdgeSel of TIO_DI_ONCE. As soon as TIO_DI_ONCE has recorded a time stamp according to the value of EdgeSel, the enable is considered granted. You take the enable back by resetting REQ.

The following figure shows an example with EdgeSel = 4n (first positive, then falling edge). In this case the first valid positive edge at DI0 grants the enable for DQ0 after the start of a read-in job.



1 Start of enable at positive edge of enable input

2 End of enable when falling edge at REQ

If required, you can use the time stamps detected by the instruction for your application.

Reaction to error

The Error output indicates if the instruction was processed correctly. In the event of an error, the cause of the error is displayed at the Status output.

Parameter

The table below shows the parameters of the TIO_DI_ONCE instruction.

Parameter	Declaration	Data type	Default	Description
		S7-1500		
REQ	Input	Bool	False	Starts the job at a positive edge.
HWID*	Input	HW_IO	0	Hardware identifier for TIO module from hardware configuration
Channel*	Input	UInt	0	Number (0 ... m) of the digital input of the connected TIO module
EdgeSel	Input	UInt	3	Specify the edges for which time stamps are detected: 0_D: Invalid 1: Two rising edges

* Checked once at startup of the CPU

Parameter	Declaration	Data type S7-1500	Default	Description
				2: Two falling edges 3: Rising and falling edge (order depending on occurrence) 4: First rising, then falling edge 5: First falling, then rising edge 6 to 255: Invalid If edge-triggered enable is used, the following also applies: 1: Enable at first positive DI edge 2: Enable at first falling DI edge 3: Enable at first DI edge 4: Enable at first positive DI edge 5: Enable at first falling DI edge EdgeSel can be changed during normal operation.
DONE	Output	Bool	False	DONE = True: The job was completed without errors.
BUSY	Output	Bool	False	BUSY = True: The job has not yet been completed.
Error	Output	Bool	False	Error = True: An error has occurred. For detailed information see Status parameter. Error is reset as soon as the error is corrected.
Status	Output	DWord	16#0	Status of the instruction: see description of Status parameter
DI	Output	Bool	False	Status of digital input. If an inversion of the digital input is configured, this parameter is inverted as well.
TimeStampRE	Output	LTime	LT#0ns	Time stamp: EdgeSel = 1: The last but one read-in time at which a positive edge was detected (if *multiple* positive edges have occurred). EdgeSel = 2: The last read-in time at which a falling edge was detected (if *multiple* falling edges have occurred). EdgeSel = 3; 4; 5: The last read-in time at which a falling edge was detected.
TimeStampFE	Output	LTime	LT#0ns	Time stamp: EdgeSel = 1: The last read-in time at which a positive edge was detected (if *multiple* positive edges have occurred). EdgeSel = 2: The last but one read-in time at which a falling edge was detected (if *multiple* falling edges have occurred). EdgeSel = 3; 4; 5: The last read-in time at which a positive edge was detected.
LEC	Output	UInt	0	Counter: Number of edges for which no time stamp could be saved. The module can count a maximum of seven edges during REQ. The counter is reset with the falling edge at REQ.
TIO_SYNC_Data*	InOut	"TIO_SYNC_Data"		System time provided for the TIO instructions of the TIO modules by the TIO_SYNC instruction. See UDT TIO_SYNC_Data (Page 45). Connect this input parameter with the "TIO_SYNC_Data" output parameter of the TIO_SYNC instruction.
Initialized	Static	Bool	False	Instruction is initialized and ready

* Checked once at startup of the CPU

Status parameter

Error codes or status information is output as double word at the Status output.

The double word is divided as follows:

Error code (DW#16#...)	Meaning
z0yywwww	Error of a system function: • during startup (z = 1) • during normal operation (z = 0) System functions with subordinate use are coded in yy: See table with error codes. wwww specifies the RET_VAL of the system function. The error information is available in the help for the system function.
z0yy0000	An error that does not originate in a system function. This error receives a consecutive error number yy. The error can occur: • during startup (z = 1) • during normal operation (z = 0)

Table with error codes

Error code (DW#16#...)	Meaning	Solution
00000000	No error.	—
10010000	The assigned number of the digital input at the Channel input parameter is outside the permitted range (depending on addressed module and channel configuration).	Correct the value at the Channel input parameter.
10020000	The TIO_DI_ONCE instruction is not called in an isochronous OB. The instruction can only be used without errors in an isochronous OB.	Make sure that TIO_DI_ONCE is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10030000	An error occurred when reading the HWID input parameter.	Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.
x0040000	The data in TIO_SYNC_Data is invalid/incorrect.	Check the TIO_SYNC instruction and the interconnection of its TIO_SYNC_Data output.
1005xxxx	An error has occurred during execution of the RD_SINFO system function. The low word xxxx displays the error information of the RET_VAL return value from RD_SINFO.	• Read the description of the RD_SINFO in the STEP 7 (TIA Portal) information system. • Make sure that TIO_DI_ONCE is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10060000	No TIO module found. Possible cause: The module configured using the hardware identifier is not a TIO module.	• Make sure that the configured module is a TIO module. • Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration.
10070000	An internal error occurred during the address calculation.	Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.

Error code (DW#16#...)	Meaning	Solution
00080000	TIO module is not synchronized using the TIO_SYNC instruction. The error code can also indicate that: • A job was already present before the first run of the instruction. • The assigned number at the Channel input parameter is not a digital input.	Check the instruction TIO_SYNC.
10090000	The read cycle time of the isochronous OB is outside the permitted range of $0 < T_{APP} <= 16$ ms and is therefore invalid. The instruction can only be used without errors in an isochronous OB.	• Correct the cycle time. • Make sure that TIO_DI_ONCE is called in a "Synchronous Cycle" or "MC-PostServo" OB.
100A0000	The time T_O of the TIO model stored in TIO_SYNC_Data is outside the permissible range of $0 < T_o <= 4$ ms.	Check the instruction TIO_SYNC.
100Bxxxx	An error has occurred during execution of the RD_ADDR system function. The low word xxxx displays the error information of the RET_VAL return value from RD_ADDR.	Read the description of the RD_ADDR in the STEP 7 (TIA Portal) information system.
000C0000	The converted time stamp is invalid. Possible cause: Communication error	Check the communication with the TIO module.
000D0000	The Quality Information of the digital input indicates that an error has occurred at the digital input.	Check the supply voltage L+/1L+/2L+.
000E0000	The assigned number at the Channel input parameter is not a digital input configured as Timer DI.	• Check the channel configuration (only for TM Timer DIDQ 24x24V). • Check the operating mode of the digital input.
000F0000	The assigned value at the EdgeSel input parameter is outside the valid range of 1 to 5.	Correct the value at the EdgeSel input parameter.
10100000	The send clock is outside the permitted range of 0 < SendClock <= 4 ms and is therefore invalid. The error code can also indicate that • The data in TIO_SYNC_Data is invalid or does not exist. • The TIO_DI instruction is not called in an isochronous OB.	Correct the send clock.
x0130000	MC-Servo (OB91) is not isochronous to the bus cycle time.	Correct the value of the cycle time of the MC-Servo to the value of the bus cycle time. Note: Calling TIO instructions in an OB of the type "MC-PostServo" with reduction ratio "MC-Servo" can result in incorrect calculation of time stamps.
10140000	The configured value at the HWID input parameter is not present in the structure at the TIO_SYNC_Data parameter. The HWID and TIO_SYNC_Data parameters are not consistent.	Correct the value at the HWID input parameter or the structure at the TIO_SYNC_Data parameter.
x0FF0000	General internal error.	—

4.3.4 TIO_DQ: Output edges time-controlled at the digital output

Description

TIO_DQ enables a digital output of a TIO module to be switched at specified times.

Startup characteristics

During startup of the CPU, the instruction TIO_DQ applies the input parameters once and checks the following:

- Checking HWID
- Checking to see if the number of the digital input (Channel) is in the permitted range (depending on addressed module and channel configuration)
- Checking TIO_SYNC_Data.Error: Is an error present at TIO_SYNC?
- Checking TIO_SYNC_Data.TO_TIMES for plausibility (0 ms to 4 ms)
- Checking to see whether the OB is isochronous

If startup takes place without errors, the instruction changes to normal operation. The input parameters REQ, Out_Mode, TimeStampRE and TimeStampFE can be changed during normal operation. In the event of an error, the instruction does not change to normal operation and generates an error message.

Functional description

The instruction outputs edges time-controlled at a digital output during normal operation.

- At the time defined at the TimeStampRE input parameter, a positive edge is output at the digital output.
- At the time defined at the TimeStampFE input parameter, a falling edge is output at the digital output.

Depending on the program execution model, a time stamp must exceed the following value:

Program execution model	**TimeStampRE> ... TimeStampFE > ...**
IPO model	TIO_Time + T_{APP} + T_O
OIP model	TIO_Time + T_{APP} + SendClock + T_O

Use the input parameter Out_Mode to determine if only one edge or both edges are output.

You connect the input TIO_SYNC_Data with the output of the same name of the TIO_SYNC instruction. This ensures a shared time basis.

You start an output job with a positive edge at the REQ parameter. You can only start a new job when there is no error pending and no job is active. When the output job is started, the digital output is switched at the times defined with TimeStampRE and TimeStampFE.

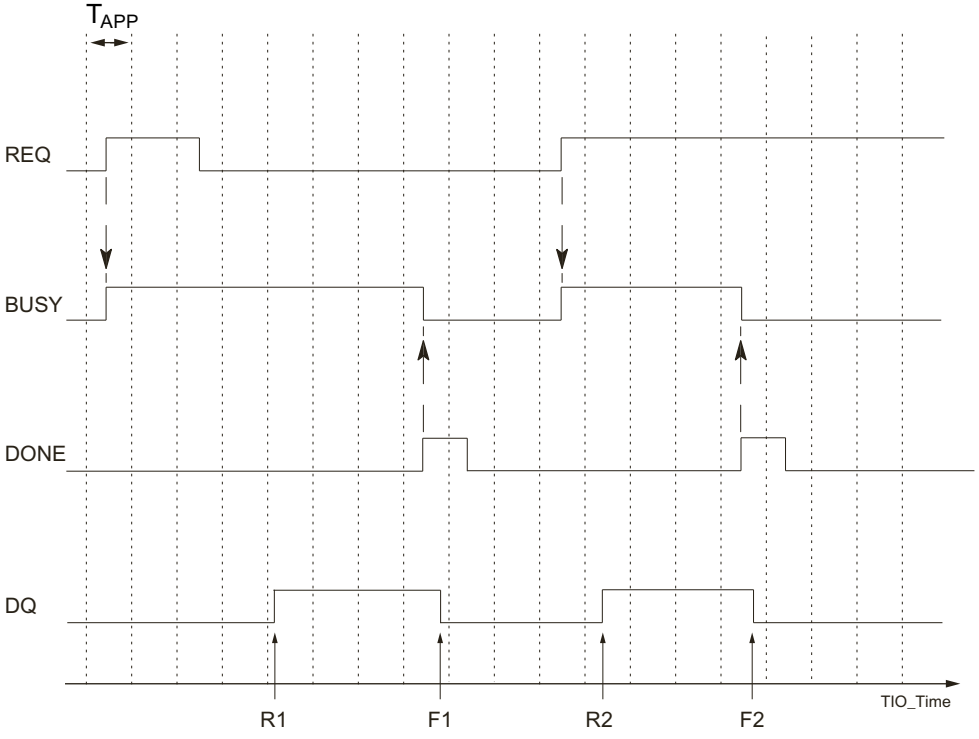
- If the digital output is already set at time TimeStampRE, the output job is not transferred to the module for the positive edge.
- If the digital output is not set at time TimeStampFE, the output job is not transferred to the module for the negative edge.

This means the digital output is not switched in both cases.

The job is done when the last application cycle is executed before the second output time is reached (DONE). Status and Error are constantly being updated during the job runtime. You can cancel an active output job by changing TimeStampRE or TimeStampFE to an invalid time stamp, e.g. LT#5µs.

The figure below shows an example for the reaction of the bits DONE and BUSY at the start of an output job under the following conditions:

- Out_Mode = 2 (both edges are output)
- The two time stamps are not changed between the start of the job and the output.



T_{APP}	Application cycle
R1, R2	Specified times of a positive DQ edge
F1, F2	Specified times of a falling DQ edge

NOTE

Once the job has been started with a positive edge at REQ, you can change the output times with a new input of TimeStampRE and TimeStampFE without having to restart the job.

Constraint:

If a changed time stamp is less than two application cycles before the output time (TimeStampRE - TIO_Time < 2*T_{APP} or TimeStampFE - TIO_Time < 2*T_{APP}), it is not taken into consideration. In this case, the last valid time stamp is used because it was already transferred to the TIO module.

NOTE

If you specify the same value for TimeStampRE and TimeStampFE, the instruction ignores the job and does not output an edge.

If you specify the value 0 for TimeStampRE or TimeStampFE, you can output the respective edge directly at the digital output with the input parameter Out_Mode = 3. This gives you the option to implement a direct control from the TIO module without time stamp in manual mode. You can use the direct control to interrupt an ongoing job.

Reaction to error

The Error output indicates if the instruction was processed correctly. In the event of an error, the cause of the error is displayed at the Status output.

Parameter

The table below shows the parameters of the TIO_DQ instruction.

Parameter	Declaration in library version		Data type	Default	Description
	< V2.0	≥ V2.0	S7-1500		
REQ	Input		Bool	False	Starts the job at a positive edge.
HWID*	Input		HW_IO	0	Hardware identifier for TIO module from hardware configuration
Channel*	Input		UInt	0	Number (0 ... m) of the digital output of the connected TIO module
Out_Mode	Input		UInt	2	Specify the output mode for the edges at the digital output: 0: Only rising edge is output (TimeStampRE). 1: Only falling edge is output (TimeStampFE). 2: Both edges are output (TimeStampRE and TimeStampFE). 3: Each edge is output directly if TimeStampRE = 0 or TimeStampFE = 0 If both time stamps have the value "0" or if no time stamp has the value "0", no edge is output. 4 to 255: Invalid
TimeStampRE	Input		LTime	LT#0ns	Time stamp: Time when a positive edge is to be output.
TimeStampFE	Input		LTime	LT#0ns	Time stamp: Time when a falling edge is to be output.
StatusDQ	Output		Bool	False	Actual status of the digital output. If an inversion of the digital output is configured, StatusDQ is inverted as well. StatusDQ shows the internal state of the digital output independent of the effect of any configured HW enable.
DONE	Output		Bool	False	DONE = True is displayed for one cycle: The job was completed without errors.
BUSY	Output		Bool	False	BUSY = True: The job has not yet been completed.
Error	Output		Bool	False	Error = True: An error has occurred. In this case, BUSY and DONE are set to False. For detailed information see Status parameter. Error is reset as soon as the error is corrected.
Status	Output		DWord	16#0	Status of the instruction: see description of Status parameter
TIO_SYNC_Data*	Input	InOut	"TIO_SYNC_Data"		System time provided for the TIO instructions of the TIO modules by the TIO_SYNC instruction. See UDT TIO_SYNC_Data (Page 45). Connect this parameter with the TIO_SYNC_Data output parameter of the TIO_SYNC instruction.

* Checked once at startup of the CPU

Status parameter

Error codes or status information is output as double word at the Status output.

The double word is divided as follows:

Error code (DW#16#...)	Meaning
z0yywwww	Error of a system function: • during startup (z = 1) • during normal operation (z = 0) System functions with subordinate use are coded in yy: See table with error codes. wwww specifies the RET_VAL of the system function. The error information is available in the help for the system function.
z0yy0000	An error that does not originate in a system function. This error receives a consecutive error number yy. The error can occur: • during startup (z = 1) • during normal operation (z = 0)

Table with error codes

Error code (DW#16#...)	Meaning	Solution
00000000	No error.	—
10010000	The assigned number of the digital output at the Channel input parameter is outside the permitted range (depending on addressed module and channel configuration).	Correct the value at the Channel input parameter.
10020000	The TIO_DQ instruction is not called in an isochronous OB. The instruction can only be used without errors in an isochronous OB.	Make sure that TIO_DQ is called in an OB of the type "Synchronous Cycle" or "MC-PostServo".
10030000	An error occurred when reading the HWID input parameter.	Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.
x0040000	The data in TIO_SYNC_Data is invalid/incorrect.	Check the TIO_SYNC instruction and the interconnection of its TIO_SYNC_Data output.
1005xxxx	An error has occurred during execution of the RD_SINFO system function. The low word xxxx displays the error information of the RET_VAL return value from RD_SINFO.	• Read the description of the RD_SINFO in the STEP 7 (TIA Portal) information system. • Make sure that TIO_DQ is called in a "Synchronous Cycle" or "MC-PostServo" OB.
10060000	No TIO module found. Possible cause: The module configured using the hardware identifier is not a TIO module.	• Make sure that the configured module is a TIO module. • Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration.
10070000	An internal error occurred during the address calculation.	Check the value at the HWID input parameter. Specify the hardware identifier of the TIO module from its module properties in the hardware configuration. An internal system constant of data type Hw_SubModule is available for the symbolic addressing.

Error code (DW#16#...)	Meaning	Solution
x0080000	TIO module is not synchronized using the TIO_SYNC instruction. The error code can also indicate that: • A job was already present before the first run of the instruction. • The assigned number at the Channel input parameter is not a digital output.	Check the instruction TIO_SYNC.
10090000	The read cycle time of the isochronous OB is LT#0ms or has as negative value and is therefore invalid. Correct the value. The instruction can only be used without errors in an isochronous OB.	• Correct the cycle time. • Make sure that TIO_DQ is called in a "Synchronous Cycle" or "MC-PostServo" OB.
100A0000	The time T_O of the TIO model stored in TIO_SYNC_Data is outside the permissible range of $0 < T_o <= 4$ ms.	Check the instruction TIO_SYNC.
100Bxxxx	An error has occurred during execution of the RD_ADDR system function. The low word xxxx displays the error information of the RET_VAL return value from RD_ADDR.	Read the description of the RD_ADDR in the STEP 7 (TIA Portal) information system.
000C0000	One or both time stamps at the TimeStampRE and TimeStampFE input parameters are invalid. The error is only signaled for the duration of one application cycle.	Check the TimeStampRE and TimeStampFE input parameters.
000D0000	The Quality Information of the digital output indicates that an error has occurred at the digital output.	• Check the parameter assignment of the digital output. • Check the supply voltage L+/1L+/2L+. • Check the wiring of the digital output for short-circuit, overload, and overtemperature.
000E0000	The number configured at the Channel input parameter is not a digital output configured as Timer DQ.	• Check the channel configuration (only for TM Timer DIDQ 24x24V). • Check the operating mode of the digital output.
100F0000	The read cycle time of the OB of type "Synchronous Cycle" is too long: $T_{APP} > 16$ ms.	Configure a smaller multiple of the send clock as the cycle time.
10100000	The send clock is outside the permitted range of 0 < SEND_CLOCK <= 4 ms and is therefore invalid. The error code can also indicate that • The data in TIO_SYNC_Data is invalid or does not exist. • The TIO_DQ instruction is not called in an isochronous OB.	Correct the send clock.
00110000	The assigned value at the Out_Mode input parameter is outside the valid range of 0 to 3.	Correct the value at the Out_Mode input parameter.
x0130000	MC-Servo (OB91) is not isochronous to the bus cycle time.	Correct the value of the cycle time of the MC-Servo to the value of the bus cycle time. Note: Calling TIO instructions in an OB of the type "MC-PostServo" with reduction ratio "MC-Servo" can result in incorrect calculation of time stamps.
10140000	The configured value at the HWID input parameter is not present in the structure at the TIO_SYNC_Data parameter. The HWID and TIO_SYNC_Data parameters are not consistent.	Correct the value at the HWID input parameter or the structure at the TIO_SYNC_Data parameter.
x0FF0000	General internal error.	—

4.3.5 UDT TIO_SYNC_Data

Description

The data type UDT TIO_SYNC_Data contains the central structure and data for synchronization of the modules and passing of the TIO_Time.

Parameter

Parameter	Data type	Description
	S7-1500	
TIO_TIME	LTime	Shared time basis (relative time) of the TIO modules
PIP_MODE	USInt	Mode for data update (is forwarded by the PIP_Mode input parameter of the TIO_SYNC instruction)
APP_CYC	LTime	Application cycle of the "MC-PostServo" or "Synchronous Cycle", "MC-PreServo" OB
SEND_CLOCK	LTime	Send clock of sync domain (is forwarded by the SendClock parameter of the TIO_SYNC instruction)
SYNC_MODULES	HW_IO array [1...8]	Hardware identifiers of the TIO modules from hardware configuration
TO_TIMES	UDInt-Array [1...8]	T_O for each TIO module:
TIO_TIME_BASE	LTime	Internal use
TBASE	LTime	
ERROR	Bool	

SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200AL
Designing interference-free controllers

Function Manual

Documentation guide 1

Basic information on electromagnetic compatibility 2

Interference-free cable routing 3

Cable shielding 4

Equipotential bonding 5

Special measures for interference-free operation 6

Lightning protection and overvoltage protection 7

06/2014
A5E03461486-AB

Preface

Purpose of the documentation

This documentation will support you in installing and commissioning programmable controllers.

Correct configuration is essential for fault-free operation of programmable controllers.

Basic knowledge required

The following knowledge is required in order to understand the documentation:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge of VDE (German Association for Electrical, Electronic and Information Technologies) and EC regulations
- Knowledge of the rules for installing controllers and switchgear

Conventions

You should also pay particular attention to notes such as the one shown below:

NOTE

A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.

Scope of the documentation

This documentation is valid for all products of the product series SIMATIC S7-1500, ET 200MP, ET 200SP and ET 200AL.

The product series SIMATIC S7-1500, ET 200MP and ET 200SP are approved for IP20 degree of protection, i.e. the modules of these product series must be installed in a control cabinet.

The SIMATIC ET 200AL product series is approved for IP65/IP67 degree of protection, i.e. the modules need **not** be installed in a control cabinet.

Changes compared to previous version

Changes / enhancements described in this manual, compared to the previous version (version 01/2013):

- Extension of the scope of validity to the distributed I/O system ET 200AL
- Supplement to the section Connection of the cable shielding for ET 200AL
- Components for lightning protection potential equalization amended

Additional support

Additional information on SIMATIC products is available on the Internet. The associated documentation is also available on the Internet.

- The range of technical documentation for the individual SIMATIC products and automation systems can be found on the Internet (http://www.siemens.com/simatic-tech-doku-portal).
- The online catalog and the ordering system are available on the Internet (http://mall.automation.siemens.com).

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security on the Internet (http://www.siemens.com/industrialsecurity).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find more information on the Internet (http://support.automation.siemens.com).

Table of contents

1 Documentation guide 5

2 Basic information on electromagnetic compatibility 6

2.1 Overview of possible interference 6

2.2 Coupling mechanisms 7

3 Interference-free cable routing 8

3.1 Classifying cables into cable categories 8

3.2 Cable routing inside cabinets in buildings 9

3.3 Cable routing outside cabinets and inside buildings 9

3.4 Cable routing outside buildings 10

3.5 Underground cable routing 10

3.6 Bending radii and tensile strength of cables 11

4 Cable shielding 13

4.1 Connecting the cable shielding for S7-1500 and ET 200MP 14

4.2 Connecting the cable shielding for ET 200SP 16

4.3 Connecting the cable shielding for ET 200AL 17

4.4 Connecting the cable shield for bus cables 18

4.5 Connecting the cable shield for other components 19

5 Equipotential bonding 20

6 Special measures for interference-free operation 22

7 Lightning protection and overvoltage protection 23

7.1 What is lightning and overvoltage protection? 23

7.2 Lightning protection zone concept 24

7.3 Rules and components for the transitions between lightning protection zones 26

Documentation guide

1

Introduction

The documentation of the SIMATIC products has a modular structure and covers diverse topics concerning your automation system.

The complete documentation for the S7-1500, ET 200SP, ET 200MP and ET 200AL systems consists of the respective system manuals, function manuals and product manuals.

The STEP 7 information system (online help) also supports you when configuring and programming your automation system.

Overview of documentation on the subject of designing interference-free controllers

The following table lists additional documentation which supplements this description of designing interference-free controllers.

Table 3-103 Documentation on the subject of designing interference-free controllers

Topic	Documentation	Most important contents
System description	System manual S7-1500 Automation System (http://support.automation.siemens.com/WW/view/en/59191792)	• Application planning • Installation • Wiring • Commissioning
	System manual ET 200SP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/58649293)	
	System Manual ET 200MP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/59193214)	
	System manual Distributed I/O System ET 200AL (http://support.automation.siemens.com/WW/view/en/89254965)	

SIMATIC manuals

All current manuals for SIMATIC products are available for download free of charge from the Internet (http://www.siemens.com/automation/service&support).

Basic information on electromagnetic compatibility 2

2.1 Overview of possible interference

Introduction

SIMATIC products and their components have been developed for use in industrial environment and meet the legal EMC requirements (EMC - Electromagnetic Compatibility). However, you still need to conduct an EMC assessment before installing your controller in order to identify possible sources of interference and to include these in your considerations.

Electromagnetic compatibility

Electromagnetic compatibility describes the ability of an electrical device to function properly in its particular electromagnetic environment. Neither the environment itself nor the electrical device are influenced in an unacceptable manner.

Possible interference

Electromagnetic interference can influence an automation system in various ways. The most significant interferences and their causes are as follows:

- Electromagnetic fields having a direct influence on the system
- Interference coupling caused by bus signals (for example, PROFINET)
- Interference influencing the system via the process wiring
- Interference which reaches the system via the power supply and/or protective ground

The figure below shows the likely paths of electromagnetic interference.

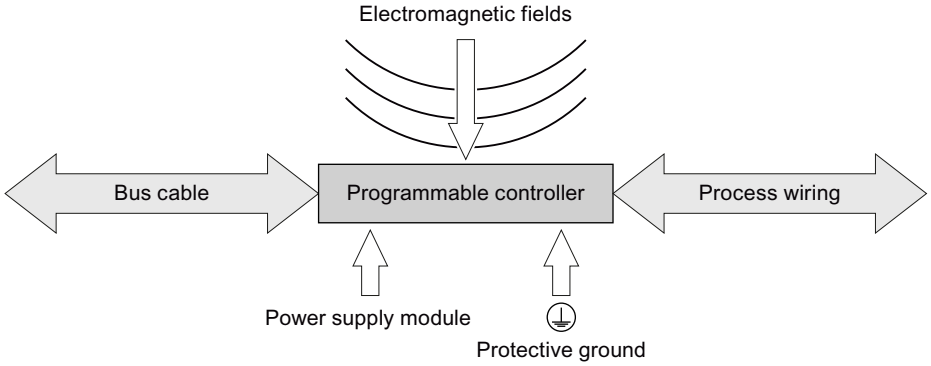


Figure 3-622 Electromagnetic interference

2.2 Coupling mechanisms

Depending on the emitting medium and the distance between the source of interference and the device, interference can reach the automation system via four different coupling mechanisms.

The following table shows possible causes and typical sources of interference for the various coupling mechanisms:

Table 3-104 Coupling mechanisms

Coupling mechanism	**Cause**	**Typical sources of interference**
Galvanic coupling	Two electric circuits share the same cable	• Clocked devices (influence on the network due to converters and third-party power supply units) • Starting motors • Potential differences on component enclosures with shared power supply
Capacitive coupling	Potential difference between conductors	• Interference coupling due to parallel routing of signal cables • Static discharge of the operator
Inductive coupling	Mutual influencing of current-carrying conductor loops. The magnetic fields caused by the current flow induce interference voltages.	• Transformers, motors, electrical welding equipment • Power supply cables routed in parallel • Cables whose currents are switched • High-frequency signal cables • Unwired coils
Radiation coupling	Effect of an electromagnetic wave on a cable configuration. This wave induces currents and voltages.	• Neighboring transmitters (for example, walkie-talkies) • Spark gaps (spark plugs, collectors of electrical motors, welding devices)

Interference-free cable routing

3

This chapter describes the EMC-compatible classification of cables and cable routing for bus, data, signal and supply lines.

3.1 Classifying cables into cable categories

Classify the cables into cable categories according to their sensitivity to interference coupling and interference emission. The further away from one another cables of different cable categories are installed, the lower the mutual influence by capacitive and inductive coupling.

The following table shows the cable categories into which you can classify your cables accordingly.

Table 3-105 Cable categories

Category A	• Signal lines to I/O modules • Bus and data lines (for example, PROFIBUS, PROFINET) • Lines to HMI devices • Supply lines for extra-low voltages (< 24V DC or < 60V AC)
Category B	• Supply lines with safe electrical isolation (SELV) • Supply voltages < 400 V
Category C	• Supply voltages > 400 V

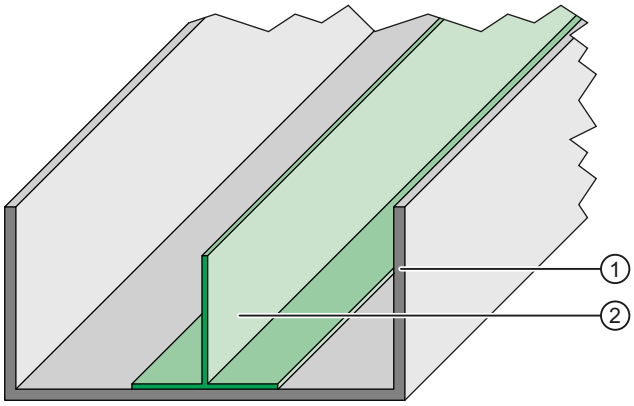
The following table shows the minimum clearance you must maintain when installing cables.

Table 3-106 Combination of cable categories

	Category A	Category B	Category C
Category A	• In common bundles or cable channels	• In separate bundles or cable channels (no minimum clearance necessary)	• Inside cabinets in separate bundles or cable channels • Outside cabinets, but inside buildings, on separate cable racks with at least 10 cm clearance
Category B	• In separate bundles or cable channels (no minimum clearance necessary)	• In common bundles or cable channels	
Category C	• Inside cabinets in separate bundles or cable channels • Outside cabinets, but inside buildings, on separate cable racks with at least 10 cm clearance		• In common bundles or cable channels

If you install different cable categories in the same cable channel, use metallic cable channels with metallic partition.

The following figure show a schematic view of a cable channel with partition.



① Metallic cable channel
② Metallic partition

Figure 3-623 Cable channel with partition

3.2 Cable routing inside cabinets in buildings

Rule

Observe the following rules for proper cable routing inside of control cabinets:

- If a crossing of cables is unavoidable, then cross the cables at an angle of 90°, if possible, in order to keep interference from electrical fields as low as possible.
- Do not route cables coming into the cabinet from outside parallel to the shield supports.

3.3 Cable routing outside cabinets and inside buildings

Rule

Observe the following rules for proper cable routing outside control cabinets and inside buildings:

- Read the information in section Assigning cables to cable categories (Page 8).
- If you route the cables in metallic cable channels, you can rearrange the cable channels next to each other.
- Connect metallically conductive cable racks to the potential equalization of the building.
- If a crossing of cables is unavoidable, then cross the cables at an angle of 90°, if possible, in order to keep interference from electrical fields as low as possible.

3.4 Cable routing outside buildings

If possible, lay the cables outside buildings on metallic cable holders. Connect the cable holder joints galvanically to each other and ground the cable holders.

Rule

Observe the following rules when laying cables outside of buildings:

- Use metallic auxiliary terminal boxes to connect cables coming from outside at the junction to cables inside the building. Ground these boxes.
- If a crossing of cables is unavoidable, then cross the cables at an angle of 90°, if possible, in order to keep interference from electrical fields as low as possible.
- Integrate bus cables installed outside of buildings into your lightning and overvoltage concept.

Lightning protection

When you lay cables for SIMATIC devices outside of buildings, you have to take internal and external lightning protection measures.

Reference

For additional information about lightning protection, refer to chapter Lightning protection and overvoltage protection (Page 23).

3.5 Underground cable routing

Rule

Observe the following rules for underground cable routing:

- Lay the cable at least 60 cm below the ground surface.
- Install equipotential bonding approximately 20 cm above the cable. You can use a zinc-plated ground strip, for example. The ground strips also serve as protection against lightning strikes.
- Protect the cable against mechanical damage by, for example, using a plastic pipe and/or a cable warning tape in the ground, approximately 40 cm above the cable.
- Separate the various cable categories in the ground using cable channels, for example.

The following figure shows the arrangement of cable warning tape, equipotential bonding and a cable.

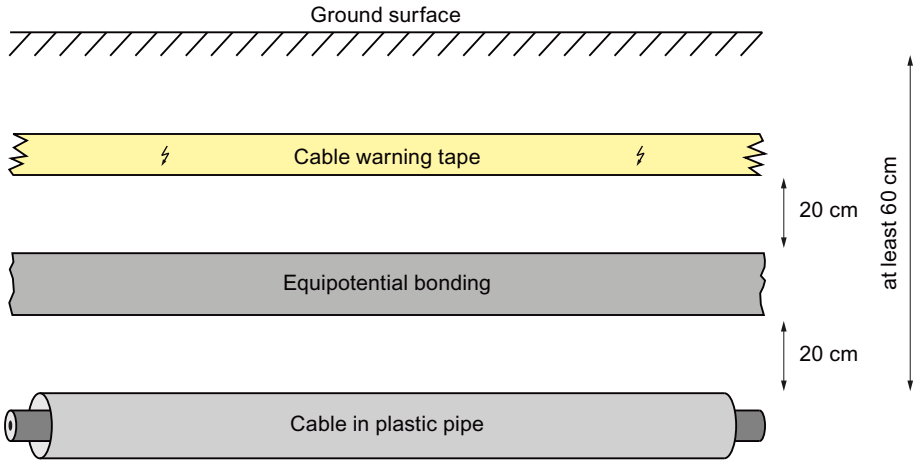


Figure 3-624 Arrangement underground

Lightning protection

When you lay cables for SIMATIC devices outside of buildings, you have to take internal and external lightning protection measures.

Reference

For additional information about lightning protection, refer to chapter Lightning protection and overvoltage protection (Page 23).

3.6 Bending radii and tensile strength of cables

Tensile strain

A high strain on the cables due to tensile forces leads to conductor material flow. The tensile forces thus cause a change in the structure of the material and lower the conductor cross-section. This decrease of the conductor cross-section leads, in turn, to a heating of the conductor and premature wear of the conductor insulation.

Use the supplied cable ties to relieve the terminal points on the plugs for the I/O modules of the product series SIMATIC S7-1500 and SIMATIC ET 200MP.

Bending radius

If you select too small bending radii when laying cables, this will cause the materials to stretch and compress and changes the mechanical structure of the cables. The electrical properties are impaired as a result.

Pay particular attention to the bending radii of fiber-optic cables. If the bending radii are too small, the optical properties of the fiber-optic cable are adversely affected. Reliable transmission is no longer guaranteed.

Cable shielding

4

Shielding is a measure to attenuate (dampen) magnetic, electrical or electromagnetic interference fields.

Interference currents on cable shields are diverted from the shield connection to ground. To avoid interference as a result of these currents, it is imperative to provide a low-impedance connection to the protective conductor.

Rules

Ideally, you should use cables equipped with a protective braided shield. The shield's contacting must be more than 80% at the contact point. Avoid tensile and compression strain on cables with a foil shield. This type of strain can damage the foil shield very slightly at the fastening point. The result is a reduced shielding effect.

Shield connection with grounding at both ends

Always connect the cable shields to the ground at both ends. Low and high frequency interference can be reduced only by connecting both ends of the shield to the ground.

NOTE

Laying an additional equipotential bonding cable

Whenever potential differences develop between the grounding points, an equalizing current flows on a shielding that is connected at both ends. In this case, lay an additional equipotential bonding cable. You can find more information on this topic in the chapter Equipotential bonding (Page 20).

Shield connection with capacitive grounding at one end

If you do not have the option of installing equipotential bonding (in plants covering a large area, for example), connect capacitive grounding to one end of your shield. In this case, only high-frequency interference will be reduced.

The following figure shows the capacitive grounding of a cable shield. The values indicated in the figure are indicative and will differ from system to system. The capacity diverts the high-frequency interference. This capacity provides high-impedance protection for the power frequency (50 or 60 Hz), thus preventing equalizing currents via the shield. A parallel switched high-impedance resistance prevents the capacity from loading a direct current.

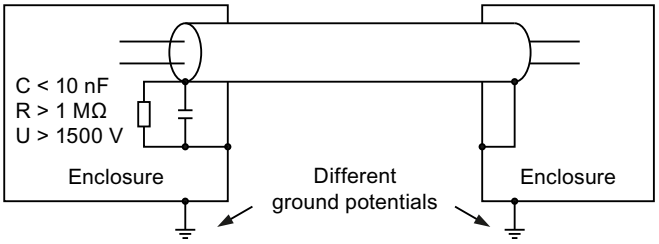


Figure 3-625 Capacitive grounding of the shield

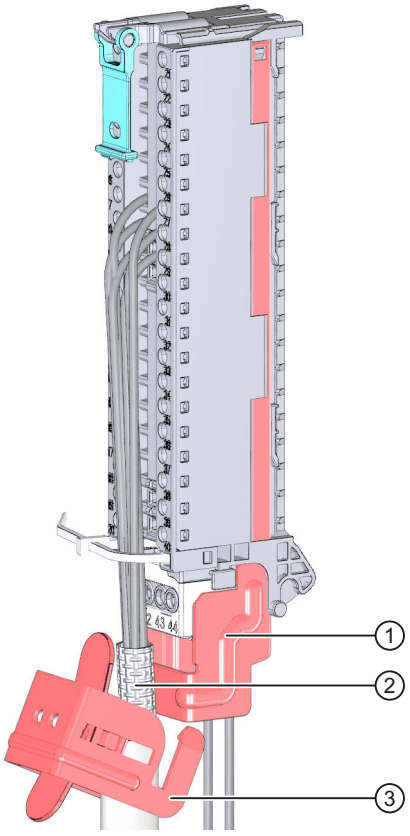
4.1 Connecting the cable shielding for S7-1500 and ET 200MP

A special shield design has been developed for the automation system S7-1500 and the distributed I/O system ET 200MP for the shield connection of the signal lines. The connection element for the cable shield consists of a shield clamp and a shield terminal.

If the front connector is located in the module, the interference currents which occur are diverted by the connection element to the ground via the module and mounting rail.

The shield clamp is a pluggable mount for the analog and technology modules. The shield clamp allows the low-impedance application of cable shields with minimum installation times.

The following figure shows a front connector with mounted shield clamp and associated shield terminal.



① Shield clamp
② Stripped cable shield
③ Shield terminal

Figure 3-626 Shield clamp and shield terminal on front connector

The shield clamp is inserted from below onto the front connector until the shield clamp latches audibly. The shield terminal is fastened to the shield clamp.

Additional information

For additional information on installing the shield clamp and shield terminal, refer to the "Connecting front connectors" chapter in the S7-1500 automation system (http://support.automation.siemens.com/WW/view/en/59191792) or ET 200MP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/59193214) system manuals.

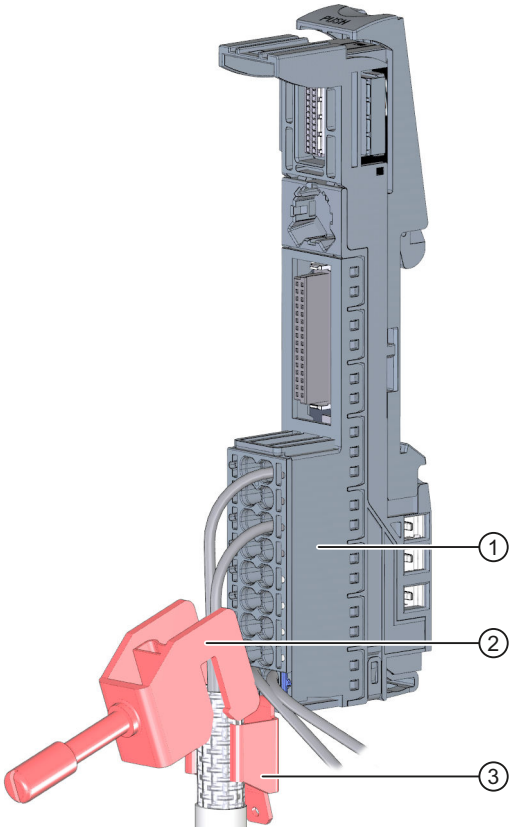
4.2 Connecting the cable shielding for ET 200SP

A special shield design has been developed for the shield connection of the signal lines of the ET 200SP distributed I/O system. The connection element for the cable shield consists of a shield terminal.

If the front connector is located in the module, the interference currents that occur are diverted by the connection element via BaseUnit and mounting rail to the ground.

The shield terminal is plugged into a mount of the BaseUnit. The shield terminal allows the low-impedance application of cable shields with minimum installation times. There is no need for the otherwise standard connection of the cable shield at the cabinet entry.

The following figure shows a BaseUnit with shield terminal and shield support.



① BaseUnit of ET 200SP
② Shield terminal
③ Shield support with flat plug for terminal sockets

Figure 3-627 BaseUnit with shield terminal

Additional information

For more information on mounting the shield terminal, refer to the "Connecting cable shields" chapter of the system manual ET 200SP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/58649293).

4.3 Connecting the cable shielding for ET 200AL

Each module of the ET 200AL distributed I/O system features a functional ground connection.

Use only shielded cables for connection of analog signals, PROFINET and PROFIBUS signals and for the ET-Connection. If you have screwed the plug in correctly, the interference currents that occur are diverted to the metal parts and functional ground.

If you attach an ET 200AL module to a **conductive**, grounded base, the lower mounting bolt establishes a conductive connection to the earth potential.

If you attach an ET 200AL module to a **non-conductive** base, connect the lower mounting bolt to the ground wire at the same time.

The following figure shows how to connect the functional ground via a ground wire, using the IM 157-1 PN interface module as an example.

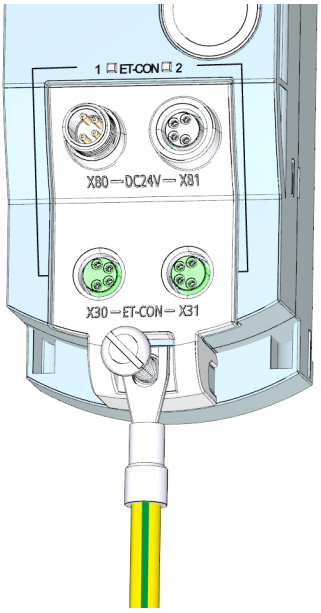


Figure 3-628 Connect functional ground via a ground wire

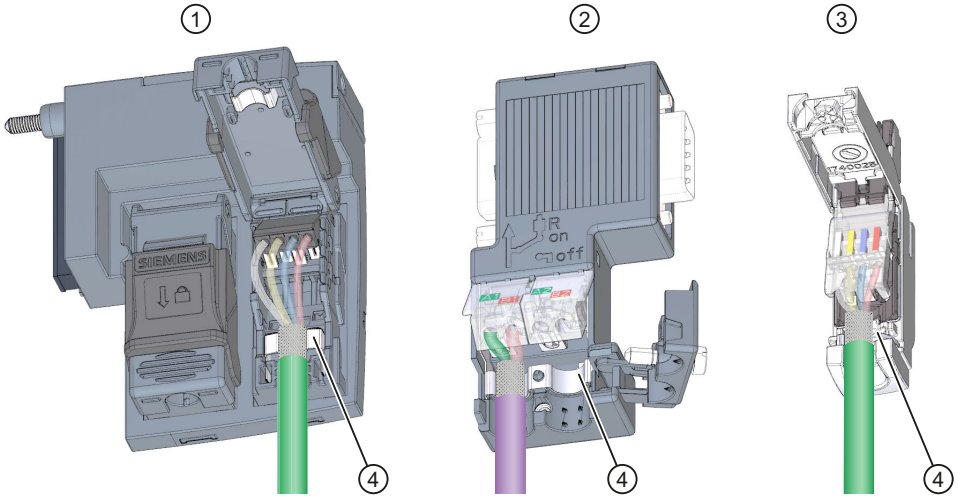
Additional information

You can find more information on installing ET 200AL modules in the Installing Modules section of the system manual Distributed I/O System ET 200AL (http://support.automation.siemens.com/WW/view/en/89254965).

4.4 Connecting the cable shield for bus cables

In the S7-1500, ET 200MP and ET 200SP systems, the cable shields of PROFIBUS and PROFINET cables are connected to the existing bus connection elements. Cable shield and shield support are thus galvanically connected to each other. If the connector is plugged into the module, the coupled interferences are diverted via the module carrier to the ground. There is no need for the otherwise standard connection of the shield at the cabinet entry.

The following figure shows examples of the shield connection for various bus connection elements.



① BusAdapter BA 2xRJ45 for ET 200SP
② PROFIBUSconnector, 9-pin D-Sub
③ PROFINETconnector RJ45
④ Shield support of respective connector

Figure 3-629 Shield connection for bus connection elements

Reference

For more information on installing the connectors, refer to the "Connecting PROFINET IO BusAdapter BA 2xRJ45 to the interface module" chapter of the system manual ET 200SP Distributed I/O System (http://support.automation.siemens.com/WW/view/en/58649293) and to the supplied product information.

4.5 Connecting the cable shield for other components

The following procedures for connecting the shield to devices that do not have any special shield terminals have proven themselves in practice.

Rule

Note the following points when handling the shield:

- Always use metal clamps to mount the protective braided shields of the cables. The clamps must cover a large area of the shield and provide appropriate contact force.
- Attach the shield to a shielding bus directly after the point where the cable enters the cabinet. If you route the shield further to the module, do not connect the shield again in front of the module, as this would create ground loops.

The following figure shows standard types of shield fastening.

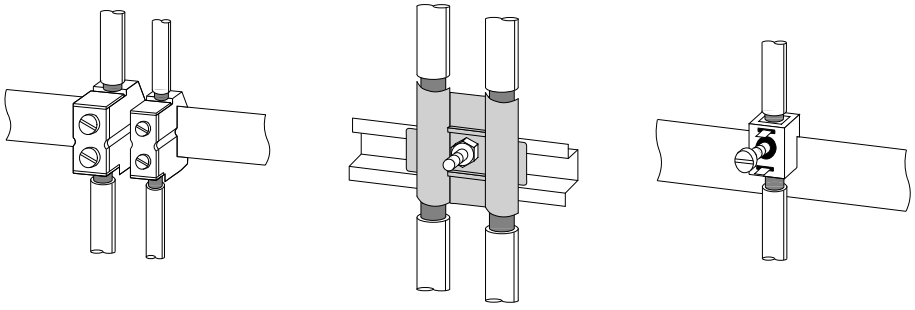


Figure 3-630 Cable shielding

Equipotential bonding

5

Definition according to DIN VDE 0100

Equipotential bonding is an electrical connection which brings the bodies of electrical equipment and external conductive parts to the same, or nearly the same, potential.

Equipotential bonding is divided into:

- Main equipotential bonding
- Additional local equipotential bonding

Both versions of equipotential bonding are of great importance not only for protection against electric shock, but also for EMC.

Main equipotential bonding

Main equipotential bonding is required by DIN VDE 0100 Part 410 as a protective measure and is mandatory, regardless of other measures for protection against direct and indirect contact.

Additional local equipotential bonding

Additional local equipotential bonding is required if:

- Unfavorable grounding conditions exist between plant parts due to different conductivity of the soil (for example, sandy or stony ground)
- Cables bridge a large distance
- Electrical energy is fed in from various power supplies (for example, in the case of multiple substations)
- Considerable electrical power is used (for example, welding robots, large drives)

Measures

In such cases, an additional equipotential bonding cable between the individual potentials can solve the problem. The equipotential bonding cable must also be able to divert large currents and carry lightning stroke current. The following equipotential bonding systems have proven themselves in practice:

- 16 mm^2 for copper equipotential bonding cables up to 200 m long
- 25 mm^2 for copper equipotential bonding cables over 200 m long

To prevent ground loops, equipotential bonding cables are installed in parallel and, whenever possible, near to the signal/bus cable. This allows the area between the two cables to be kept as small as possible.

The following figure shows a schematic view of the installation of an equipotential bonding cable.

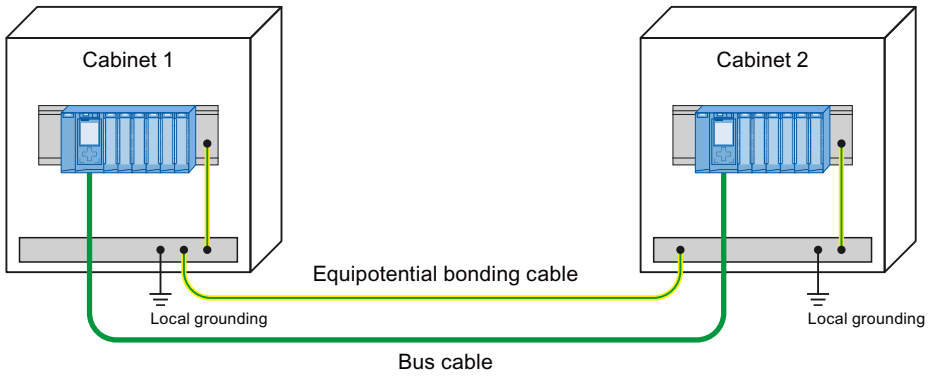


Figure 3-631 Installation of equipotential bonding cables

Rule

Note the following issues regarding equipotential bonding:

- The lower the impedance of an equipotential bonding cable, the more effective is equipotential bonding. The impedance of the additionally installed equipotential bonding cable should not exceed 10% of the shield impedance.
- Connect the equipotential bonding cables to a large area of the grounding system.
- Protect the connection points against corrosion.
- Avoid ground loops.
- Install the equipotential bonding cables in such a way as to minimize the areas enclosed between the equipotential bonding cables and signal lines.

Special measures for interference-free operation

6

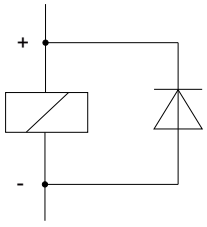
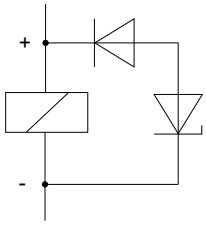
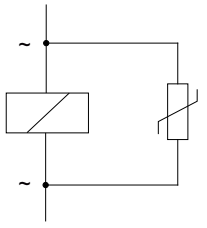
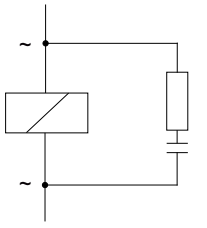
Connecting inductances to quenching elements

Ideally, the inductances (for example, contactor or relay coils) controlled by SIMATIC do not require any wiring to external quenching elements. The required quenching elements are already integrated into the modules.

If the SIMATIC output circuit can also be switched off by built-in contacts (such as relay contacts for EMERGENCY OFF), the module's integrated quenching elements are no longer effective. In this case, the inductances must be wired to quenching elements.

Wire inductances to freewheeling diodes, varistors or RC elements, for example.

Table 3-107 Wiring inductances

Wiring DC-operated inductances		Wiring AC-operated inductances	
with diode	with Z diode	with varistor	with RC element
			

Programming devices

Provide a socket in each cabinet for the supply of the programming devices. The sockets are supplied from the distribution board to which the protective conductor for the cabinet is also connected.

Observe the following points during the installation of the socket in the control cabinet:

- Include the grounding of the socket in your consideration of the equipotential bonding.
- The common star point of the two ground potentials (cabinet and socket) must be close to the two end points.
- An equipotential bonding cable is not permitted as communication cable between programming device and controller.

Lightning protection and overvoltage protection 7

7.1 What is lightning and overvoltage protection?

Introduction

The term "Lightning and overvoltage protection" covers both the concept and system for the protection of structural systems (such as buildings or electrical equipment). This concept also includes the protection of people and animals.

Overvoltages are most frequently caused by lightning strikes.

Lightning protection system

The lightning protection system is the complete system used to reduce physical damage to a structural system as a result of direct lightning strikes and overvoltages. The lightning protection system is divided into external and internal lightning protection.

External lightning protection

External lightning protection is part of the lightning protection system and comprises an interception device, an arrester and a grounding system. In the event of a lightning strike, the external lightning protection serves to divert the lightning current safely to the ground. This measure most frequently prevents fire damage.

Internal lightning protection

Internal lightning protection is part of the lightning protection system and comprises lightning protection equipotential bonding and/or electrical isolation with respect to the external lightning protection. In the event of a lightning strike, the internal lightning protection reduces the damage caused by overvoltages resulting from the lightning.

Even at larger distances of up to 1.5 km, lightning strikes can sometimes still cause damage. You obtain effective lightning protection by expanding the external lightning protection into an overall protection system. This system includes equipotential bonding and surge protection devices.

7.2 Lightning protection zone concept

Introduction

Each building requires a coordinated protection zone concept. The grading of the protection is of key importance for this. Sufficient protection can only be guaranteed if this grading requirement is satisfied.

The lightning protection zone concept described in the standards IEC 62305-4 and DIN EN 62305-4 is used for this purpose. The lightning protection zone concept groups devices and areas that have the same risk potential and can be wired to arresters of the same type.

Use overvoltage protection devices at the transitions of the lightning protection zones based on the requirements. Install the overvoltage protection devices at an appropriate location such as the main or sub-distribution board.

Principle of the lightning protection zone concept

The principle behind the lightning protection zone concept is the division of the areas to be protected from overvoltages, for example buildings, into lightning protection zones based on EMC considerations.

Schematic diagram of the lightning protection zone concept

The following is a schematic diagram of the lightning protection zone concept in a physical structure.

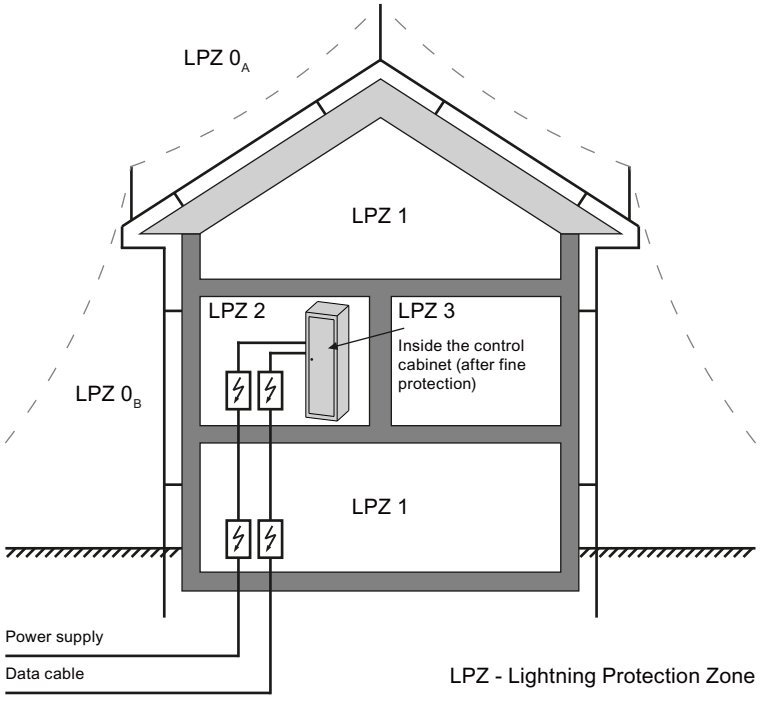


Figure 3-632 Division of a structural system into lightning protection zones

Division of lightning protection zones

The various lightning protection zones (LPZ - Lightning Protection Zone) are limited spatially as follows and not necessarily by physical boundaries, such as walls or floors.

The following table explains the division into various lightning protection zones.

Table 3-108 External and internal lightning protection zones

Lightning protection zones	
External lightning protection zones:	
LPZ 0_A	• Risk from direct lightning strikes • Risk from the full electromagnetic field of the lightning
LPZ 0_B	• Protected against direct lightning strike • Risk from the full electromagnetic field of the lightning
Internal lightning protection zones:	
LPZ 1	• Protected against direct lightning strike • Attenuated electromagnetic field of the lightning
LPZ 2	• Protected against direct lightning strike • Reduced leakage currents and electromagnetic fields compared to LPZ 1 • Protected terminal devices
LPZ 3	• Protected against direct lightning strike • Protected area inside the terminal device • Local equipotential bonding

Effects of the lightning strike

Direct lightning strikes occur in the lightning protection zone LPZ 0_A. Effects of the lightning strike are high-energy lightning currents and strong electromagnetic fields. These effects are reduced from one lightning protection zone to the next through suitable lightning current or overvoltage arrester/shielding measures.

Frequent damage caused by lightning strikes includes:

- Injury to people and animals, which may in worst cases lead to death
- Damage to buildings
- Fire caused by strong heat development of a lightning strike

Overvoltages

Electromagnetic fields of the lightning channel can be reduced with appropriate shielding measures. Overvoltages due to inductions can be reduced to a safe level starting in lightning protection zone LPZ 0_B with overvoltage arresters.

7.3 Rules and components for the transitions between lightning protection zones

Introduction

This chapter provides you with information on the rules for transitions between lightning protection zones. Measures must be taken to reduce the surge current load and the magnetic fields at the transitions between the lightning protection zones.

Each zone-penetrating metallic/electrical system is incorporated into the equipotential bonding at the zone transition.

The metallic systems include channels, structural parts, and pipes (for water, gas, and heat, for example).

Electrical systems include power and IT cables and wires (for example, power cables and bus cables).

Transitions between lightning protection zones

Overvoltage protection must be provided at the transitions between lightning protection zones (LPZ - Lightning Protection Zone) in accordance with DIN EN 62305. The protection levels are defined at the transitions and implemented by means of overvoltage protection devices (SPD - Surge Protective Device).

- SPD Type 1 - Coarse protection for the transition from LPZ 0 to LPZ 1
- SPD Type 2 - Medium protection for the transition from LPZ 1 to LPZ 2
- SPD Type 3 - Fine protection for the transition from LPZ 2 to LPZ 3

The following figure illustrates the lightning protection zones and the type classes from the supply line to the consumer.

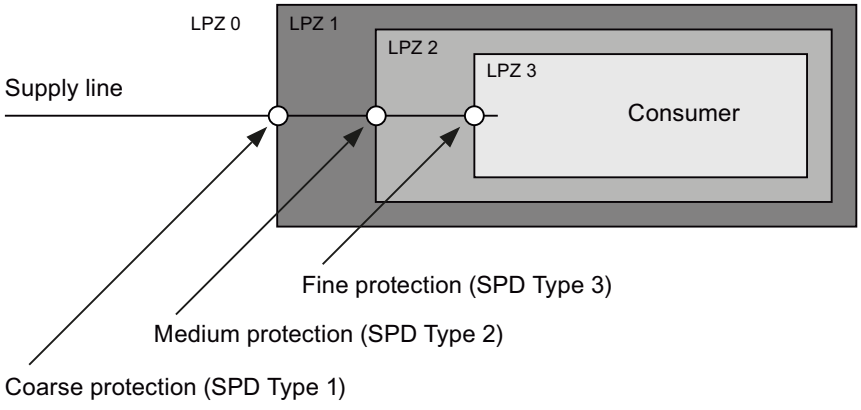


Figure 3-633 Lightning protection zone transitions

Rule for transition from lightning protection zone 0_A to 1

Lightning protection equipotential bonding is required at the transition from lightning protection zone 0_A to 1. The following applies to the transition at the interface of lightning protection zone 0_A to 1:

- Use of lightning arresters prevents introduction of partial lightning currents into structural systems
- Creation of local equipotential bonding at the transition of lightning protection zones, with incorporation of metallic supply systems (for example, pipes, air ducts, cable channels or cable ducts)

Components for lightning protection equipotential bonding from lightning protection zone 0_A to 1

The following table shows components for lightning protection equipotential bonding from lightning protection zone 0_A to 1.

Table 3-109 Components for transition from lightning protection zone 0_A to 1

Seq. no.	Cables for ...	Connection at the 0_A interface to 1 with:	
		S7-1500/ET 200MP/ET 200SP/ET 200AL	Article number
1	Three-phase TN-C system	DEHNventil® DV M TNC 255	951 300
		DEHNventil® DV M TNC 255 FM *	951 305 *
2	Three-phase TN-S system	DEHNventil® DV M TNS 255	951 400
		DEHNventil® DV M TNS 255 FM *	951 405 *
3	Three-phase TT system	DEHNventil® DV M TT 255	951 310
		DEHNventil® DV M TT 255 FM *	951 315 *
4	AC TN-S system	DEHNventil® DV M TN 255	951 200
		DEHNventil® DV M TN 255 FM *	951 205 *
5	AC TT system	DEHNventil® DV M TT 2P 255	951 110
		DEHNventil® DV M TT 2P 255 FM *	951 115 *
6	Supply U_N = 24 V DC	BLITZDUCTOR® XT, base section BXT BAS	920 300
		BLITZDUCTOR® XT, module BXT ML2 B 180 (I_L = 1.2 A) (2-wire)	920 211
7	Supply U_N = 24 V DC	DEHNbloc® M, DB M 1 150	961 110
		DEHNbloc® M, DB M 1 150 FM * (2 pieces required)	961 115 *
8	Bus cable MPI RS 485, RS 232 (V.24)	BLITZDUCTOR® XT, base section BXT BAS	920 300
		BLITZDUCTOR® XT, module BXT ML2 B 180 (2-wire)	920 211
9	Inputs/outputs of digital modules U_N = 24 V DC	BLITZDUCTOR® XT, base section BXT BAS	920 300
		BLITZDUCTOR® XT, module BXT ML4 B 180 (I_L = 1.2 A) (4-wire)	920 310
10	Inputs/outputs of digital modules U_N = 230 V AC	DEHNbloc® M, DB M 1 255	961 120
		DEHNbloc® M, DB M 1 255 * (2 pieces required)	961 125 *

Seq. no.	Cables for ...	Connection at the 0_A interface to 1 with:	
		S7-1500/ET 200MP/ET 200SP/ET 200AL	Article number
11	Inputs/outputs of analog modules (e.g., 4-20 mA, 1-10 V)	BLITZDUCTOR® XT, base section BXT BAS	920 300
		BLITZDUCTOR® XT, module (I_L = 1.2 A) (4-wire)	920 310
* Version with remote indication contact Components of the series BLITZDUCTOR® XT can be remotely monitored with the appropriate accessories. Additional information is available on the Internet (http://www.dehn.de) **Components can be ordered directly from:** DEHN+SÖHNE GMBH+CO.KG. Hans-Dehn-Straße 1 D-92318 Neumarkt			

Rule for the transition from lightning protection zone 0_B to 1, 1 to 2, or 2 to 3

The transition from lightning protection zone 0_B to 1, 1 to 2, or 2 to 3 prevents strong electromagnetic coupling and serves as overvoltage protection. The following applies to the transition at the interface from lightning protection zone 0_B to 1, 1 to 2, or 2 to 3:

- Use of power cables with surge current-carrying cable shields or twisted-pair IT cables
- Laying cables and lines
  - In continuous, surge current-carrying metal pipes that are grounded at both ends
  - In reinforced concrete channels capable of carrying surge current with grounding at both ends
  - On closed metal cable racks that are grounded at the beginning and end
- Use of fiber-optic cables without a metal shield if such a transmission is intended
- Creation of local equipotential bonding at the transition of lightning protection zones, with incorporation of metallic supply systems (for example, pipes, air ducts, cable channels or cable ducts)

Additional measures

If the actions listed above cannot be implemented, protection by means of overvoltage arresters must be provided. The following sections contain tables with overvoltage arresters that are very suitable for protecting the plant.

Components for lightning protection equipotential bonding from lightning protection zone 0_B to 1 and 1 to 2

The following table shows components for lightning protection equipotential bonding from lightning protection zone 0_B to 1 and 1 to 2.

Table 3-110 Components for transition from lightning protection zone 0_B to 1 and 1 to 2

Seq. no.	Cables for ...	Connection at the 0_B interface to 1 with:	
		S7-1500/ET 200MP/ET 200SP/ET 200AL	**Article number**
1	Three-phase TN-C system	DEHNguard® DG M TNC 275	952 300
		DEHNguard® DG M TNC 275 FM *	952 305 *
2	Three-phase TN-S system	DEHNguard® DG M TNS 275	952 400
		DEHNguard® DG M TNS 275 FM *	952 405 *
3	Three-phase TT system	DEHNguard® DG M TT 275	952 310
		DEHNguard® DG M TT 275 FM *	952 315 *
4	AC TN-S system	DEHNguard® DG M TN 275	952 200
		DEHNguard® DG M TN 275 FM *	952 205 *
5	AC TT system	DEHNguard® DG M TT 2P 275	952 110
		DEHNguard® DG M TT 2P 275 FM *	952 115 *
6	Supply U_N = 24 V DC	BLITZDUCTOR® VT, BVT AVD 24	918422
7	Bus cable MPI/DP RS 485	BLITZDUCTOR® XT, base section BXT BAS	920 300
		BLITZDUCTOR® XT, module BXT ML2 BD HFS 5	920 271
8	Bus cable RS 232 (V.24)	BLITZDUCTOR® XT, base section BXT BAS	920 300
		BLITZDUCTOR® XT, module BXT ML2 BE S 12	920 222
9	Industrial Ethernet	DEHNpatch® DPA M CLE RJ45B 48	929 121
10	Inputs of digital modules U_N = 24 V DC	DEHNconnect® RK, DCO RK E 60 (I_L = 0.5 A)	919 990
11	Outputs of digital modules U_N = 24 V DC	DEHNconnect® RK, DCO RK D 5 24 (I_L = 10.0 A)	919 986
12	Inputs/outputs of digital modules U_N = 230 V AC	DEHNguard® DG S 275	952 070
		DEHNguard® DG S 275 FM *	952 090 *
		N-PE arrester in the TT system	
		DEHNgap® C S, DGP C S	952 030
		DEHNgap® C S, DGP C S FM *	952 035 *
13	Inputs/outputs of analog modules (e.g., 4-20 mA, 1-10 V)	DEHNconnect® RK, DCO RK E 60 (I_L = 0.5 A)	919 990
14	Inputs/outputs of the fail-safe modules (24 V DC)	DEHNconnect® RK, DCO RK D 5 24	919 986

* Version with remote indication contact
Components of the series BLITZDUCTOR® XT can be remotely monitored with the appropriate accessories. Additional information is available on the Internet (http://www.dehn.de)
Components can be ordered directly from:
DEHN+SÖHNE GMBH+CO.KG.

Seq. no.	Cables for ...	Connection at the 0_B interface to 1 with:	
		S7-1500/ET 200MP/ET 200SP/ET 200AL	Article number
Hans-Dehn-Straße 1 D-92318 Neumarkt			

Components for lightning protection equipotential bonding from lightning protection zone 2 to 3

The following table shows components for lightning protection equipotential bonding from lightning protection zone 2 to 3 that you can use for S7-1500/ET 200MP and ET 200SP.

Table 3-111 Components for transition from lightning protection zone 2 to 3 (for S7-1500/ET 200MP and ET 200SP)

Seq. no.	Cables for ...	Connection at the interface 2 to 3 with:			
		S7-1500/ET 200MP	Article number	ET 200SP	Article number
1	Three-phase TN-S, TT system	DEHNrail® DR M 4P 255	953 400	DEHNguard® DG M TNS 275	952 400
				DEHNguard® DG MOD 275	952 010
		DEHNrail® DR M 4P 255 FM * (I_L = 25.0 A)	953 405 *	DEHNguard® DG M TT 275	952 310
				DEHNguard® DG MOD 275	952 010
				DEHNguard® DG MOD NPE	952 050
2	AC TN-S, TT system	DEHNrail® DR M 2P 255	953 200	DEHNguard® DG M TN 275	952 200
				DEHNguard® DG MOD 275	952 010
		DEHNrail® DR M 2P 255 FM * (I_L = 25.0 A)	953 205 *	DEHNguard® DG M TT 2P 275	952 110
				DEHNguard® DG MOD 275	952 010
				DEHNguard® DG MOD NPE	952 050
3	Supply U_N = 24 V DC	BLITZDUCTOR® VT, BVT AVD 24	918 422	BLITZDUCTOR® VT, BVT AVD 24 ® VT	918 422
4	Bus cable MPI/DP RS 485	BLITZDUCTOR® XT, base section BXT BAS	920 300	---	---
		BLITZDUCTOR® XT, module BXT ML2 BD HFS 5	920 271	---	---
5	Bus cable RS 232 (V.24)	BLITZDUCTOR® XT, base section BXT BAS	920 300	---	---
		BLITZDUCTOR® XT, module BXT ML2 BE S 12	920 222	---	---
6	Industrial Ethernet	DEHNpatch® DPA M CLE RJ45B 48	929 121	---	---

Seq. no.	Cables for ...	Connection at the interface 2 to 3 with:			
		S7-1500/ET 200MP	**Article number**	**ET 200SP**	**Article number**
7	Inputs of digital modules U_N = 24 V DC	DEHNconnect® RK, DCO RK E60 (I_L = 0.5 A)	919 990	BLITZDUCTOR® XT, BXT ML4 BD 24 (I_L < 1 A)	920 344
				BLITZDUCTOR® XT, base section BXT BAS (I_L < 1 A)	920 300
8	Outputs of digital modules U_N = 24 V DC	DEHNconnect® RK, DCO RK D 5 24 (I_L = 10.0 A)	919 986	BLITZDUCTOR® XT, BXT ML4 BD 24 (I_L < 1 A)	920 344
				BLITZDUCTOR® XT, base section BXT BAS (I_L < 1 A)	920 300
				DEHNconnect® SD2, DCO SD2 E 48 (I_L < 10 A)	917 989
9	Inputs/outputs of digital modules U_N = 230 V AC	DEHNguard® DG S 275	952 070	DEHNguard® DG S 275	952 070
				DEHNguard® DG MOD 275	952 010
		DEHNguard® DG S 275 FM *	952 090 *	---	---
		N-PE arrester in the TT system			
		DEHNgap® C S, DGP C S	952 030	---	---
		DEHNgap® C S, DGP C S FM *	952 035 *	---	---
10	Inputs/outputs of analog modules (e.g., 4-20 mA, 1-10 V)	DEHNconnect® RK, DCO RK E 60 (I_L = 0.5 A)	919 990	BLITZDUCTOR® XT, BXT ML4 BD 24 (I_L < 1 A)	920 344
				BLITZDUCTOR® XT, base section BXT BAS (I_L < 1 A)	920 300
11	Inputs/outputs of the fail-safe modules (24 V DC)	---	---	DEHNconnect® RK, DCO RK D 5 24	919 986
				DEHNconnect® RK, DCO RK E 60	919 990

* Version with remote indication contact
Components of the series BLITZDUCTOR® XT can be remotely monitored with the appropriate accessories. Additional information is available on the Internet (http://www.dehn.de)
Components can be ordered directly from:
DEHN+SÖHNE GMBH+CO.KG.
Hans-Dehn-Straße 1
D-92318 Neumarkt

The following table shows components for lightning protection equipotential bonding from lightning protection zone 2 to 3 that you can use for ET 200AL.

Table 3-112 Components for transition from lightning protection zone 2 to 3 (for ET 200AL)

Seq. no.	Cables for ...	Connection at the interface 2 to 3 with:	
		ET 200AL	**Article number**
1	Supply U_N = 24 V DC	BLITZDUCTOR® VT, BVT AVD 24 ® VT	918 422
Components of the series BLITZDUCTOR® XT can be remotely monitored with the appropriate accessories. Additional information is available on the Internet (http://www.dehn.de) **Components can be ordered directly from:** DEHN+SÖHNE GMBH+CO.KG. Hans-Dehn-Straße 1 D-92318 Neumarkt			