SIEMENS

CPU 410SIS

System Manual

08/2017
A5E39417937-AA

Preface 1

Introduction to the CPU 410SIS 2

Design of CPU 410SIS 3

PROFIBUS DP 4

I/O configuration variants 5

System and operating states of the CPU 410SIS 6

Link-up and update 7

Special functions of the CPU 410SIS 8

Time synchronization and time stamping 9

Plant changes in RUN - CiR 10

Plant changes during redundant operation - H-CiR 11

Replacement of failed components during redundant operation 12

Synchronization modules 13

System expansion card 14

Technical data 15

Supplementary information 16

Characteristic values of redundant automation systems A

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. 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/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. 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 AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E39417937-AA
℗ 08/2017 Subject to change

Copyright © Siemens AG 2017.
All rights reserved

Table of contents

1 Preface 9

1.1 Preface 9

1.2 Security information 11

2 Introduction to the CPU 410SIS 13

2.1 Application area of the CPU 410SIS 13

2.2 Possible applications 15

2.3 The CPU 410SIS basic system for stand-alone operation 16

2.4 The basic system for redundant operation 17

2.5 Rules for assembly of an AS 410H SIS 19

2.6 I/O for the CPU 410SIS 20

2.7 Configuration variants of the I/O on a CPU 410SIS 20

2.8 Tools for configuration (HW Config, SIMATIC SIS compact) 21

2.9 The SIMATIC SIS compact project 21

2.9.1 Licensing 21

3 Design of CPU 410SIS 23

3.1 Operator controls and display elements of the CPU 410SIS 23

3.2 Monitoring functions of the CPU 410SIS 27

3.3 Status and error displays 29

3.4 PROFIBUS DP interface (X1) 33

3.5 PROFINET interfaces (X5, X8) 33

3.6 Overview of parameters for CPU 410SIS 35

4 PROFIBUS DP 37

4.1 CPU 410SIS as PROFIBUS DP master 37

4.2 Diagnostics of the CPU 410SIS as PROFIBUS DP master 37

5 I/O configuration variants 39

5.1 Stand-alone operation 39

5.2 Fail-safe operation 41

5.3 Fault-tolerant automation systems (redundancy operation) 45

5.3.1 Redundant SIMATIC automation systems 45

5.3.2 Increase of plant availability, reaction to errors 47

5.4 Using single-channel switched I/O 49

5.5 Connection of two-channel I/O to the PROFIBUS DP interface 53

5.5.1 Connecting redundant I/O....53
5.5.2 Signal modules for redundancy....56
5.5.3 Evaluating the passivation status....69

6 System and operating states of the CPU 410SIS....71

6.1 Operating states of the CPU 410SIS....71
6.1.1 RUN mode....71
6.1.2 STOP mode....72
6.1.3 STARTUP mode....72
6.1.4 HOLD mode....73
6.1.5 LINK-UP and UPDATE modes....74
6.1.6 ERROR-SEARCH mode....74
6.1.7 DEFECTIVE state....75

6.2 System states of the redundant CPU 410SIS....76
6.2.1 Introduction....76
6.2.2 The system states of the AS 410H SIS....79
6.2.3 Displaying and changing the system state of a fault-tolerant system....79
6.2.4 System status change from the STOP system state....80
6.2.5 System status change from the standalone mode system status....80
6.2.6 System status change from the redundant system state....81
6.2.7 System diagnostics of a fault-tolerant system....82

6.3 Self-test....84

6.4 Performing a memory reset....87

7 Link-up and update....89

7.1 Effects of link-up and updating....89

7.2 Link-up and update via an ES command....90

7.3 Time monitoring....90
7.3.1 Time response....93
7.3.2 Determining the monitoring times....94
7.3.3 Performance values for link-up and update....100
7.3.4 Influences on time response....100

7.4 Special features in link-up and update operations....101

8 Special functions of the CPU 410SIS....103

8.1 Security functions of the CPU 410SIS....103

8.2 Security levels....104

8.3 Security event logging....106

8.4 Field Interface Security....108

8.5 Access-protected blocks....109

8.6 Retentive load memory....110

8.7 Type update with interface change in RUN....111

8.8 Resetting the CPU 410SIS to delivery condition (reset to factory setting)....112

8.9 Reset during operation....113

8.10 Response to fault detection....113

8.11 Reading service data....115
8.12 Updating firmware in stand-alone operation....116
8.13 Updating firmware in redundant mode....118
9 Time synchronization and time stamping....121
10 Plant changes in RUN - CiR....123
10.1 Motivation for CiR via PROFINET DP....123
10.2 Permitted changes over PROFIBUS DP....124
10.3 CiR objects and CiR modules for PROFINET DP....125
10.3.1 Basic Requirements....125
10.3.2 Types of CiR Elements....126
10.3.3 CiR Elements and I/O Address Areas....127
10.4 Procedure for PROFIBUS DP....128
10.4.1 Basic Procedures in STOP Mode....128
10.4.1.1 Overview....128
10.4.1.2 Defining CiR Elements....129
10.4.1.3 Deleting CiR Elements....132
10.4.2 Basic Procedure in RUN Mode....132
10.4.2.1 Overview....132
10.4.2.2 add slaves or modules....133
10.4.2.3 Reconfigure the hardware when adding a slave....134
10.4.2.4 change process image partition assignment....134
10.4.2.5 reconfigure existing modules in ET200M / ET200iSP stations....134
10.4.2.6 Undo previous changes (Undo function):....135
10.4.2.7 Replacing Slaves or Modules....135
10.4.2.8 Using CiR Elements in RUN Mode....136
10.4.2.9 Undoing Previous Changes....137
10.5 Reconfigure existing modules in ET200M / ET200iSP stations....138
10.5.1 Requirements for Reconfiguration....138
10.5.2 Module Response During a Reconfiguration....139
10.5.3 CPU response during reconfiguration....139
10.5.4 Reconfiguration Procedure....141
10.5.4.1 Using a Previously Unused Channel....141
10.5.4.2 Reconfiguring an already used channel....141
10.5.4.3 Delete an already used channel....142
10.6 Notes on Reconfiguration in RUN Mode Depending on the I/O....143
10.6.1 DP slaves....143
10.6.2 Modules in ET 200M Modular Slaves....144
10.6.3 Modules in ET200iSP Modular Slaves....144
10.7 Effects on the process when re-configuring in RUN....145
10.7.1 Effects on Operating System Functions During the CiR Synchronization Time....145
10.7.2 Behavior of the CPU after download of the configuration in RUN....145
10.7.2.1 Overview....145
10.7.2.2 Error displays....146
11 Plant changes during redundant operation - H-CiR....147
11.1 The H-CiR wizard....147

11.2 Replacing central components....148
11.3 Motivation for H-CiR via PROFIBUS DP....148
11.4 Permitted changes over PROFIBUS DP....150
11.5 Adding components....151
11.5.1 Modify hardware....152
11.5.2 Change hardware configuration offline....152
11.5.3 Opening the H-CiR wizard....153
11.5.4 Modify and download the user program....154
11.5.5 Use of free channels on an existing module....154
11.6 Removal of components....155
11.6.1 Change hardware configuration offline....156
11.6.2 Modify and download the user program....157
11.6.3 Opening the H-CiR wizard....157
11.6.4 Modify hardware....158
11.7 Editing CPU parameters....159
11.7.1 Editing CPU parameters....159
11.7.2 Changing CPU parameters offline....160
11.7.3 Opening the H-CiR wizard....161
11.8 Re-parameterization of a module....162
11.8.1 Re-parameterization of a module....162
11.8.2 Editing parameters offline....162
11.8.3 Opening the H-CiR wizard....163
12 Replacement of failed components during redundant operation....165
12.1 Replacement of central components....165
12.1.1 Replacement of a CPU during redundant operation....165
12.1.2 Replacement of a power supply module....167
12.1.3 Replacement of synchronization module or fiber-optic cable....168
12.2 Replacement of components of the distributed I/O on PROFIBUS DP....170
12.2.1 Replacement of a redundant PROFIBUS DP interface module....171
12.2.2 Replacement of a PROFIBUS DP slave....171
12.2.3 Replacement of PROFIBUS DP cables....172
13 Synchronization modules....175
13.1 Synchronization modules for the CPU 410SIS....175
13.2 Installation of fiber-optic cables....178
13.3 Selecting fiber-optic cables....181
14 System expansion card....187
15 Technical data....189
15.1 Technical specifications of CPU 410SIS (6ES7410-5FM08-0AB0)....189
15.2 Technical specifications of the system expansion card....197
16 Supplementary information....199
16.1 Configuring....199
16.1.1 Rules for assembling an AS 410H SIS....199

16.1.2 Configuring hardware....199
16.1.3 Assigning parameters to modules in an H system....200
16.1.4 Recommendations for setting CPU parameters, fixed settings....200
16.1.5 Networking configuration....201
16.2 PG functions....202
16.3 Communication services....202
16.3.1 Overview of communication services....202
16.3.2 PG communication....204
16.3.3 OP communication....204
16.3.4 S7 routing....204
16.3.5 Data set routing....208
16.3.6 SNMP network protocol....210
16.4 Basics and terminology of fault-tolerant communication....211
16.5 Usable networks....214
16.6 Communication via S7 connections....214
16.6.1 Custom connection to single-channel systems....215
16.7 Communication via fault-tolerant S7 connections....216
16.7.1 Communication between fault-tolerant systems....218
16.7.2 Communication between fault-tolerant systems and a fault-tolerant CPU....220
16.7.3 Communication between fault-tolerant systems and PCs....221
16.8 Link-up and update sequence....223
16.8.1 Link-up sequence....226
16.8.2 Update sequence....227
16.8.3 Switch to CPU with modified configuration....230
16.8.4 Disabling of link-up and update....231
16.9 The user program....232
16.10 Cycle and response times of the CPU 410SIS....232
16.10.1 Cycle time....232
16.10.2 Calculating the cycle time....234
16.10.3 Cycle load due to communication....237
16.10.4 Response time....239
16.10.5 Calculating cycle and response times....244
16.10.6 Interrupt response time....245
16.10.7 Reproducibility of delay and watchdog interrupts....247
16.11 Runtimes of the FCs and FBs for redundant I/Os....247
A Characteristic values of redundant automation systems....249
A.1 Basic concepts....249
A.2 Comparison of MTBF for selected configurations....253
A.2.1 System configurations with redundant CPU 410....253
A.2.2 System configurations with distributed I/Os....254
A.2.3 Comparison of system configurations with standard and fault-tolerant communication. 257
Index....259

Preface

1

1.1 Preface

Purpose of this manual

The information in this manual enables you to look up operator inputs, function descriptions and technical specifications of the central processing unit CPU 410SIS.

For information on installing and wiring this and other modules in order to set up an automation system, refer to Manual *Automation System S7-400, Hardware and Installation*.

Scope of the manual

The manual is valid for the following component:

CPU 410SIS; 6ES7410-5FM08-0AB0 Firmware Version V8.2 or higher

Basic knowledge required

This manual requires general knowledge of automation engineering.

Knowledge of the use of computers or PC-like tools such as programming devices with a Windows operating system is also required. The SIS compact readme includes information about suitable operating systems for your SIS compact configuration. Because the CPU 410SIS is configured with the SIS compact software, you must also know how to use this software.

In particular when operating a CPU 410SIS system in potentially explosive atmospheres, you should always observe the information on the electrical safety of electronic control systems provided in the appendix of Manual *Automation System S7-400, Hardware and Installation*.

Approvals

For details on certifications and standards, refer to Manual *S7-400 Automation System, Module Data*, Chapter 1.1, Standards and Certifications. Here you will also find the technical specification for the entire S7-400.

Online help

You will need the SIS compact Programming Package V9.0 or higher to work with CPU 410SIS.

In addition to the manual, you will find detailed support on how to use this software in the software's integrated online help system.

The help system can be accessed using various interfaces:

- The **Help** menu contains several commands: **Contents** opens the Help index. You will find help on fault-tolerant systems in **Configuring fault-tolerant systems**.
- **Using Help** provides detailed instructions on using the online help system.
- The context-sensitive help system provides information on the current context, for example, on an open dialog or active window. You can call this help by clicking "Help" or using the F1 key.
- The status bar provides a further form of context-sensitive help. It shows a short description of each menu command when you position the mouse pointer over a command.
- A short info text is also shown for the toolbar buttons when you hold the mouse pointer briefly over a button.

If you prefer to read the information of the online help in printed form, you can print individual topics, books or the entire help system.

Recycling and disposal

Because it is constructed from environmentally compatible materials, the CPU 410SIS can be recycled. For ecologically compatible recycling and disposal of your old device, contact a certificated disposal service for electronic scrap.

Additional support

If you have any questions relating to the products described in this manual, and do not find the answers in this documentation, please contact your Siemens partner at our local offices.

You will find information on who to contact at:

Contact partners (http://www.siemens.com/automation/partner)

A guide to the technical documents for the various SIMATIC products and systems is available at:

Documentation (http://www.automation.siemens.com/simatic/portal/html_76/techdoku.htm)

You can find the online catalog and order system under:

Catalog (http://mall.industry.siemens.com/)

Functional Safety Services

Siemens Functional Safety Services is a comprehensive performance package that supports you in risk assessment and verification all the way to plant commissioning and modernization. We also offer consulting services for the application of fail-safe and fault-tolerant SIMATIC S7 automation systems.

Additional information is available at:

Functional Safety Services (http://www.industry.siemens.com/topics/global/en/safety-integrated/process-safety/Pages/process-safety.aspx)

Submit your requests to:

Mail Functional Safety Services (mailto:safety-services.industry@siemens.com)

Training center

We offer a range of relevant courses to help you to get started with the SIS compact product. Please contact your local training center or the central training center.

Training (http://www.sitrain.com/index_en.html)

Technical Support

For technical support of all Industry Automation products, fill in and submit the online Support Request:

Support Request (http://www.siemens.de/automation/support-request)

Service & Support on the Internet

In addition to our documentation, we offer a comprehensive online knowledge base on the Internet at:

Service & Support (http://www.siemens.com/automation/service&support)

There you will find:

- The newsletter containing the latest information on your products.
- The latest documents via our search function in Service & Support.
- A forum for global information exchange by users and specialists.
- Your local Automation representative.
- Information on field service, repairs and spare parts. Much more can be found under "Services".

1.2 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.

Introduction to the CPU 410SIS

2

2.1 Application area of the CPU 410SIS

SIMATIC SIS compact and CPU 410SIS

With SIMATIC SIS compact (SIS = Safety Instrumented System), you can configure and program fail-safe automation systems based on the SIMATIC Safety Integrated product portfolio.

Fail-safe automation systems ("F systems") are used in plants with increased safety requirements. The purpose of SIMATIC SIS compact is to control processes with an immediately achievable safe state. These are processes for which immediate disconnection does not entail any danger to people or the environment.

This functional safety is realized by safety functions in the software.

You can use SIMATIC SIS compact to create customized and project-specific solutions tailored to specific safety requirements.

CPU 410SIS is specifically designed as a CPU for SIMATIC SIS compact.

The SIMATIC SIS compact project

A SIMATIC SIS compact project includes the following objects:

- Hardware configuration
- Blocks
- CFCs

These objects are always present - regardless of the number of operator stations and modules and their networking.

SIMATIC SIS compact applications

You create a SIMATIC SIS compact project on an engineering station (ES for short). A variety of applications are available on the ES:

- SIMATIC Manager - the central application of SIMATIC SIS compact. From here you can open all other applications in which you have to make settings for the SIMATIC SIS compact project. You will set up your entire project from SIMATIC Manager.
- HW Config – configuration of all hardware of a system
- S7 F Systems – configuration and programming fail-safe automation systems
- CFC Editor – creation of CFCs
- Safety Matrix Engineering – creation of safety programs for fail-safe automation systems according to the rules of a cause/effect matrix
- SIMATIC SIS compact OS with various editors – performance of OS configuration

Every application has a graphic user interface for easy operation and clear representation of your configuration data.

Important information on configuration

⚠ WARNING

Open equipment

Risk of death or serious injury.

S7-400 modules are classified as open equipment. This means you may only install a controller consisting of S7-400 modules in enclosures, cabinet, or switch rooms that require a key or tool for access Only instructed or authorized personnel are permitted to access these enclosures, cabinets, or switch rooms.

See also

Overview of parameters for CPU 410SIS (Page 35)

SIMATIC Industrial Software S7 F/FH Systems (https://support.industry.siemens.com/cs/ww/en/view/2201072)

2.2 Possible applications

Configuration of an AS 410H SIS

The following figure shows an example of an AS 410H SIS configuration with shared distributed I/O and connection to a redundant plant bus. The following pages describe the hardware and software components required to set up and operate the AS 410H SIS.

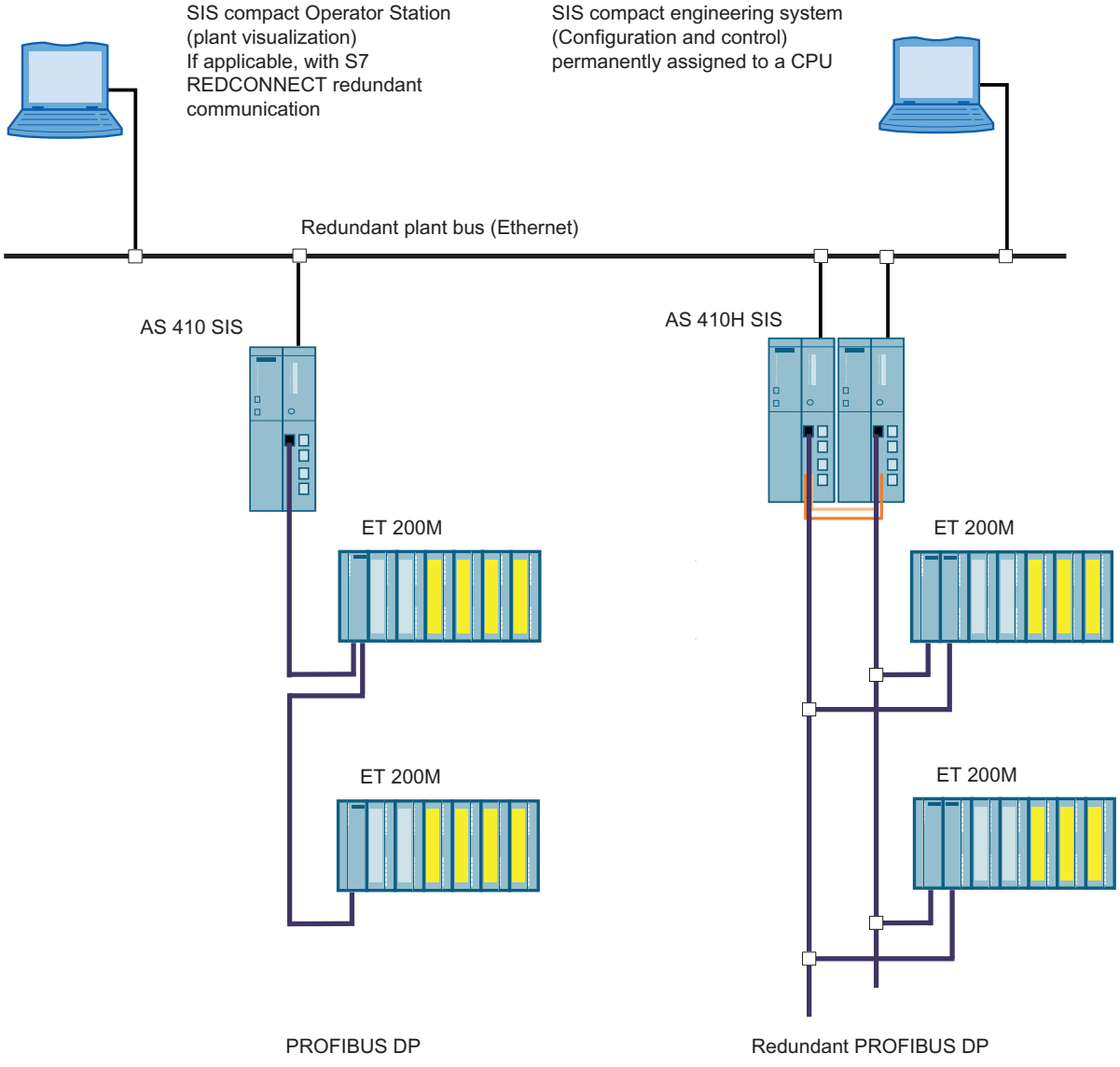


Figure 2-1 Overview

2.3 The CPU 410SIS basic system for stand-alone operation

Definition

Stand-alone operation refers to the use of a CPU 410SIS in an AS 410 SIS.

Note

Rack number "0" must be set on the CPU.

Hardware of the basic system

The basic system consists of the required hardware components of a controller. The following figure shows the components in the configuration.

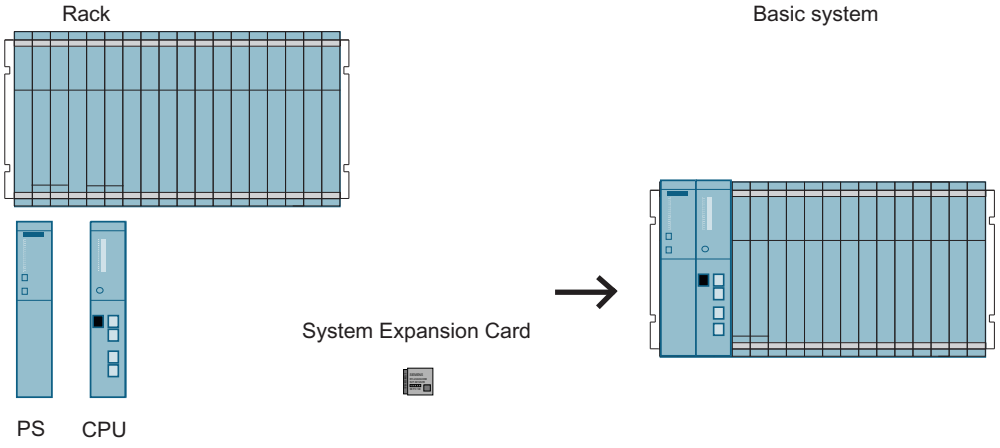


Figure 2-2 The hardware of the AS 410 SIS basic system

Central controller

The rack containing the CPU is called the central controller (CC).

Power supply

For the power supply you need a power supply module from the standard S7-400 system range (PS 407).

Operation

You need the system expansion card SEC E4MB for operation of a CPU 410SIS. The system expansion card forms a hardware unit with the CPU 410SIS.

2.4 The basic system for redundant operation

Hardware of the basic system

The basic system consists of the hardware components required for a fault-tolerant controller. The following figure shows the components in the configuration.

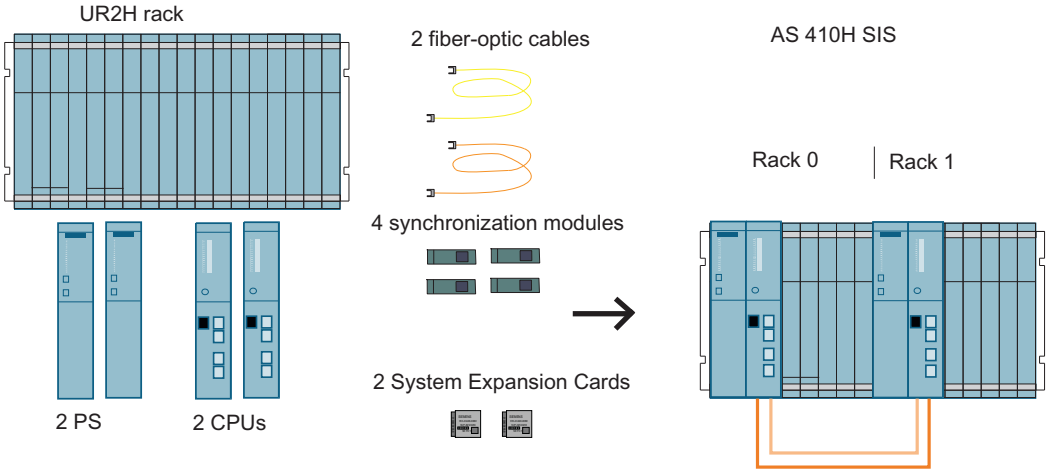


Figure 2-3 The hardware of the AS 410H SIS

Central processing units

The core of the AS 410H SIS is formed by two 410SIS CPUs. Use the switch **on the rear** of the CPU to set the rack numbers. In the following sections, we will refer to the CPU in rack 0 as CPU 0, and to the CPU in rack 1 as CPU 1.

Rack for the AS 410H SIS

The UR2-H rack supports the installation of two separate subsystems with nine slots each, and is suitable for installation in 19" cabinets.

Alternatively, you can install the AS 410H SIS on two separate racks. The racks UR1, UR2, and CR3 are available for this purpose.

Power supply

For each of the two subsystems of the AS 410H SIS, you need a power supply module from the standard system range of the S7-400 (PS 407).

Synchronization modules

The synchronization modules are used to connect the two CPUs. They are installed in the CPUs and interconnected via fiber-optic cables.

The following synchronization modules are available:

- Synchronization modules for synchronization cables up to 10 meters long
- Synchronization modules for synchronization cables up to 10 kilometers long

You must use 4 synchronization modules of the same type in an AS 410H SIS. For a description of the synchronization modules, refer to the section Synchronization modules for the CPU 410SIS. (Page 175).

Fiber-optic cable

The fiber-optic cables connect the synchronization modules for redundancy coupling between the two CPUs. They interconnect the upper and lower synchronization modules in pairs.

You can find the specification of the fiber-optic cables you can use in an AS 410H SIS in the section Selecting fiber-optic cables (Page 181).

Operation

You need the system expansion card SEC E4MB for operation of a CPU 410SIS. The system expansion card forms a hardware unit with the CPU 410SIS.

2.5 Rules for assembly of an AS 410H SIS

In addition to the general rules applicable to the assembly of modules, the following requirements must be met for an AS 410H SIS:

- The CPUs must be plugged into the same slots.
- Redundantly used CPUs must be identical, which means they must have the same article number, product version and firmware version. It is not the marking on the front side that is decisive for the product version, but the revision of the "Hardware" component ("Module status" dialog mask) to be read using STEP 7.
- Redundantly used other modules must be identical, i.e. they must have the same article number, product version and - if available - firmware version.

2.6 I/O for the CPU 410SIS

You can use the following SIMATIC S7 I/O with the CPU 410SIS:

- ET 200M fail-safe I/O modules
  You can use up to 2 standard I/O modules per station.
- ET 200iSP fail-safe I/O modules
  You can use up to 2 standard I/O modules per station.
- SIMOCODE pro V with fail-safe expansion modules
- SINAMICS G120 Control Units with fail-safe inputs/outputs

2.7 Configuration variants of the I/O on a CPU 410SIS

I/O configuration variants

The following configuration variants are available for the input/output modules:

- In stand-alone operation: one-sided configuration.
  In the one-sided configuration, there is a single set of the input/output modules (single-channel) that are addressed by the CPU.
- In redundant operation: Single-channel switched configuration with enhanced availability.
  In the single-channel switched distributed configuration, there is a single set of the I/O modules, but they can be addressed by both subsystems.
- In redundant operation: Dual-channel configuration with maximum availability.
  In dual-channel switched configuration, there are two of each of the input/output modules and the modules can be addressed by both subsystems.

2.8 Tools for configuration (HW Config, SIMATIC SIS compact)

You configure the CPU 410SIS with HW Config.

You can find information on limitations for configuring CPUs and the H system in the online help of HW Config.

2.9 The SIMATIC SIS compact project

STEP 7

The core component for configuring the SIMATIC SIS compact with the engineering system is STEP 7.

STEP 7 supports the various tasks involved in creating a project with the following project views:

- Component view (HW Config)
- Process object view
- Technological perspective

The hardware that you need in a SIMATIC project, such as automation systems, communication components, and process I/O, is stored in an electronic catalog. You configure this hardware and assign the hardware parameters with HW Config.

2.9.1 Licensing

Use of the system expansion card

The license information for a CPU 410SIS is stored on a System Expansion Card (SEC). You insert the SEC in a slot on the back of the CPU before commissioning the CPU. The SEC is an essential part of the CPU hardware. The CPU cannot be operated without an SEC. If no valid SEC is detected, the corresponding CPU does not start up. A sync loss is triggered in an AS 410H SIS, whereby startup prevention prevents renewed automatic connection.

Design of CPU 410SIS

3

3.1 Operator controls and display elements of the CPU 410SIS

Arrangement of the operator controls and display elements of the CPU 410SIS

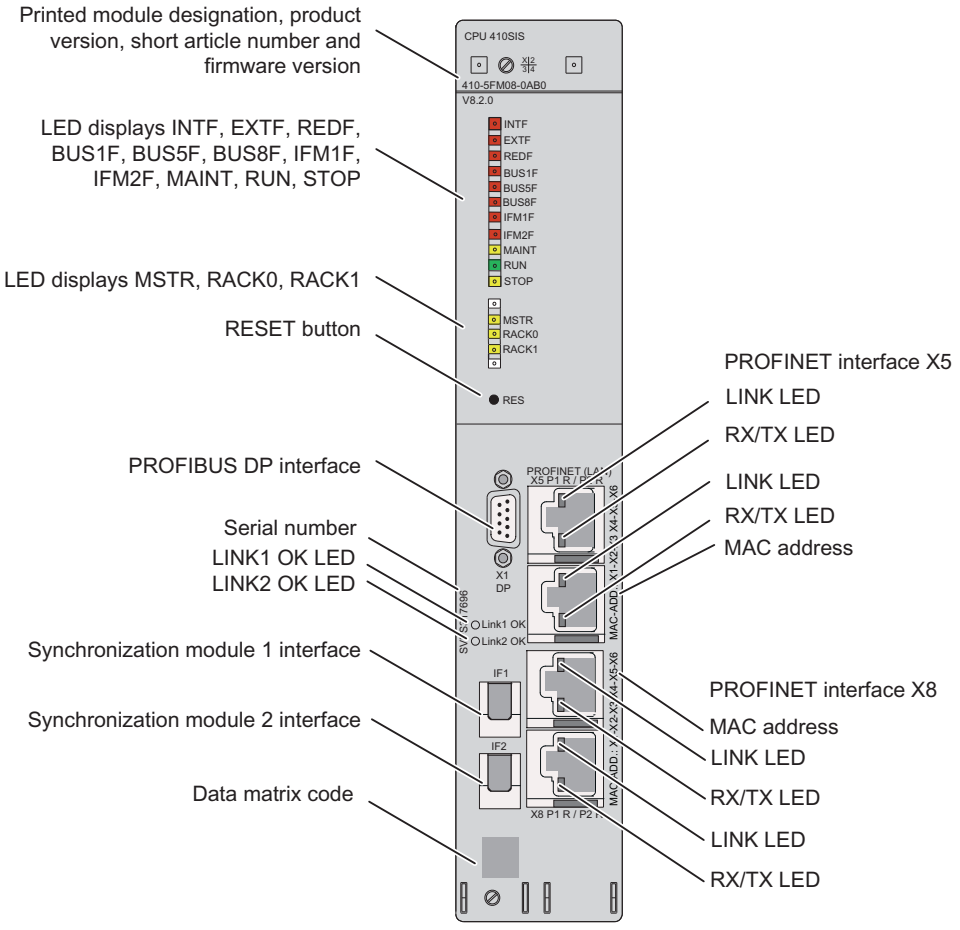


Figure 3-1 Arrangement of the operator controls and display elements of the CPU 410SIS

LED displays

The following table gives an overview of the available LED displays.

Sections Monitoring functions of the CPU 410SIS (Page 27) and Status and error displays (Page 29) describe the states and errors/faults indicated by these LEDs.

Table 3-1 LED displays on the CPUs

LED display	Color	Meaning
Top bar		
INTF	red	Internal fault
EXTF	red	External fault
REDF	red	Loss of redundancy/Redundancy fault
BUS1F	red	Bus fault at the PROFIBUS interface
BUS5F	red	Bus fault at the first PROFINET interface
BUS8F	red	Bus fault at the second PROFINET interface
IFM1F	red	Error in synchronization module 1
IFM2F	red	Error in synchronization module 2
MAINT	yellow	Maintenance request pending
RUN	green	RUN mode
STOP	yellow	STOP mode
Bottom bar		
MSTR	yellow	CPU controls the process
RACK0	yellow	CPU in rack 0
RACK1	yellow	CPU in rack 1
For the interfaces		
LINK	green	Connection at the PROFINET IO interface is active
RX/TX	orange	Receiving or sending data at the PROFINET interface.
LINK 1 OK	green	Connection via synchronization module 1 is active and OK
LINK 2 OK	green	Connection via synchronization module 2 is active and OK

Reset button

You operate the reset button in the following cases:

- You want to reset the CPU to the factory state, see section Resetting the CPU 410SIS to delivery condition (reset to factory setting) (Page 112)
- You want to reset the CPU during operation, see section Reset during operation (Page 113)

The reset button is on the front of the CPU directly below the LED strip. Press it with a suitably thin round object.

Slot for synchronization modules

The synchronization modules for redundant operation are inserted in these slots. See section Synchronization modules (Page 175).

PROFIBUS DP interface

You can connect the distributed I/O to the PROFIBUS DP interface.

PROFINET interface

The PROFINET interfaces establish the connection to the Industrial Ethernet. The PROFINET interfaces also serve as the access point for the engineering system. The PROFINET interfaces each have 2 switched ports with external connectors (RJ 45).

The meaning of the interface labels is as follows:

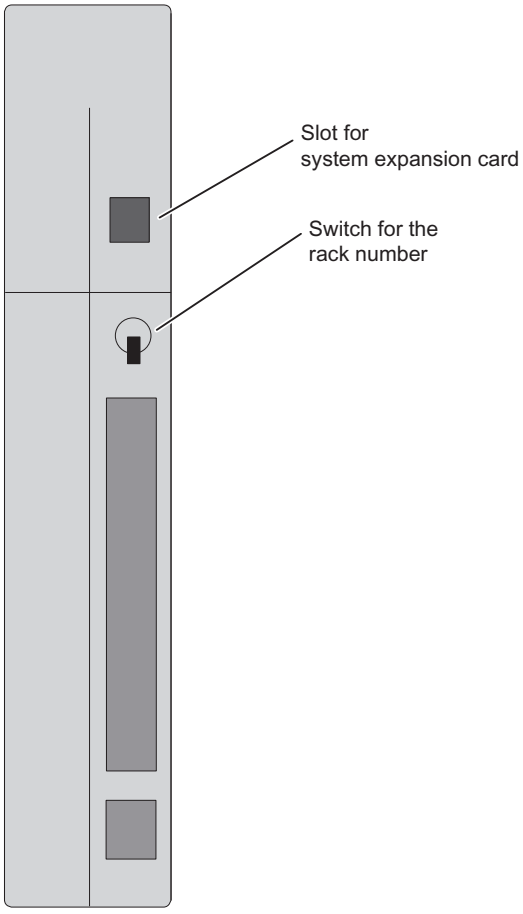
Label	Meaning
X5 P1 R	Interface X5, Port 1
X5 P2 R	Interface X5, Port 2
X8 P1 R	Interface X8, Port 1
X8 P2 R	Interface X8, Port 2

NOTICE

Connecting only to Ethernet LAN

These interfaces only allow connection to an Ethernet LAN. You cannot connect them to the public telecommunication network, for example.

Rear of the CPU 410SIS



Setting the rack number

Use the switch on the rear panel of the CPU to set the rack number. The switch has two positions: 1 (up) and 0 (down). One CPU is allocated rack number 0, and the partner CPU is assigned rack number 1. The default setting of all CPUs is rack number 0.

Slot for system expansion card

The back of the CPU has a slot in which you insert the system expansion card (SEC) before commissioning the CPU. The SEC is an essential part of the CPU hardware. The CPU cannot be operated without an SEC. If an SEC is not detected, the corresponding CPU goes to STOP and requests a memory reset. "STOP by CPU memory management" is also entered in the diagnostics buffer.
You need a small screwdriver to remove the SEC. Place the screwdriver at the top of the SEC slot and lift out the SEC with the screwdriver.

3.2 Monitoring functions of the CPU 410SIS

Monitoring functions and error messages

The hardware of the CPU and operating system provide monitoring functions to ensure proper operation and defined reactions to errors. Various errors may also trigger a reaction in the user program.

The table below provides an overview of possible errors and their causes, and the corresponding responses of the CPU.

Additional test and information functions are available in each CPU; they can be initiated in STEP 7.

Type of error	Cause of error	Error LED
Access error	Module failure	EXTF
Time error	• The user program execution time (OB 1 and all interrupts and error OBs) exceeds the specified maximum cycle time. • Overflow of the start information buffer • Time-of-day error interrupt	INTF
Power supply module(s) fault (not power failure)	In the central rack • at least one backup battery of the power supply module is completely discharged. • the backup battery voltage is missing. • the 24 V supply to the power supply module has failed.	EXTF
Diagnostic interrupt	An I/O module with interrupt capability reports a diagnostic interrupt The synchronization module signals a diagnostic interrupt; see Chapter Synchronization modules for the CPU 410SIS. (Page 175) The LED EXTF lights up with the first incoming diagnostic interrupt and goes out with the outgoing diagnostic interrupt.	EXTF
Swapping interrupt	Removing or inserting a module as well as inserting an incorrect module type. Removing a synchronization module.	EXTF
Redundancy error	• Loss of redundancy on the CPUs • Redundancy loss/ station failure of a switched DP station • Failure of a DP master	REDF
CPU hardware fault	• A memory error was detected and eliminated	INTF
Program execution error	• Process image update error	INTF EXTF
Failure of a rack/station	• Failure of a DP segment	EXTF BUSF for DP REDF for redundant segments
Communication error	Communication error: • Time synchronization • Access to DB when exchanging data via communications function blocks	INTF

Type of error	Cause of error	Error LED
Execution canceled	The execution of a program block was canceled. Possible reasons for the cancellation are: • Nesting depth of nesting levels too great • Nesting depth of master control relay too great • Nesting depth of synchronization errors too great • Nesting depth of block call commands (U stack) too great • Nesting depth of block call commands (B stack) too great • Error during allocation of local data Such errors cannot occur with blocks from a SIMATIC SIS compact library.	INTF
Missing license for Runtime software	The Runtime software could not be completely licensed (internal error).	INTF
Programming error	User program error: • BCD conversion error • Range length error • Range error • Alignment error • Write error • Timer number error • Counter number error • Block number error • Block not loaded Such errors cannot occur with blocks from a SIMATIC SIS compact library.	INTF
MC7 code error	Error in the compiled user program, for example, illegal OP code or a jump beyond the block end Such errors cannot occur with blocks from a SIMATIC SIS compact library.	INTF

3.3 Status and error displays

RUN and STOP LEDs

The RUN and STOP LEDs provide information about the CPU's currently active operating state.

Table 3-2 Possible states of the RUN and STOP LEDs

LED		Meaning
RUN	STOP	
Lit	Dark	CPU is in RUN state.
Dark	Lit	CPU is in STOP state. The user program is not being executed. Cold restart/restart is possible.
Flashes 2 Hz	Flashes 2 Hz	The CPU has detected a serious error that is blocking startup. All other LEDs also flash at 2 Hz.
Flashes 0.5 Hz	Lit	HOLD status has been triggered by a test function.
Flashes 2 Hz	Lit	A cold restart/restart was initiated. The cold restart/warm start may take a minute or longer, depending on the length of the called OB. If the CPU still does not change to RUN, there might be an error in the system configuration, for example.
Dark	Flashes 2 Hz	• A high-quality RAM test (self-test) is executed after POWER ON. The duration of the self-test is at least 7 minutes. • CPU memory reset is active.
Dark	Flashes 0.5 Hz	The CPU requests a memory reset.
Flashes 0.5 Hz	Flashes 0.5 Hz	• Troubleshooting mode • Startup (POWER ON) of a CPU on which a large number of blocks is loaded. If encrypted blocks are loaded, startup may take a longer time depending on the number of such blocks. This display also indicates that internal processes are busy on the CPU and prevent access to the CPU until completed.
Flashes 0.5 Hz	Flashes 2 Hz	The CPU has downloaded another program and is powering up after power on. Note that, if necessary, another program and a configuration may be present in the retentive load memory in the CPU. Ensure that this cannot pose a hazard if the CPU switches automatically to RUN state. If you have no information about the content of the load memory, set the CPU to delivery state before powering it up.

MSTR, RACK0, and RACK1 LEDs

The three LEDs MSTR, RACK0, and RACK1 provide information about the rack number set on the CPU and show which CPU controls the switched I/O.

Table 3-3 Possible states of the MSTR, RACK0 and RACK1 LEDs

LED			Meaning
MSTR	RACK0	RACK1	
Lit	Irrelevant	Irrelevant	CPU controls switched I/O
Irrelevant	Lit	Dark	CPU on rack number 0
Irrelevant	Dark	Lit	CPU on rack number 1

INTF and EXTF LEDs

The two INTF and EXTF LEDs provide information about errors and other particular things that happen during user program execution.

Table 3-4 Possible states of the INTF and EXTF LEDs

LED		Meaning
INTF	EXTF	
Lit	Irrelevant	An internal error was detected (programming, parameter assignment, or license error).
Irrelevant	Lit	An external error has been detected (i.e. an error not caused by the CPU)

BUS1F, BUS5F, and BUS8F LEDs

The BUS1F, BUS5F and BUS8F LEDs indicate errors associated with the PROFIBUS DP interface and the PROFINET interfaces.

Table 3-5 Possible states of the BUS1F, BUS5F, and BUS8F LEDs

LED			Meaning
BUS1F	BUS5F	BUS8F	
Lit	Irrelevant	Irrelevant	An error was detected on the PROFIBUS DP interface X1.
Irrelevant	Lit	Irrelevant	An error was detected on the first PROFINET interface X5.
Irrelevant	Irrelevant	Lit	An error was detected on the second PROFINET IO interface X8.
Flashes	Irrelevant	Irrelevant	One or more slaves on the PROFIBUS DP interface X1 is not responding.

IFM1F and IFM2F LEDs

The IFM1F and IFM2F LEDs indicate errors on the first or second synchronization module.

Table 3-6 Possible states of the IFM1F and IFM2F LEDs

LED		Meaning
IFM1F	IFM2F	
Lit	Irrelevant	An error was detected on synchronization module 1.
Irrelevant	Lit	An error was detected on synchronization module 2

LINK and RX/TX LEDs

The LINK and RX/TX LEDs indicate the current state of the Ethernet interfaces.

Table 3-7 Possible states of the LINK and RX/TX LEDs

LED		Meaning
LINK	RX/TX	
Lit	Irrelevant	Connection at the PROFINET IO interface is active
Irrelevant	Flashes 6 Hz	Receiving or sending data at the PROFINET interface.

Note

The LINK and RX/TX LEDs are located directly next to the sockets of the PROFINET interfaces. They are not labeled.

REDF LED

The REDF LED indicates specific system states and redundancy errors.

Table 3-8 Possible states of the REDF LED

REDF LED	System state	Basic requirements
Flashes 0.5 Hz	Link-up	-
Flashes 2 Hz	Update	-
Dark	Redundant (CPUs are redundant)	No redundancy error
Lit	Redundant (CPUs are redundant)	There is an I/O redundancy error: • Failure of a DP master, or partial or total failure of a DP master system • Loss of redundancy on the DP slave • Loss of redundancy on the DP slave/slave failure

LEDs LINK1 OK and LINK2 OK

When commissioning the fault-tolerant system, you can use the LINK1 OK and LINK2 OK LEDs to check the quality of the connection between the CPUs.

Table 3-9 Possible states of the LINK1 OK and LINK2 OK LEDs

LED LINKx OK	Meaning
Lit	The connection is OK
Flashes	The connection is not reliable, and the signal is disrupted Check the connectors and cables Ensure that the fiber-optic cables are installed in accordance with the guidelines in Chapter Installation of fiber-optic cables (Page 178). Check whether the synchronization module works in another CPU.
Dark	The connection is interrupted, or there is insufficient light intensity Check the connectors and cables Ensure that the fiber-optic cables are installed in accordance with the guidelines in Chapter Installation of fiber-optic cables (Page 178). Check whether the synchronization module works in another CPU. If necessary, replace the synchronization module in the other CPU.

LED MAINT

This LED indicates that maintenance is required. Maintenance is required due to problems with the synchronization modules For more information, refer to the STEP 7 Online Help.

The LED MAINT also displays an error during address assignment of the PROFINET interfaces X5 or X8.

Diagnostics buffer

In STEP 7, you can select "PLC -> Module Information" to read the cause of an error from the diagnostics buffer.

3.4 PROFIBUS DP interface (X1)

Connectable devices

The PROFIBUS DP interface can be used to set up a PROFIBUS master system, or to connect PROFIBUS I/O devices.

All DP slaves that conform to the standard can be connected to the PROFIBUS DP interface.

You can connect the PROFIBUS DP I/O to the PROFIBUS DP interface in redundant or single-channel switched configuration.

In this case, the CPU is the DP master, which is connected to the passive slave stations or, in stand-alone operation, to other DP masters.

Some of the devices that can be connected draw 24 V from the interface for their power supply. This voltage is provided as non-isolated voltage at the PROFIBUS DP interface.

Connectors

Use only PROFIBUS DP bus connectors or PROFIBUS cables for connecting devices to the PROFIBUS DP interface (*see installation manual*).

Redundant operation

The PROFIBUS DP interfaces have the same baud rate and the same operating mode in redundant operation.

3.5 PROFINET interfaces (X5, X8)

Assigning an IP address

You assign an IP address to a PROFINET interface in the CPU properties of HW Config. Download the modified configuration to the CPU. The IP address is valid for the duration of the project.

For technical reasons, the two interfaces X5/X8 must be located in different IP subnets.

Devices that can be connected via Ethernet

- SIMATIC SIS compact ES/OS with Ethernet network adapter or CP16xx communication processor
- Active network components, e.g., Scalance X200
- S7-300/S7-400, e.g., CPU 417-5H or communication processor CP443-1

Connectors

The PROFINET interfaces are implemented as Ethernet RJ45 interfaces. Always use RJ45 connectors to hook up devices to a PROFINET interface.

Properties of the PROFINET interfaces

Connection per interface	
Version	2 x RJ45
	Switch with 2 ports
Media	Twisted pair Cat5
Transmission rate	10/100 Mbps
	Autosensing Autocrossing Autonegotiation

Reference

- For detailed information about Ethernet networks, network configuration and network components refer to SIMATIC NET Manual: Twisted-Pair and Fiber-Optic Networks (https://support.industry.siemens.com/cs/ww/de/view/8763736/en?dl=en).
- For additional information about PROFINET, refer to: PROFINET (http://profibus.com/)

3.6 Overview of parameters for CPU 410SIS

Default values

All parameters are set to factory defaults. With these default values, which are suitable for a wide range of standard applications, you can use the CPU 410SIS directly without having to make any additional settings.

The default values can be determined with HW Config.

Parameter blocks

The responses and properties of the CPU are defined in parameters. The CPU 410SIS has a defined default setting. You can modify this default setting by editing the parameters in the hardware configuration.

The list below provides an overview of the assignable system properties of the CPUs.

- General properties such as the CPU name
- Watchdog interrupts, e.g., priority, interval duration
- Diagnostics/clock, e.g., time-of-day synchronization
- Security levels
- H parameters, e.g., duration of a test cycle
- Startup, for example, times for completed message from modules and transfer of parameters to modules

Parameter assignment tool

You can set the individual CPU parameters with HW Config. For additional information, see I/O configuration variants (Page 39).

Further settings

- The rack number of a CPU 410SIS, 0 or 1
  Use the selector switch on the rear panel of the CPU to change the rack number.
- The operating mode of a CPU 410SIS, stand-alone operation or redundant operation
  You set the operating mode in HW Config by configuring either a SIMATIC 400 station (stand-alone mode) or a SIMATIC H station.

PROFIBUS DP

4

4.1 CPU 410SIS as PROFIBUS DP master

Startup of the DP master system

You use the following parameters to set startup monitoring of the DP master:

- Ready message from module
- Transfer of parameters to modules

This means that the DP slaves must be started up and their parameters assigned by the CPU (as DP master) within the set time.

PROFIBUS address of the DP master

PROFIBUS addresses 0 to 126 are permissible.

Output and input data length

The maximum output or input data length you can use for each DP station is 244 bytes.

4.2 Diagnostics of the CPU 410SIS as PROFIBUS DP master

Diagnostics using LED displays

The following table explains the meaning of the BUS1F LED.

Table 4-1 Meaning of the "BUSF" LED of the CPU 410SIS as DP master

BUS1F	Meaning	Remedy
Off	Configuration correct; all configured slaves are addressable	-
Lit	• Bus fault (physical fault)	• Check whether the bus cable has shorted.
	• DP interface fault • Different baud rates in multi-DP master operation (only in stand-alone operation)	• Analyze the diagnostic data. Reconfigure or correct the configuration.
Flashes	• Station failure • At least one of the assigned slaves cannot be addressed	• Check whether the bus cable is connected to the CPU 410SIS or the bus is interrupted. • Wait until the CPU 410SIS has started up. Check the DP slaves if the LED does not stop flashing. If possible, evaluate the diagnostics of the DP slaves with direct access via the bus.

Diagnostic addresses for the DP master

You assign diagnostic addresses for PROFIBUS DP for the CPU 410SIS.

When configuring the DP master, you specify a diagnostic address for the DP slave in the associated project of the DP master.

This diagnostic address is used by DP master to obtain information about the status of DP slave or a bus interruption.

I/O configuration variants

5

5.1 Stand-alone operation

Overview

This section provides information needed for stand-alone operation of the CPU 410SIS. You will learn:

- how stand-alone operation is defined
- what you have to take into account for stand-alone operation
- how the fault tolerance-specific LEDs react in stand-alone operation
- how you configure a CPU 410SIS for stand-alone operation
- how you can expand a CPU 410SIS into an H system
- which system modifications are possible during stand-alone operation and which hardware requirements must be met

Note

The self-test is an integral component of the F-concept of the CPU 410SIS and is performed even in stand-alone operation.

Definition

Stand-alone operation is the use of a CPU 410SIS in a standard SIMATIC-400 station.

What you must observe for stand-alone operation of a CPU 410SIS

Observe the following for stand-alone operation of a CPU 410SIS:

- No synchronization modules are permitted to be inserted in stand-alone operation of a CPU 410SIS.
- The rack number must be set to "0".

Note the different procedures described below for any system change during operation:

Table 5-1 System modifications during operation

CPU 410SIS in stand-alone operation	CPU 410SIS in redundant system state
As described in Plant changes in RUN - CiR (Page 123).	As described in section Plant changes during redundant operation - H-CiR (Page 147) for redundant operation.

Fault tolerance-specific LEDs

The REDF, IFM1F, IFM2F, MSTR, RACK0 and RACK1 LEDs show the reaction specified in the table below in stand-alone operation.

LED	Behavior
REDF	Dark
IFM1F	Dark
IFM2F	Dark
MSTR	Lit
RACK0	Lit
RACK1	Dark

Configuring stand-alone operation

Requirement: No synchronization module is permitted to be inserted in the CPU 410SIS.

Procedure:

1. Insert the CPU 410SIS in a standard rack (Insert > Station > SIMATIC 400 Station in SIMATIC Manager).
2. Configure the station with the CPU 410SIS corresponding to your hardware configuration.
3. Assign the parameters of the CPU 410SIS. Use the default values, or customize the necessary parameters.
4. Configure the necessary networks and connections. For stand-alone operation, you can also configure "fault-tolerant S7 connections".

For help on procedure refer to the Help topics in SIMATIC Manager.

Expanding the configuration to a fault-tolerant system

If you want to expand the CPU 410SIS into an H system later, follow these steps:

1. Open a new project and insert a fault-tolerant station.
2. Copy the entire rack from the standard SIMATIC-400 station and insert it twice into the fault-tolerant station.
3. Insert the required subnets.
4. Copy the DP slaves from the old stand-alone operation project to the fault-tolerant station as required.
5. Reconfigure the communication connections.
6. Carry out all changes required, such as the insertion of one-sided I/O.

For information on how to configure the project, refer to the online help.

Changing the operating mode of a CPU 410SIS

To change the operating mode of a CPU 410SIS, you proceed differently depending on which operating mode you want to change to and which rack number was configured for the CPU:

Change from stand-alone to redundant operation, rack number 0

1. Insert the synchronization modules into the CPU.
2. Carry out a CPU memory reset or load a project to the CPU in which the CPU is configured for redundant operation.
3. Insert the synchronization cables into the synchronization modules.

Change from stand-alone mode to redundant operation, rack number 1

1. Set rack number 1 on the CPU.
2. Install the CPU.
3. Carry out a CPU memory reset.
4. Insert the synchronization modules into the CPU.
5. Insert the synchronization cables into the synchronization modules.

Changing from redundant to stand-alone operation

1. Remove the CPU.
2. Remove the synchronization modules.
3. Set rack number 0 on the CPU.
4. Install the CPU.
5. Download a project to the CPU in which the CPU is configured for stand-alone operation.

5.2 Fail-safe operation

Ensuring functional safety

A safety-related system encompasses sensors for signal acquisition, an evaluation unit for processing the signals, and actuators for signal output.

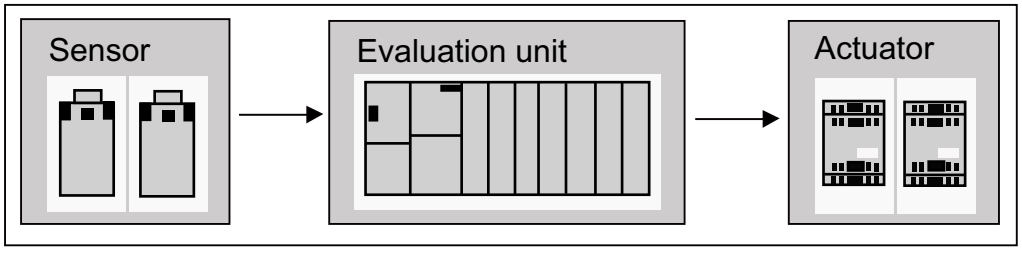


Figure 5-1 Processing chain: acquire, process, output

All of the components contribute to the functional safety of the system, in order, when a dangerous event occurs, to put the system into a safe state or to keep it in a safe state.

Safety of fail-safe SIMATIC Safety Integrated systems

For SIMATIC Safety Integrated systems, the evaluation unit consists, for example, of fail-safe single-channel CPUs and fail-safe dual-channel I/O modules. The fail-safe communications take place via the safety-related PROFIsafe profile.

Functions of a fail-safe CPU

A fail-safe CPU has the following functions:

- Comprehensive self-tests and self-diagnostics check the fail-safe state of the CPU.
- Simultaneous execution of standard and safety programs on one CPU. When there are changes to the standard user program, there are no unwanted effects on the safety program.

S7 F/FH Systems

The S7 F Systems optional package adds safety functions to the CPU 410SIS. The current TÜV certificates are available at the Internet address (http://support.automation.siemens.com) under "Product Support".

Fail-safe I/O modules (F-modules)

F-modules have all of the required hardware and software components for safe processing in accordance with the required safety class. This includes wire tests for short-circuit and cross-circuit. You only program the user safety functions.

Safety-related input and output signals form the interface to the process. This enables, for example, direct connection of single-channel and two-channel I/O signals from devices such as EMERGENCY STOP buttons or light barriers.

Safety-related communication with PROFIsafe profile

PROFIsafe was the first communication standard according to the IEC 61508 safety standard that permits both standard and safety-related communication on one bus line. This not only results in an enormous savings potential with regard to cabling and part variety, but also the advantage of retrofit ability.

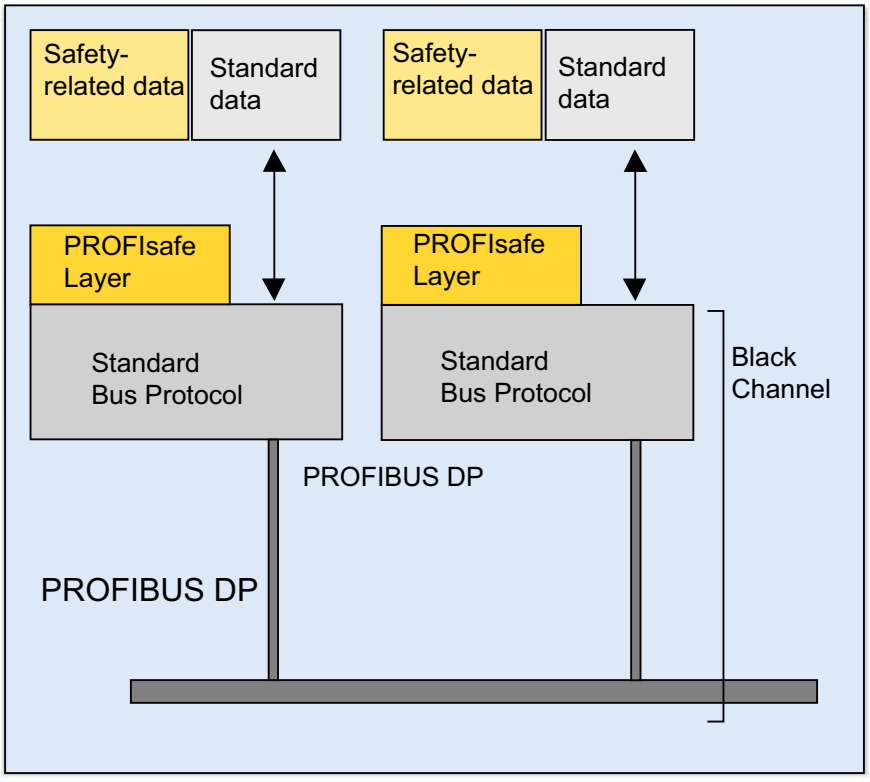


Figure 5-2 Safety-related communication

Safety-related and standard data are transmitted with PROFIsafe over the same bus line. Black channel means that collision-free communication via a bus system with media-independent network components (also wireless) is possible.

PROFIsafe is an open solution for safety-related communication via standard fieldbuses. Numerous manufacturers of safety components and end users of safety technology have helped to develop this vendor-neutral and open standard for PROFIBUS International (PI).

The PROFIsafe profile supports safe communication for the open PROFIBUS DP standard buses.

PROFIsafe is certified to IEC 61784-3 and meets the highest requirements for the manufacturing and process industry.

PROFIBUS is the global standard for fieldbuses with approximately 13 million installed nodes. Its market acceptance is so high because a large number of manufacturers offer many products for PROFIBUS. With the PA transmission variant (IEC 1158-2), PROFIBUS extends the unified system concept of distributed automation to the process world.

PROFIsafe uses PROFIBUS services for safe communication. A fail-safe CPU 410SIS and the fail-safe I/O exchange both user data as well as status and control information; no additional hardware is required for this.

PROFIsafe takes the following measures to counteract the various possible errors when transferring messages.

Table 5-2 Measures in PROFIsafe for error avoidance

Measure/ Error	Consecutive number	Time expectation with acknowledgment	Identifier for sender and receiver	Data backup CRC
Repetition	✓			
Loss	✓	✓		
Insertion	✓	✓	✓	
Incorrect sequence	✓			
Data falsification				✓
Delay		✓		
Coupling of safety-related messages and standard messages (masquerade)		✓	✓	✓
FIFO errors (first-in-first-out data register for maintaining the sequence)		✓		

See also

S7 F Systems optional package (https://support.industry.siemens.com/cs/ww/en/view/109482252)

5.3 Fault-tolerant automation systems (redundancy operation)

5.3.1 Redundant SIMATIC automation systems

Operating objectives of redundant automation systems

Redundant automation systems are used in practice with the aim of achieving a higher degree of availability or fault tolerance.

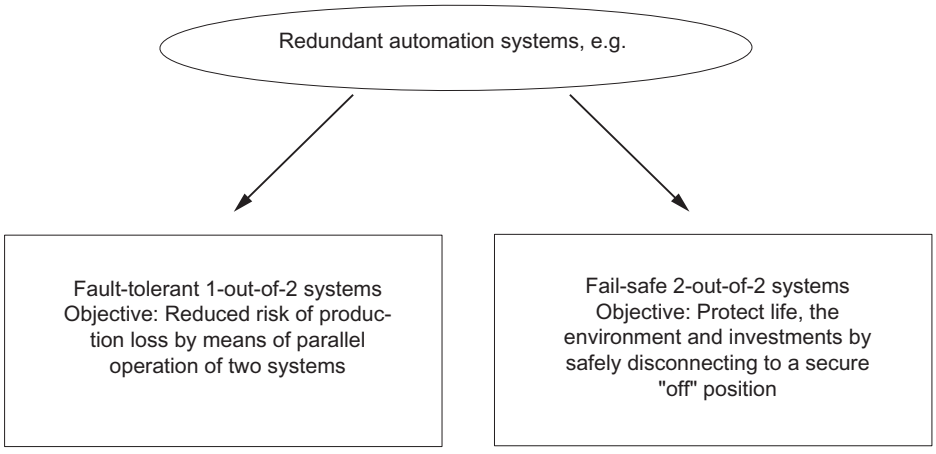


Figure 5-3 Operating objectives of redundant automation systems

You may only use the AS 410 SIS to control safety-related processes if you have programmed it and assigned its parameters in accordance with the rules for F systems.

You can find information on this in following manual: SIMATIC Industrial Software S7 F/FH Systems (http://support.automation.siemens.com/WW/view/en/109742100)

Why fault-tolerant automation systems?

The purpose of using fault-tolerant automation systems is to reduce production downtimes, regardless of whether the failures are caused by an error/fault or are due to maintenance work.

The higher the costs of production stops, the greater the need to use a fault-tolerant system. The generally higher investment costs of fault-tolerant systems are soon recovered since production stops are avoided.

Redundant I/O

Input/output modules are termed redundant when they exist twice and they are configured and operated as redundant pairs. The use of redundant I/O provides the highest degree of availability, because the system tolerates the failure of a CPU or of a signal module.

Single-channel switched I/O

In single-channel switched configuration, there is one of each of the input/output modules. In redundant operation, these modules can addressed by both subsystems. The single-channel switched I/O configuration is recommended for system components which tolerate the failure of individual modules.

See also

Connection of two-channel I/O to the PROFIBUS DP interface (Page 53)

5.3.2 Increase of plant availability, reaction to errors

System-wide integration

The CPU 410SIS and all other SIMATIC components, such as the SIMATIC SIS compact control system, are designed to be compatible. The system-wide integration, ranging from the control room to the sensors and actuators, is implemented as a matter of course and ensures maximum system performance.

Graduated availability by duplicating components

AS 410H SIS is configured redundantly to ensure its availability at all times. This means: all essential components are duplicated.

The CPU, the power supply and the hardware for connecting the two CPUs are available in duplicate.

You yourself decide on any other components you want to duplicate to increase availability depending on the specific process you are automating.

Redundancy nodes

Redundant nodes represent the fail safety of systems with redundant components. A redundant node can be considered as independent when the failure of a component within the node does not result in reliability constraints in other nodes or in the overall system.

The availability of the overall system can be illustrated simply in a block diagram. With a 1-out-of-2 system, **one** component of the redundant node may fail without impairing the operability of the overall system. The weakest link in the chain of redundant nodes determines the availability of the overall system

No error/fault

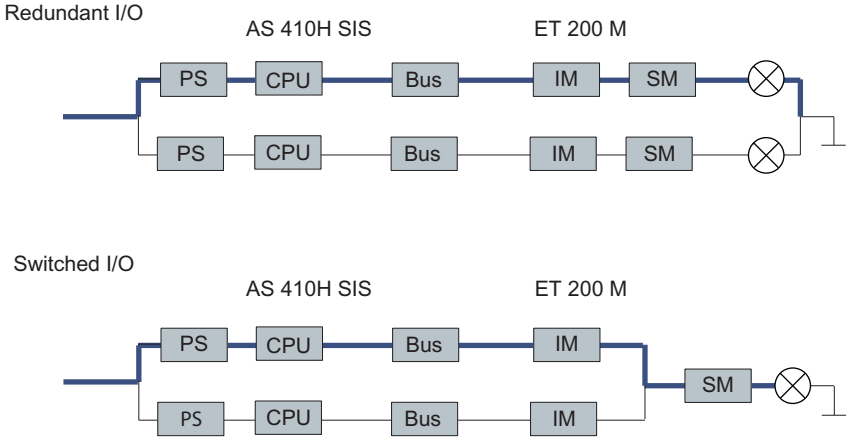


Figure 5-4 Example of redundancy in a network without error

With error/fault

The following figure shows how a component may fail without impairing the functionality of the overall system.

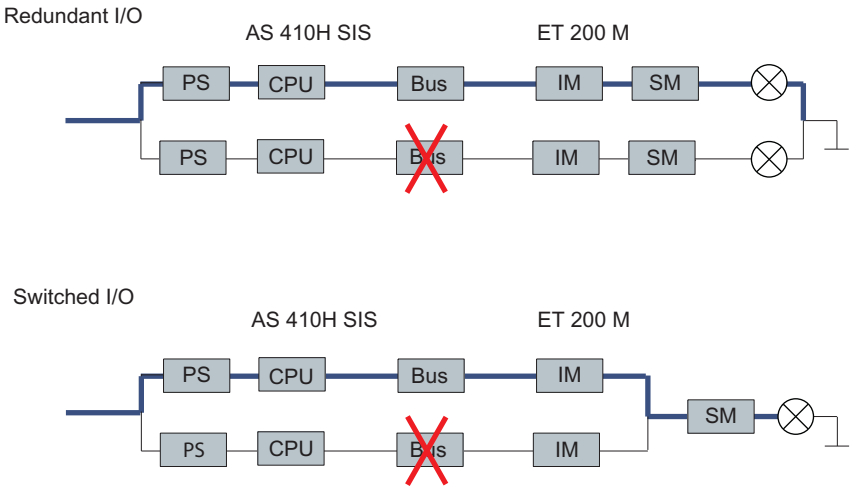


Figure 5-5 Example of redundancy in a 1-out-of-2 system with error

Failure of a redundant node (total failure)

The following figure shows that the overall system is no longer operable, because both subunits have failed in a 1-out-of-2 redundancy node (total failure).

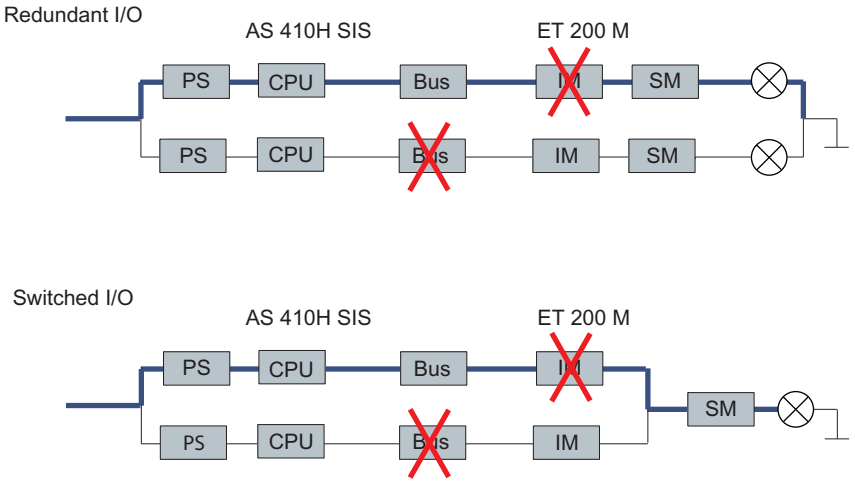


Figure 5-6 Example of redundancy in a 1-out-of-2 system with total failure

5.4 Using single-channel switched I/O

What is single-channel switched I/O?

In single-channel switched configuration, there is one of each of the input/output modules.

In redundant operation, these can addressed by both subsystems.

In stand-alone operation, the master subsystem always addresses **all switched I/O** (in contrast to one-sided I/O).

The single-channel switched I/O configuration is recommended for system components that tolerate the failure of individual modules within the ET 200M or ET 200iSP.

Single-channel switched I/O configuration at the PROFIBUS DP interface

The installation with single-channel switched I/O is possible with the ET 200M distributed I/O device with active backplane bus and redundant PROFIBUS DP slave interface and with the ET 200iSP distributed I/O device.

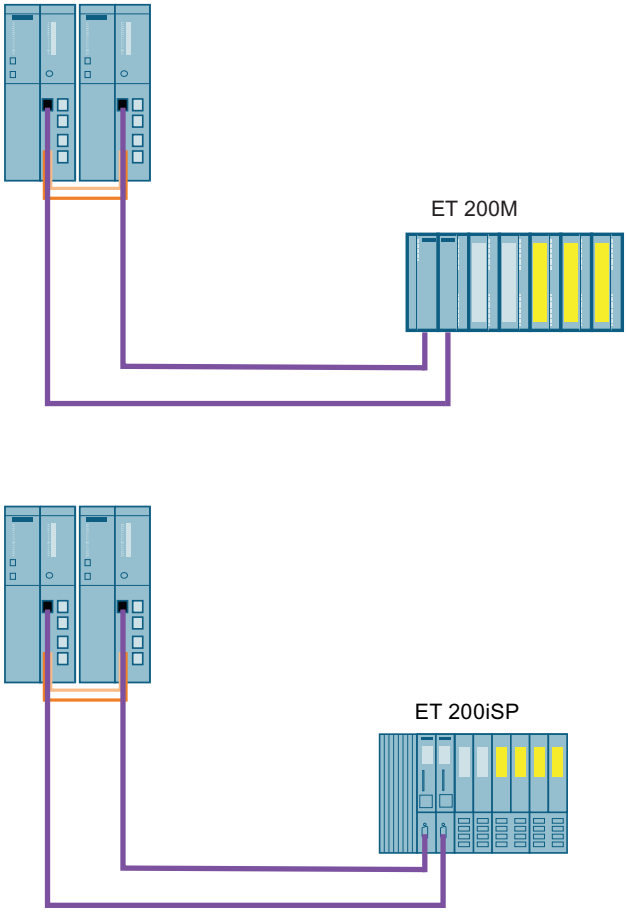


Figure 5-7 Single-channel switched distributed I/O configuration at the PROFIBUS DP interface

You can use the following interface modules for the I/O configuration at the PROFIBUS DP interface:

Table 5-3 Interface modules for use of single-channel switched I/O configuration at the PROFIBUS DP interface

Interface module	Article No.
IM 152 for ET 200iSP	6ES7152-1AA00-0AB0 V2.0 or higher
IM 153-2 for ET 200M	6ES7153-2BA70-0XB0

Each subsystem of the AS 410H SIS is connected to one of the two DP slave interfaces of the ET 200M over a DP master interface.

Bus modules for hot swapping

You can use the following bus modules for hot swapping a variety of components:

Table 5-4 Bus modules for hot swapping

Bus module	Article No.
BM PS/IM for load power supply and IM 153	6ES7195-7HA00-0XA0
BM 2 x 40 for two modules with 40 mm width	6ES7195-7HB00-0XA0
BM 1 x 80 for a module with 80 mm width	6ES7195-7HC00-0XA0
BM IM/IM for two IM 153-2/2 FO for design of redundant systems	6ES7195-7HD10-0XA0

Y-Link

The Y-Link consists of two IM 153-2 interface modules and one Y coupler that are connected with one another by bus modules.
The Y-Link creates a gateway from the redundant DP master system of an AS 410H SIS to a non-redundant DP master system. This means that devices with only one PROFIBUS DP interface can be connected to an AS 410H SIS as switched I/Os.

A single-channel DP master system can be connected to a redundant system via a Y coupler. The following IM 157 Y coupler is permissible: 6ES7197-1LB00 0XA0.

You can use the following Y-Link:

Y-Link	Article No.
ET 200M as Y-Link with	6ES7153-2BA70-0XB0

Rule for PROFIBUS DP

If you are using single-channel switched I/O, CPU 410SIS must be in the same slot in both subsystems, for example, in slot 4 in both subsystems.

Single-channel switched I/O and user program

In redundant operation, in principle any subsystem can access single-channel switched I/O. The data is automatically transferred via the synchronization link and compared. An identical value is available to the two subsystems at all times owing to the synchronized access.

If you have connected the I/O over two IMs, the CPU accesses the I/O over one IM. The active IM is indicated by illumination of the ACT LED.

The path via the currently active DP interface is called the **active channel**, while the path via the other interface is called the **passive channel**. The DP cycle is always active on both channels. However, only the input and output values of the active channel are processed in the user program or output to the I/O. The same applies to asynchronous activities, such as interrupt processing and the exchange of data records.

Failure of the single-channel switched I/O

If a fault occurs, the AS 410H SIS with single-channel switched I/O behaves as follows:

- The faulty I/O is no longer available if an input/output module or a connected device fails.
- In certain failure situations (for example failure of a subsystem, a DP master system or an IM153-2 DP slave interface), the single-channel switched I/O continues to be available for the process.
  This is achieved by a changeover between active and passive channel. This changeover takes place separately for each DP station. A distinction is made between the following two types of failure:
  - Failures affecting only one station (such as failure of the DP slave interface of the channel currently active)
  - Failures affecting all stations of a DP master system
    These include removal of the connector at the DP master interface, shutdown of the DP master system and a short-circuit in the cable harness of a DP master system.

The following applies to each station affected by a failure: If both DP slave interfaces are functional and the active channel fails, the previously passive channel automatically becomes the active channel. A redundancy loss is reported to the user program when OB 70 starts (event W#16#73A3).

Once the problem is eliminated, redundancy is restored. This also starts OB 70 (event W#16#72A3). In this situation, there is no changeover between the active and passive channel.

If one channel has already failed, and the remaining (active) channel also fails, then there is a complete station failure. This starts OB 86 (event W#16#39C4).

Duration of a changeover of the active channel

The maximum changeover time is

DP error detection time + DP changeover time + changeover time of the DP slave interface

You can determine the first two values from the bus parameters of your DP master system in STEP 7. You determine the last two values from the manuals of the DP slave interfaces in question.

Note

For fail-safe modules, you need to select the monitoring time of each fail-safe module longer than the switching time of the active channel in the fault-tolerant system. If you ignore this rule, you risk passivation of the fail-safe modules during the changeover of the active channel.

You can use the Excel file "s7ftime.xls" to calculate the monitoring and response times. The file is available at the following address:

http://support.automation.siemens.com/WW/view/en/22557362

Note

Please note that the CPU can only detect a signal change if the signal duration is greater than the specified changeover time.
When there is a changeover of the entire DP master system, the changeover time of the slowest DP component applies to all DP components. As a rule, a Y-Link determines the switching time and the associated minimum signal duration. We therefore recommend that you connect Y-Links to a separate DP master system.

Changeover of the active channel during link-up and updating

During link-up and updating with master/standby changeover (see Link-up and update (Page 89)), a changeover between the active and passive channels occurs for all stations of the switched I/O. At the same time OB 72 is called.

Bumpless changeover of the active channel

To prevent the I/O failing temporarily or outputting substitute values during the changeover between the active and passive channel, the DP stations of the switched I/O put their outputs on hold until the changeover is complete and the new active channel has taken over.

To ensure that total failures of a DP station that happen during changeover are also detected, the changeover is monitored by the individual DP stations and by the DP master system.

See also

Time monitoring (Page 90)

s7ftimea (https://support.industry.siemens.com/cs/ww/de/view/22557362/en?dl=en)

5.5 Connection of two-channel I/O to the PROFIBUS DP interface

5.5.1 Connecting redundant I/O

Redundant I/O in the switched DP slave

To achieve this, the signal modules are installed in pairs in ET 200M distributed I/O devices with active backplane bus.

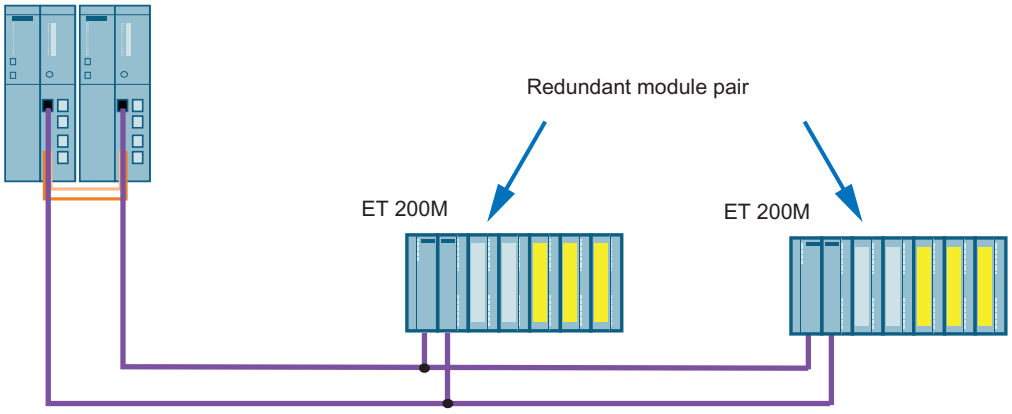


Figure 5-8 Redundant I/O in the switched DP slave

Principle of channel group-specific redundancy

Channel errors due to discrepancy cause the passivation of the respective channel. Channel errors due to diagnostic interrupts (OB82) cause the passivation of the channel group affected. Depassivation depassivates all affected channels as well as the modules passivated due to module errors. Channel group-specific passivation significantly increases availability in the following situations:

- Relatively frequent encoder failures
- Repairs that take a long time
- Multiple channel errors on one module

Note

Channel and channel group

Depending on the module, a channel group contains a single channel, a group of several channels, or all channels of the module. You can therefore operate all modules with redundancy capability in channel group-specific redundancy mode.

You can find an up-to-date list of modules with redundancy capability in Signal modules for redundancy (Page 56).

"Functional I/O redundancy" block library

The blocks you use for channel group-specific redundancy are located in the "Redundant IO CGP V50" library.

The "Functional I/O redundancy" block libraries that support the redundant I/O each contain the following blocks:

- FC 450 "RED_INIT": Initialization function
- FC 451 "RED_DEPA": Initiate depassivation
- FB 450 "RED_IN": Function block for reading redundant inputs
- FB 451 "RED_OUT": Function block for controlling redundant outputs
- FB 452 "RED_DIAG": Function block for diagnostics of redundant I/O
- FB 453 "RED_STATUS": Function block for redundancy status information

Configure the numbers of the management data blocks for the redundant I/O in HW Config "CPU Properties -> H Parameters". Assign unassigned DB numbers for these data blocks. The data blocks are created by FC 450 "RED_INIT" during CPU startup. The default setting for the management data block numbers is 1 and 2. These data blocks are not the instance data blocks of FB 450 "RED_IN" or FB 451 "RED_OUT".

You can open the libraries in the SIMATIC Manager with "File -> Open -> Libraries"

The relevant online help describes the functions and use of the blocks.

Using the blocks

Before you use the blocks, configure the redundant modules in HW Config as redundant.

The OBs into which you need to link the various blocks are listed in the table below:

Block	OB
FC 450 "RED_INIT"	• OB 72 "CPU redundancy error" (only with fault-tolerant systems) FC 450 is only processed after start event B#16#33:"Standby/ master switchover by operator" • OB 80 "Timeout error" (only in single mode) FC 450 is only executed after the start event "Resume RUN after reconfiguring" • OB 100 "Restart" (the administration DBs are recreated, see the online help) • OB 102 "Cold restart"
FC 451 "RED_DEPA"	If you call FC 451 in OB 83 while inserting modules or in OB 85 during alarm output, depassivation is delayed by approximately 3 seconds. In addition the FC 451 should be executed after the removal of the error response as specific call in OB 1 and/or OB 30 to 38. The FC451 only depassivates modules in the corresponding process image partition. Depassivation is delayed by 10 s.
FB 450 "RED_IN"	• OB 1 "Cyclic program" • OB 30 to OB 38 "Watchdog interrupt"

Block	OB
FB 451 "RED_OUT"	• OB 1 "Cyclic program" • OB 30 to OB 38 "Watchdog interrupt"
FB 452 "RED_DIAG"	• OB 72 "CPU redundancy error" • OB 82 "Diagnostic interrupt" • OB 83 "Remove/insert interrupt" • OB 85 "Program execution error"
FB 453 "RED_STATUS"	• OB 1 "Cyclic program" (fault-tolerant systems only) • OB 30 to OB 38 "Watchdog interrupt"

To be able to address redundant modules using process image partitions in watchdog interrupts, the relevant process image partition must be assigned to this pair of modules and to the watchdog interrupt. Call FB 450 "RED_IN" in this watchdog interrupt before you call the user program. Call FB 451 "RED_OUT" in this watchdog interrupt after you call the user program.

The valid values that can be processed by the user program are always located at the lower address of both redundant modules. This means that only the lower address can be used for the application; the values of the higher address are not relevant for the application.

Note

Use of FB 450 "RED_IN" and 451 "RED_OUT" when using process image partitions

For each priority class used (OB 1, OB 30 ... OB 38), you must use a separate process image partition.

HW configuration and configuring the redundant I/O

Follow the steps below to use redundant I/O:

1. Insert all the modules you want to operate redundantly. Please also observe the default rules for configuration detailed below.
2. Configure the module redundancy under HW Config in the object properties of the respective module.
   Either search for a partner module for each module or use the default settings.
   If the module is inserted in the slave with a DP address at slot X, the module in the slave with the next Profibus address at slot X will be suggested.
3. Enter the remaining redundancy parameters for the input modules.

Note

System modifications during operation are also supported with redundant I/O.

Note

Always switch off power to the station or rack before you remove a redundant digital input module that does not support diagnostics functions and is not passivated. You might otherwise passivate the wrong module. This procedure is necessary, for example, when replacing the front connector of a redundant module.

Redundant modules must be in the process image of the inputs or outputs. Redundant modules are always accessed using the process image.

If you are using redundant modules, you must set the following in "HW Config -> CPU 41x-H Properties" in the "Cycle/Clock memory" tab:

"OB 85 call on I/O area access error > Only incoming and outgoing errors"

5.5.2 Signal modules for redundancy

Signal modules as redundant I/O

You can use the signal modules listed below as redundant distributed I/O connected to PROFIBUS DP. Read the current information on using the modules in the SIMATIC SIS compact readme.

Note

The statements on the individual signal modules in this section refer exclusively to their use in redundant operation. Restrictions and special features listed here especially do not apply to the use of the corresponding module in stand-alone operation.

Take into account that you can only use modules of the same product version and same firmware version as redundant pairs.

A complete list of all modules released for SIMATIC SIS compact V9.0 can be found in the SIMATIC SIS compact technical documentation, see Technical documentation.

Table 5-5 Signal modules for redundancy

Module	Article No.
Redundant DI dual-channel	
DI16xDC 24 V, interrupt	6ES7 321-7BH00-0AB0
DI16xDC 24 V	6ES7 321-7BH01-0AB0
In the event of an error on one channel, the entire group (2 channels) is passivated. When using the module with HF index, only the faulty channel is passivated in the event of a channel error. Use with non-redundant encoder • This module supports the "wire break" diagnostic function. To implement this function, make sure that a total current between 2.4 mA and 4.9 mA flows even at signal state "0" when you use an encoder that is evaluated at two inputs in parallel. You achieve this by connecting a resistor across the encoder. Its value depends on the type of switch and usually ranges between 6800 and 8200 ohms for contacts. For BEROS, calculate the resistance using the following formula: (30 V / (4.9 mA - I_R_Bero) < R < (20 V / (2.4 mA - I_R_Bero)	
DI16xDC 24 V	6ES7 321-1BH02-0AA0
In some system states, it is possible that an incorrect value of the first module is read in briefly when the front connector of the second module is removed. This is prevented by using series diodes.	
DI32xDC 24 V	6ES7 321-1BL00-0AA0
In some system states, it is possible that an incorrect value of the first module is read in briefly when the front connector of the second module is removed. This is prevented by using series diodes.	
DI 8xAC 120/230V	6ES7 321-1FF01-0AA0
DI 4xNamur [EEx ib]	6ES7 321-7RD00-0AB0
You cannot use the module in redundant operation for applications in hazardous areas. Use with non-redundant encoder • You can only connect 2-wire NAMUR encoders or contact makers. • Equipotential bonding of the encoder circuit should always be at one point only (preferably encoder negative). • When selecting encoders, compare their properties with the specified input characteristics. Remember that this function must always be available, regardless of whether you are using one or two inputs.	
DI 16xNamur	6ES7321-7TH00-0AB0
Use with non-redundant encoder • Equipotential bonding of the encoder circuit should always be at one point only (preferably encoder negative). • Operate the two redundant modules on a common load power supply. • When selecting encoders, compare their properties with the specified input characteristics. Remember that this function must always be available, regardless of whether you are using one or two inputs.	
DI 24xDC 24 V	6ES7326-1BK02-0AB0
F module in standard mode and safety mode	
DI 8xNAMUR [EEx ib]	6ES7326-1RF00-0AB0
F module in standard mode and safety mode	
Redundant DO dual-channel	
DO8xDC 24 V/0.5 A	6ES7322-8BF00-0AB0

Module	Article No.
Definite evaluation of the diagnostics information "P short-circuit" and "wire break" is not possible. Deselect these individually in your configuration.	
DO8xDC 24 V/2 A	6ES7322-1BF01-0AA0
DO32xDC 24 V/0.5 A	6ES7322-1BL00-0AA0
DO8xAC 120/230 V/2 A	6ES7322-1FF01-0AA0
DO 4x24 V/10 mA [EEx ib]	6ES7322-5SD00-0AB0
You cannot use the module in redundant operation for applications in hazardous areas.	
DO 4x15 V/20 mA [EEx ib]	6ES7322-5RD00-0AB0
You cannot use the module in redundant operation for applications in hazardous areas.	
DO 16xDC 24 V/0.5 A	6ES7322-8BH01-0AB0
• The equipotential bonding of the load circuit should always be at one point only (preferably load minus). • Diagnostics of the channels is not possible.	
DO 16xDC 24 V/0.5 A	6ES7322-8BH10-0AB0
• The equipotential bonding of the load circuit should always be at one point only (preferably load minus).	
DO 10xDC 24 V/2 A	6ES7326-2BF10-0AB0
F module in safety mode	
Redundant AI dual-channel	
AI8x12Bit	6ES7331-7KF02-0AB0
Use in voltage measurement • The "wire break" diagnostics function in HW Config must not be enabled either the modules are operated with transmitters or when thermocouples are connected. Use for indirect current measurement • When determining the measuring error, observe the following: The total input resistance in measuring ranges > 2.5 V is reduced from a nominal 100 kilohms to 50 kilohms when you operate two inputs connected in parallel. • The "wire break" diagnostics function in HW Config must not be enabled either the modules are operated with transmitters or when thermocouples are connected. • Use a 50 ohm resistor (measuring range +/- 1 V) or 250 ohm resistor (measuring range 1 to 5 V) to map the current on a voltage. The tolerance of the resistor must be added on to the module error. • This module is not suitable for direct current measurement. Use of redundant encoders: • You can use a redundant encoder with the following voltage settings: +/- 80 mV (only without wire break monitoring) +/- 250 mV (only without wire break monitoring) +/- 500 mV (wire break monitoring not configurable) +/- 1 V (wire break monitoring not configurable) +/- 2.5 V (wire break monitoring not configurable) +/- 5 V (wire break monitoring not configurable) +/- 10 V (wire break monitoring not configurable) 1...5 V (wire break monitoring not configurable)	
AI 8x16Bit	6ES7 331-7NF00-0AB0

Module	Article No.
Use in voltage measurement • The "wire break" diagnostics function in HW Config must not be enabled when the modules are operated with transmitters. Use in indirect current measurement • When using indirect current measurement, ensure a reliable connection between the sensor resistances and the actual inputs, because a reliable wire break detection cannot be guaranteed in the case of a wire break of individual cables of this connection. • Use a 250 ohm resistor (measuring range 1 to 5 V) to map the current on a voltage. Use in direct current measurement • Suitable Zener diode: BZX85C8v2 • Circuit-specific additional error: If one module fails, the other may suddenly show an additional error of approx. 0.1%. • Load capability of 4-wire transmitters: R_B > 610 ohms (determined for worst case: 1 input + 1 Zener diode at an S7 overload value of 24 mA to $R_B = (R_E * I_{max} + U_{z\,max}) / I_{max)}$ • Input voltage in the circuit when operating with a 2-wire transmitter: $U_{e\text{-}2w}$ < 15 V (determined for worst case: 1 input + 1 Zener diode at an S7 overload value of 24 mA to $U_{e\text{-}2w} = R_E * I_{max} + U_{z\,max}$)	
AI 8x16Bit	6ES7 331-7NF10-0AB0
Use in voltage measurement • The "wire break" diagnostics function in HW Config must not be enabled either the modules are operated with transmitters or when thermocouples are connected. Use in indirect current measurement • Use a 250 ohm resistor (measuring range 1 to 5 V) to map the current on a voltage. Use in direct current measurement • Suitable Zener diode: BZX85C8v2 • Load capability of 4-wire transmitters: R_B > 610 ohms (determined for worst case: 1 input + 1 Zener diode at an S7 overload value of 24 mA to $R_B = (R_E * I_{max} + U_{z\,max}) / I_{max)}$ • Input voltage in the circuit when operating with a 2-wire transmitter: $U_{e\text{-}2w}$ < 15 V (determined for worst case: 1 input + 1 Zener diode at an S7 overload value of 24 mA to $U_{e\text{-}2w} = R_E * I_{max} + U_{z\,max}$)	
AI 6xTC 16Bit iso	6ES7331-7PE10-0AB0
Notice: You may use this module only with redundant sensors. You can use this module with Version 3.5 or higher of FB 450 "RED_IN" in the library "Redundant IO MGP" and Version 5.8 or higher of FB 450 "RED_IN" in the library "Redundant IO CGP" V50. Observe the following when measuring temperatures by means of thermocouples and assigned redundancy: The value specified in "Redundancy" under "Tolerance window" is always based on 2765 °C. For example, a check is made for a tolerance of 27 degrees when "1" is entered and 138 degrees when "5" is entered. A FW update is not possible in redundant operation An online calibration is not possible in redundant operation. Use in voltage measurement • The "wire break" diagnostics function in HW Config must not be enabled when the modules are operated with thermocouples. Use in indirect current measurement • Due to the maximum voltage range +/- 1 V, the indirect current measurement can be carried out exclusively via a 50 ohm resistor. Mapping that conforms to the system is only possible for the area +/- 20 mA.	
AI 4x15Bit [EEx ib]	6ES7331-7RD00-0AB0

Module	Article No.
You cannot use the module in redundant operation for applications in hazardous areas. It is not suitable for indirect current measurement. Use in direct current measurement • Suitable Zener diode 6.2 V, for example BZX85C6v2 • Load capability of 4-wire transmitters: RB > 325 ohms determined for worst case: 1 input + 1 Zener diode at an S7 overload value of 24 mA to RB = (RE * $I_{max +}$ $U_{z\ max}$)/I_{max} • Input voltage for 2-wire transmitters: Ue-2Dr < 8 V calculated for worst case: 1 input + 1 Zener diode at an S7 overload value of 24 mA to Ue-2Dr = RE * I_{max} + $U_{z\ max}$ **Note:** You can only connect 2-wire transmitters with a 24 V external supply or 4-wire transmitters. The internal power supply for transmitters cannot be used in the circuit because it outputs only 13 V, which means in the worst case it would supply only 5 V to the transmitter.	
AI 8x0/4...20mA HART	6ES7 331-7TF01-0AB0
A firmware update is not possible in redundant operation. Online calibration is not possible in redundant operation. See Manual *ET 200M Distributed I/O Device; HART Analog Modules* manual	
AI6x0/4...20mA HART	6ES7336-4GE00-0AB0
F module in safety mode	
Redundant AO dual-channel	
AO4x12 Bit	6ES7332-5HD01-0AB0
AO8x12 Bit	6ES7332-5HF00-0AB0
AO4x0/4...20 mA [EEx ib]	6ES7332-5RD00-0AB0
You cannot use the module in redundant operation for applications in hazardous areas.	
AO 8x0/4...20mA HART	6ES7 332-8TF01-0AB0
A firmware update is not possible in redundant operation. Online calibration is not possible in redundant operation. See Manual *ET 200M Distributed I/O Device; HART Analog Modules*	

Using digital input modules as redundant I/O

The following parameters were set to configure digital input modules for redundant operation:

- Discrepancy time (maximum permitted time in which the redundant input signals may differ).
  The specified discrepancy time must be a multiple of the update time of the process image and therefore also the basic conversion time of the channels.
  When there is still a discrepancy in the input values after the configured discrepancy time has expired, an error has occurred.
- Response to a discrepancy in the input values

First, the input signals of the paired redundant modules are checked for consistency. If the values match, the uniform value is written to the lower memory area of the process input image. If there is a discrepancy and it is the first, it is marked accordingly and the discrepancy time is started.

During the discrepancy time, the most recent matching (non-discrepant) value is written to the process image of the module with the lower address. This procedure is repeated until the values once again match within the discrepancy time or until the discrepancy time of a bit has expired.

If the discrepancy continues past the expiration of the configured discrepancy time, an error has occurred.

The defective side is localized according to the following strategy:

1. During the discrepancy time, the most recent matching value is retained as the result.
2. Once the discrepancy time has expired, the following error message is displayed: Error code 7960: "Redundant I/O: discrepancy time at digital input expired, error not yet localized". Passivation is not performed and no entry is made in the static error image. Until the next signal change occurs, the configured response is performed after the discrepancy time expires.
3. If another signal change now occurs, the channel in which the signal change occurred is the intact channel and the other channel is passivated.

Note

The time that the system actually needs to determine a discrepancy depends on various factors: Bus runtimes, cycle times and call times of the user program, conversion times, etc. For this reason, it is possible for redundant input signals to be different for longer than the configured discrepancy time.

Modules with diagnostics capability are also passivated by calling OB 82.

MTA Terminal Modules

MTA terminal modules (Marshalled Termination Assemblies) can be used to connect field devices, sensors and actuators to the I/O modules of the ET 200M remote I/O stations simply, quickly and reliably. They can be used to significantly reduce the costs and required work for cabling and commissioning, and prevent wiring errors.

The individual MTA terminal modules are each tailored to specific I/O modules from the ET 200M range. MTA versions for standard I/O modules are also available, as for redundant and safety-related I/O modules. The MTA terminal modules are connected to the I/O modules using 3 m or 8 m long preassembled cables.

Details on combinable ET 200M modules and suitable connecting cables and on the current MTA product range can be found at the following address: Update and expansion of the MTA terminal modules (https://support.industry.siemens.com/cs/ww/de/view/29289048/en?dl=en)

Using redundant digital input modules with non-redundant encoders

With non-redundant encoders, you use digital input modules in a 1-out-of-2 configuration:

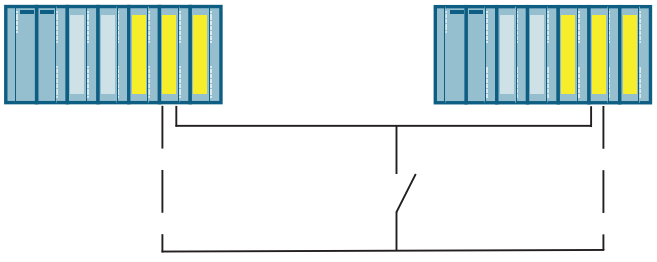


Figure 5-9 Fault-tolerant digital input module in 1-out-of-2 configuration with one encoder

The use of redundant digital input modules increases their availability.

Discrepancy analysis detects "Continuous 1" and "Continuous 0" errors of the digital input modules. A "Continuous 1" error means the value 1 is applied permanently at the input; a "Continuous 0" error means that the input is not energized. This can be caused, for example, by a short-circuit to L+ or M.

The current flow over the chassis ground connection between the modules and the encoder should be the minimum possible.

When connecting an encoder to several digital input modules, the redundant modules must operate at the same reference potential.

If you want to replace a module during operation and are not using redundant encoders, you will need to use decoupling diodes.

Note

Remember that the proximity switches (Beros) must provide the current for the channels of both digital input modules. The technical specifications of the respective modules, however, specify only the required current per input.

Using redundant digital input modules with redundant encoders

With redundant encoders, you use digital input modules in a 1-out-of-2 configuration:

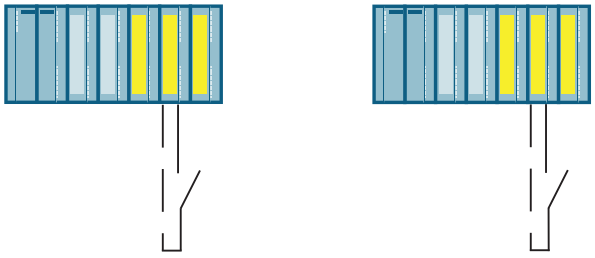


Figure 5-10 Fault-tolerant digital input modules in 1-out-of-2 configuration with two encoders

The use of redundant encoders also increases their availability. A discrepancy analysis detects all errors, except for the failure of a non-redundant load voltage supply. You can enhance availability by installing redundant load power supplies.

Redundant digital output modules

Fault-tolerant control of a final controlling element can be achieved by connecting two outputs of two digital output modules or fail-safe digital output modules in parallel (1-out-of-2 configuration).

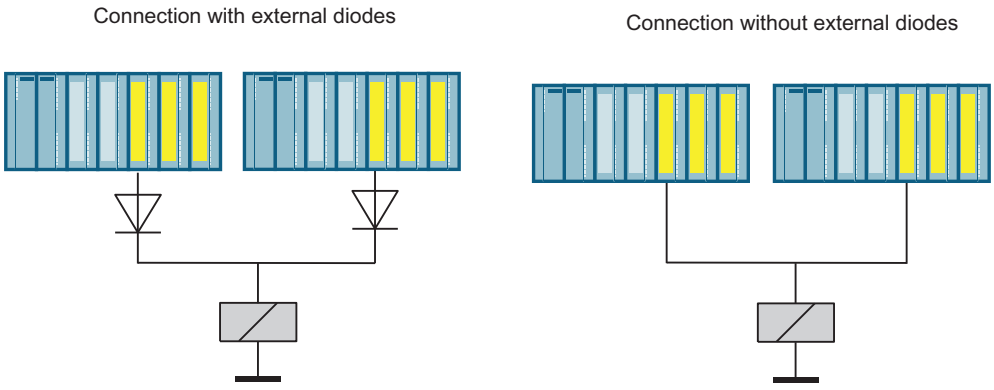


Figure 5-11 Fault-tolerant digital output modules in 1-out-of-2 configuration

The digital output modules must be connected to a common load voltage supply.

Using analog input modules as redundant I/O

You specified the following parameters when you configured the analog input modules for redundant operation:

- Tolerance window (configured as a percentage of the end value of the measuring range)
  Two analog values are considered equal if they are within the tolerance window.
- Discrepancy time (maximum permitted time in which the redundant input signals can be outside the tolerance window). The specified discrepancy time must be a multiple of the update time of the process image and therefore also the basic conversion time of the channels.
  An error is generated when there is an input value discrepancy after the configured discrepancy time has expired.
  If you connect identical sensors to both analog input modules, the default value for the discrepancy time is usually sufficient. If you use different sensors, in particular temperature sensors, you will have to increase the discrepancy time.
- Applied value
  The applied value represents the value of the two analog input values that is applied to the user program.

The system verifies that the two read-in analog values are within the configured tolerance window. If they are, the applied value is written to the lower data memory area of the process input image. If there is a discrepancy and it is the first, it is marked accordingly and the discrepancy time is started.

When the discrepancy time is running, the most recent valid value is written to the process image of the module with the lower address and made available to the current process. If the discrepancy time expires, the channel with the configured standard value is declared as valid and the other channel is passivated. If the maximum value from both modules is configured as the standard value, this value is then taken for further program execution and the other

channel is passivated. If the minimum value is set, this channel supplies the data to the process and the channel with the maximum value is passivated. Whichever is the case, the passivated channels are entered in the diagnostic buffer.

If the discrepancy is eliminated within the discrepancy time, analysis of the redundant input signals is still carried out.

Note

The time that the system actually needs to determine a discrepancy depends on various factors: Bus runtimes, cycle times and call times of the user program, conversion times, etc. For this reason, it is possible for redundant input signals to be different for longer than the configured discrepancy time.

Note

There is no discrepancy analysis when a channel reports an overflow with 16#7FFF or an underflow with 16#8000. The relevant channel is passivated immediately.

You should therefore disable all unused inputs in HW Config using the "Measurement type" parameter.

Redundant analog input modules with non-redundant encoder

With non-redundant encoders, analog input modules are used in a 1-out-of-2 configuration:

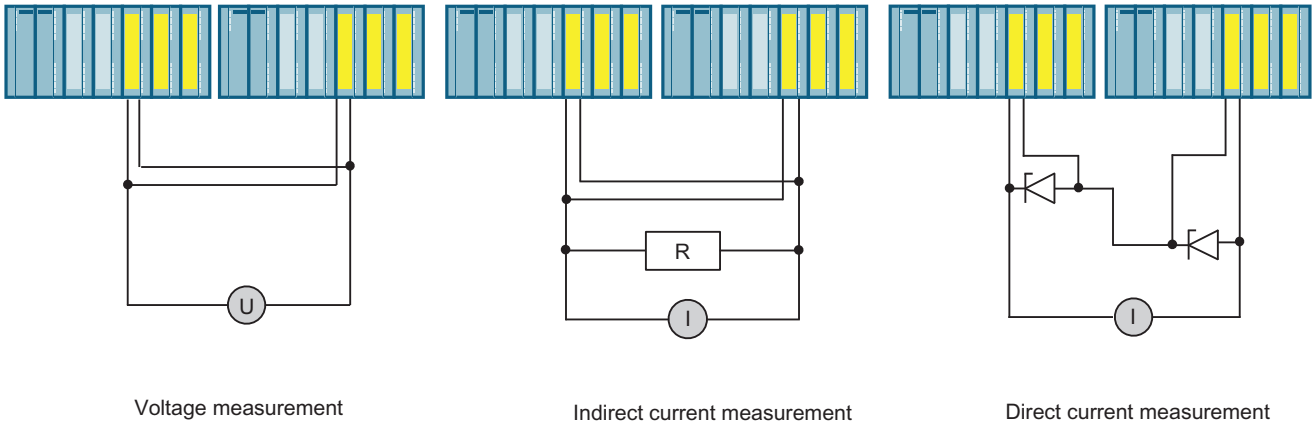


Figure 5-12 Fault-tolerant analog input modules in 1-out-of-2 configuration with one encoder

Remember the following when connecting an encoder to multiple analog input modules:

- Connect the analog input modules in parallel for voltage sensors (left in figure).
- You can convert a current into voltage using an external load to be able to use voltage analog input modules connected in parallel (center in the figure).
- 2-wire transmitters are powered externally to allow you to repair the module online.

The redundancy of the fail-safe analog input modules enhances their availability.

Redundant analog input modules for indirect current measurement

The following applies to the wiring of analog input modules:

- Suitable encoders for this circuit are active transmitters with voltage output and thermocouples.
- The "wire break" diagnostics function in HW Config must not be enabled either the modules are operated with transmitters or when thermocouples are connected.
- Suitable encoder types: active 4-wire and passive 2-wire transmitters with output ranges +/-20 mA, 0 to 20 mA, and 4 to 20 mA. 2-wire transmitters are powered by an external auxiliary voltage.
- Criteria for the selection of resistance and input voltage range are the measurement accuracy, number format, maximum resolution and possible diagnostics.
- In addition to the options listed, other input resistance and voltage combinations according to Ohm's law are also possible. However, note that the number format, diagnostic capability and resolution may then be lost. The measurement error also depends largely on the size of the measure resistance of certain modules.
- Use a measure resistance with a tolerance of +/- 0.1% and TC 15 ppm.

Additional conditions for specific modules

AI 8x12 bit 6ES7 331-7K..02-0AB0

- Use a 50 ohm or 250 ohm resistor to map the current on a voltage:

Resistor	50 ohms	250 ohms	
Current measuring range	+/-20 mA	+/-20 mA *)	4...20 mA
Input range to be assigned	+/-1 V	+/-5 V	1...5 V
Measuring range cube position	"A"	"B"	
Resolution	12 bits + sign	12 bits + sign	12 bits
S7 number format	x	x	
Circuit-specific measuring error - 2 parallel inputs - 1 input	- -	0.5% 0.25%	
"Wire break" diagnostics	-	-	x *)
Load for 4-wire transmitters	50 ohms	250 ohms	
Input voltage for 2-wire transmitters	> 1.2 V	> 6 V	
*) The AI 8x12bit outputs diagnostic interrupt and measured value "7FFF" in the event of wire break.			

The listed measuring error results solely from the interconnection of one or two voltage inputs with a measure resistance. Allowance has neither been made here for the tolerance nor for the basic/operational limits of the modules.

The measuring error for one or two inputs shows the difference in the measurement result depending on whether two inputs or, in case of error, only one input acquires the current of the transmitter.

AI 8x16 bit 6ES7 331-7NF00-0AB0

- Use a 250 ohm resistor to map the current on a voltage:

Resistor	250 ohms *)	
Current measuring range	+/-20 mA	4...20 mA
Input range to be assigned	+/-5 V	1...5 V
Resolution	15 bits + sign	15 bits
S7 number format	x	
Circuit-specific measuring error - 2 parallel inputs - 1 input	- -	
"Wire break" diagnostics	-	x
Load for 4-wire transmitters	250 ohms	
Input voltage for 2-wire transmitters	> 6 V	
*) It may be possible to use the freely connectible internal module 250 ohm resistors		

Redundant analog input modules for direct current measurement

The following applies to the wiring of analog input modules:

- Suitable encoder types: active 4-wire and passive 2-wire transmitters with output ranges +/-20 mA, 0 to 20 mA, and 4 to 20 mA. 2-wire transmitters are powered by an external auxiliary voltage.
- The "wire break" diagnostics function supports only the 4...20 mA input range. All other unipolar or bipolar ranges are excluded in this case.
- Suitable diodes include the types of the BZX85 or 1N47..A series (1.3 W Zener diodes) with the voltages specified for the modules. When selecting other elements, make sure that the reverse current is as low as possible.
- A fundamental measuring error of max. 1 µA results from this type of circuit and the specified diodes due to the reverse current. In the 20 mA range and at a resolution of 16 bits, this value leads to an error of < 2 bits. Individual analog inputs in the circuit above lead to an additional error, which may be listed in the constraints. The errors specified in the manual must be added to these errors for all modules.
- The 4-wire transmitters used must be capable of driving the load resulting from the circuit above. You will find details in the technical specifications of the individual modules.
- When connecting 2-wire transmitters, please note that the Zener diode circuit weighs heavily in the power budget of the transmitter. The required input voltages are therefore included in the technical specifications of the individual modules. Together with the inherent supply specified on the transmitter data sheet, the minimum supply voltage is calculated to $L+ > U_{e-2w} + U_{IS-TR}$

Redundant analog input modules with redundant encoders

With double-redundant encoders, it is better to use fail-safe analog input modules in a 1-out-of-2 configuration:

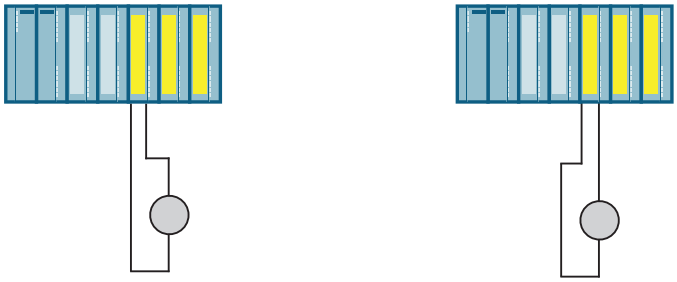


Figure 5-13 Fault-tolerant analog input modules in 1-out-of-2 configuration with two encoders

The use of redundant encoders also increases their availability.

A discrepancy analysis also detects external errors, except for the failure of a non-redundant load voltage supply.

The general comments made at the beginning of this documentation apply.

Redundant analog output modules

You implement fault-tolerant control of a final controlling element by wiring two outputs of two analog output modules in parallel (1-out-of-2 configuration)

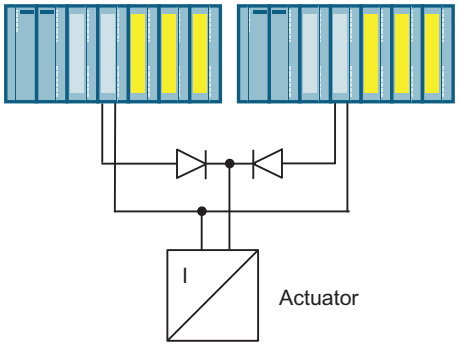


Figure 5-14 Fault-tolerant analog output modules in 1-out-of-2 configuration

The following applies to the wiring of analog output modules:

- Wire the ground connections in a star structure to avoid output errors (limited common-mode suppression of the analog output module).

Analog output signals

Only analog output modules with current outputs (0 to 20 mA, 4 to 20 mA) can be operated redundantly.

The output value is divided by 2, and each of the two modules outputs half. If one of the modules fails, the failure is detected and the remaining module outputs the full value. As a result, the surge at the output module in the event of an error is not as high.

Note

The output value drops briefly to half, and after the reaction in the program it is returned to the proper value. The duration of the output value drop is determined by the following time intervals:

- Time interval between the initial occurrence of an interrupt and the interrupt report reaching the CPU.
- Time interval until the next RED_OUT (FB 451) call.
- Time interval until the intact analog output module has doubled the output value.

In the case of passivation or a CPU STOP, redundant analog outputs output an assignable minimum current of approximately 120-1000 µA per module (or 240-1000 µA for HART analog output modules), i.e., a total of approximately 240-2000 µA (or 480-2000 µA for HART analog output modules). Considering the tolerance, this means that the output value is always positive.

A configured substitute value of 0 mA will produce at least these output values. In a redundant configuration of analog outputs, the substitute value of the current outputs is automatically set permanently to "zero current and zero voltage". You can also specify a configurable compensation current of 0-400 µA for an output range of 4-20 mA.

This means you have the option of matching the minimum/compensation current to the connected I/O.

To minimize the error of the total current at the summing point in case of one-sided passivation, the assigned compensation current is subtracted in this case from the current of the depassivated (i.e., active) channel with a pre-set value of 4 mA (range +-20 µA).

Note

If both channels of a channel pair were passivated (e.g., by OB 85), the respective half of the current value is still output to both storage locations in the process image of outputs. If one channel is depassivated, then the full value is output on the available channel. If this is not required, a substitute value must be written to the lower channels of both modules prior to executing FB 451 "RED_OUT".

Depassivation of modules

Passivated modules are depassivated by the following events:

- When the fault-tolerant system starts up
- When the fault-tolerant system switched to "redundant" mode
- After system modifications during operation
- If you call FC 451 "RED_DEPA" and at least one redundant channel or module is passivated.

The depassivation is executed in FB 450 "RED IN" after one of these events has occurred. Completion of the depassivation of all modules is logged in the diagnostics buffer.

Note

When a redundant module is assigned a process image partition and the corresponding OB is not available on the CPU, the complete passivation process may take approximately 1 minute.

5.5.3 Evaluating the passivation status

Procedure

First, determine the passivation status by evaluating the status byte in the status/control word "FB_RED_IN.STATUS_CONTROL_W". If you see that one or more modules have been passivated, determine the status of the respective module pairs in MODUL_STATUS_WORD.

Evaluating the passivation status using the status byte

The status word "FB_RED_IN.STATUS_CONTROL_W" is located in the instance DB of FB 450 "RED_IN". The status byte returns information on the status of the redundant I/Os. The assignment of the status byte is described in the online help for the respective block library.

Evaluating the passivation status of individual module pairs by means of MODUL_STATUS_WORD

MODUL_STATUS_WORD is an output parameter of FB 453 and can be interconnected accordingly. It returns information on the status of individual module pairs.

The assignment of the MODUL_STATUS_WORD status byte is described in the online help for the respective function block library.

System and operating states of the CPU 410SIS 6

6.1 Operating states of the CPU 410SIS

6.1.1 RUN mode

Reaction of the CPU

If there is no startup problem or error and the CPU was able to switch to RUN, the CPU either executes the user program or remains idle. The I/O can be accessed.

- You can read out programs from the CPU with the ES (CPU -> ES).
- You can transfer programs from the ES to the CPU (ES -> CPU).

The user program is executed by at least one CPU in the following system states:

- Stand-alone operation
- Single mode
- Link-up, update
- Redundant

Single mode, link-up, update

In the system states solo mode, link-up and update, the master CPU is in RUN and executes the user program in stand-alone mode.

Redundant system mode

The master CPU and standby CPU are always in RUN when operating in the redundant system state. Both CPUs execute the user program in synchronism, and perform mutual checks.

In redundant system mode it is not possible to test the user program with breakpoints.

The redundant system state is only supported if the two CPUs have the same version and firmware version. Redundancy will be lost if one of the errors listed in the following table occurs.

Table 6-1 Causes of error leading to redundancy loss

Cause of error	Reaction
Failure of one CPU	Replacement of a CPU during redundant operation (Page 165)
Failure of the redundant link (synchronization module or fiber-optic cable)	Replacement of synchronization module or fiber-optic cable (Page 168)
RAM comparison error	ERROR-SEARCH mode (Page 74)

Redundant use of modules

Redundantly used module pairs must be identical, i.e. the two modules that are redundant to each other must have the same article number and the same product version/firmware version.

6.1.2 STOP mode

Reaction of the CPU

The CPU does not execute the user program. The output modules output 0 or - if configured - a substitute value. The signals of the input modules are set to 0.

- You can read out programs from the CPU with the ES (CPU -> ES).
- You can transfer programs from the ES to the CPU (ES -> CPU).

Special features in redundant mode

When you download a configuration to one of the CPUs while both are in STOP operating state, observe the points below:

- Start the CPU to which you downloaded the configuration first in order to set it up for master mode.
- If the system start is requested by the ES, the CPU with the active connection is started first, regardless of its master or reserve status. Then the second CPU starts up and will become the standby CPU after link-up and update operations.

Note

A system startup may trigger a master–standby changeover.

A CPU 410SIS can only exit STOP state with a downloaded configuration.

Memory reset

The memory reset function affects only the selected CPU. To reset both CPUs, you must reset one and then the other.

6.1.3 STARTUP mode

Startup types

The CPU 410SIS distinguishes between two startup types: cold restart and warm restart.

Cold restart

- During a cold restart, all data (process image, bit memory, timers, counters and data blocks) is reset to the start values stored in the program (load memory), regardless of whether it was configured as retentive or non-retentive data.
- The associated startup OB is OB 102
- Program execution is restarted from the beginning (OB 102 or OB 1).

Warm restart

- A warm restart resets the process image and the bit memories, timers, and counters. All data blocks assigned the "Non Retain" attribute are reset to the start values from the load memory.
  The other data blocks retain their last valid value if buffering is active. If there is no buffering, the values are reset to the start values from the load memory after power off/on.
- The associated startup OB is OB 100
- Program execution is restarted from the beginning (OB 100 or OB 1).

Special features in redundant mode

The special features described below apply to startup when you operate two CPUs redundantly.

Startup processing by the master CPU

In redundant operation, the startup system state is handled exclusively by the master CPU

During STARTUP, the master CPU compares the existing I/O configuration with the hardware configuration that you created in STEP 7. If these are different, the system can only be started up if "Startup when expected/actual configurations differ" was configured.

The master CPU checks and assigns parameters for the switched I/O.

Startup of the standby CPU

The standby CPU startup routine does not call an OB 100 or OB 102.

Additional information

For detailed information on STARTUP operating state, refer to Manual *Programming with STEP 7*.

6.1.4 HOLD mode

The HOLD mode is for test purposes. You need to have set respective breakpoints in the user program for this purpose. It can only be reached from the RUN mode.

Special features in redundant mode

A transition to HOLD is only available during STARTUP and in RUN in single mode. It is not possible to set breakpoints when the fault-tolerant system is in redundant system mode. Link-up and update operations are not available while the CPU is in HOLD mode; the standby CPU remains in STOP which is logged in the diagnostics buffer.

6.1.5 LINK-UP and UPDATE modes

The master CPU checks and updates the memory content of the standby CPU before the fault-tolerant system assumes redundant system mode. This is implemented in two successive phases: link-up and update.

The master CPU is always in RUN mode and the reserve CPU is in LINK-UP or UPDATE mode during the link-up and update phases.

In addition to the link-up and update functions, which are carried out to establish redundant system mode, the system also supports linking and updating in combination with master/ reserve changeover.

For detailed information on connect and updating, refer to section Link-up and update (Page 89).

6.1.6 ERROR-SEARCH mode

The purpose of ERROR-SEARCH operating state is to find a faulty CPU. The standby CPU runs the entire self-test; the master CPU remains in RUN. If a hardware fault is detected, the CPU switches to DEFECTIVE mode. If no fault is detected the CPU is linked up again. The fault-tolerant system switches back to the redundant system state.

No communication, for example through PG access, is possible with the CPU in TROUBLESHOOTING mode. The ERROR-SEARCH operating state is indicated by the flashing RUN and STOP LEDs, see Chapter Status and error displays (Page 29).

Note

If the master CPU changes to STOP during troubleshooting, the troubleshooting is continued on the standby CPU. However, once troubleshooting is completed, the standby CPU does not start up again.

The following events will trigger the ERROR-SEARCH operating state:

1. If there is a one-sided call of OB 121 in redundant operation (at only one CPU), a hardware fault is assumed and that CPU switches to TROUBLESHOOTING mode. The other CPU becomes master, if necessary, and continues running in solo operation.
2. If a checksum error occurs on only one CPU in redundant operation, that CPU switches to ERROR-SEARCH operating state. The other CPU becomes master, if necessary, and continues running in solo operation.

3. If a RAM/PAA comparison error occurs in redundant operation, the backup CPU switches to TROUBLESHOOTING mode (default response) and the master CPU continues running in solo mode.
   A different response to a RAM/PAA comparison error can be configured (for example backup CPU switches to STOP).
4. If a multiple-bit error occurs on a CPU in redundant operation, that CPU will switch to ERROR-SEARCH operating state. The other CPU becomes master, if necessary, and continues running in solo operation.
   But: OB 84 is called if 2 or more single-bit errors occur on a CPU in redundant operation within 6 months. The CPU does not change to ERROR-SEARCH operating state.
5. If synchronization is lost during redundant operation, the standby CPU changes to ERROR-SEARCH operating state. The other CPU remains master and continues running in solo operation.

You can find additional information on the self-test in Self-test (Page 84).

6.1.7 DEFECTIVE state

CPU response following reboot

The CPU operating system tries to switch back to RUN by rebooting the CPU.

The CPU responds as follows to a reboot:

1. The CPU writes the cause of the error to the diagnostics buffer.
2. The CPU generates the current service data.
3. The CPU checks if a reboot is possible.
   A reboot is not possible in the following cases:
   - There is an inconsistency in the user data.
   - A reboot has already been carried out within the previous 24 hours.
   - The event that led to the defect is preventing an automatic reboot.
4. The CPU records the automatic reboot in the diagnostics buffers (event W#16#4309 "Memory reset launched automatically" or W#16#452B "CPU REBOOT for clearing data inconsistency")
5. The CPU runs internal tests.
6. In a redundant system, the standby CPU links up to the master in operation.
7. In stand-alone operation and solo mode, the CPU load the backed up user program and executes a warm restart

Transition to the DEFECTIVE state

If an error has occurred that cannot be automatically cleared by the operating system, the CPU switches to the DEFECTIVE state and all LEDs flash.

The CPU switches to the DEFECTIVE state in the following cases:

- The user data is inconsistent.
- A reboot has already been carried out within the previous 24 hours.
- The event that caused this error prevents automatic reboot.

6.2 System states of the redundant CPU 410SIS

6.2.1 Introduction

The S7-400H consists of two redundantly configured subsystems that are synchronized via fiber-optic cables.

The two subsystems form a fault-tolerant automation system that operates with a dual-channel (1-out-of-2) structure based on the "active redundancy" principle.

What does active redundancy mean?

Active redundancy means that all redundant resources are constantly in operation and simultaneously involved in the execution of the control task.

For the S7-400H, this means that the user programs in both CPUs are identical and executed synchronously by the two CPUs.

Convention

To identify the two subsystems, we use the traditional expressions of "master" and "standby" for dual-channel fault-tolerant systems in this description. However, the standby runs event-synchronized with the master at all times and not just when an error occurs.

The differentiation between the master and standby CPUs is primarily important for ensuring reproducible fault responses. The standby goes into troubleshooting mode when RAM/PIQ errors are detected, for example, while the master CPU remains in RUN.

Master-standby assignment

When the S7-400H is first switched on, the CPU that started up first becomes the master CPU, and the other CPU becomes the standby CPU.

The preset master-standby assignment is retained when both CPUs power up simultaneously.

The master-standby assignment changes when:

1. The standby CPU starts up before the master CPU (interval of at least 3 s)
2. The master CPU fails or switches to STOP in the redundant system state
3. No error was found in ERROR-SEARCH operating state (see Chapter ERROR-SEARCH mode (Page 74))
4. Programmed master-standby switchover with SFC 90 "H_CTRL"

5. The sequence of a system modification during operation
6. A firmware update in RUN mode
7. Switch to CPU with modified configuration
8. Switching to a CPU with modified operating system
9. Switching to a CPU using only one intact redundant link

Synchronizing the subsystems

The master and standby CPUs are linked by fiber-optic cables. Both CPUs maintain event-synchronous program execution via this connection.

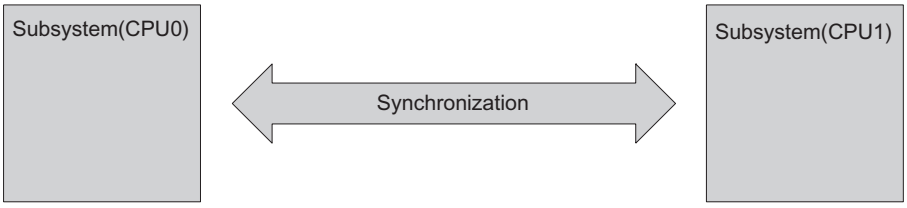


Figure 6-1 Synchronizing the subsystems

Synchronization is performed automatically by the operating system and has no effect on the user program.

Event-driven synchronization procedure

The "event-driven synchronization" procedure patented by Siemens was used for the S7-400H.

Event-driven synchronization means that the master and standby always synchronize their data when an event occurs which may lead to different internal states of the subsystems.

Such events include, for example, alarms or changes of data through communication functions.

Continued bumpless operation even if redundancy of a CPU is lost

Event-driven synchronization ensures bumpless continuation of operation by the standby CPU even if the master CPU fails. The inputs and outputs do not lose their values during the master-standby switchover.

Self-test

Malfunctions or errors must be detected, localized and reported as quickly as possible. Extensive self-test functions have therefore been implemented in the S7-400H that run automatically and entirely in the background.

The following components and functions are tested:

- Coupling of the central controllers
- Processor

- Internal memory of the CPU
- I/O bus

If the self-test detects an error, the fault-tolerant system tries to eliminate it or to suppress its effects.

A description of the self-test is available in Chapter Self-test (Page 84).

System operation without STOP

To best meet the demands of the process industry for system operation without STOP, SIMATIC SIS compact prevents possible STOP causes as much as possible. The CPU 410SIS was enhanced such that it, as a redundant system, always automatically achieves RUN redundant operating if possible. A change of the operating state is only possible through an engineering system command. RUN mode is always indicated in the diagnostic information.

6.2.2 The system states of the AS 410H SIS

The system states of the AS 410H SIS result from the operating states of the two CPUs. The term "system state" is used as a simplified term which identifies the concurrent operating states of the two CPUs.

Example: Instead of "the master CPU is in RUN and the standby CPU is in LINK-UP mode", we use "AS 410H SIS" is in the "link-up" system state.

Overview of system states

The following table shows the possible system states of the AS 410H SIS.

Table 6-2 System states of AS 410H SIS

System states of AS 410H SIS	Operating states of the two CPUs	
	Master	Standby
STOP	STOP	STOP, power off, DEFECTIVE
STARTUP	STARTUP	STOP, power off, DEFECTIVE, no synchronization
Single mode	RUN	STOP, ERROR-SEARCH, power off, DEFECTIVE, no synchronization
Link-up	RUN	STARTUP, LINK-UP
Update	RUN	UPDATE
Redundant	RUN	RUN
HOLD	HOLD	STOP, ERROR-SEARCH, power off, DEFECTIVE, no synchronization

6.2.3 Displaying and changing the system state of a fault-tolerant system

Procedure:

1. Select a CPU in SIMATIC Manager.
2. Select the menu command PLC > Diagnostics/Setting >Operating state.

Note

STOP is only possible with authorization in projects with password protection.

Result:

The "Operating state" dialog box shows the current system state of the fault-tolerant system and the operating states of the individual central processing units.

The CPU that was selected in SIMATIC Manager when the menu command was executed is the first one displayed in the table.

Changing the system state:

The options of changing the system state depend on the current system state of the fault-tolerant system.

6.2.4 System status change from the STOP system state

Requirement

You have selected one of the two CPUs in SIMATIC Manager and opened the "Operating state" dialog box with the menu command "PLC > Diagnostics/Setting > Operating mode".

Changing to redundant system mode (starting the fault-tolerant system)

1. Select the fault-tolerant system in the table.
2. Select the Restart button (warm restart).

Result:

The CPU displayed first in the table starts up as master CPU. Then the second CPU starts up and will become the standby CPU after link-up and update operations.

Changing to standalone mode (starting only one CPU)

1. In the table, select the CPU you want to start up.
2. Select the Restart button (warm restart).

6.2.5 System status change from the standalone mode system status

Requirements:

- For CPU access protection with password: You have entered the CPU access password with the menu command PLC > Access Rights > Setup in SIMATIC Manager.
- You have opened the "Operating state" dialog box using the PLC > Diagnostics/Setting > Operating state menu command in SIMATIC Manager.
- The standby CPU is not in ERROR-SEARCH operating state.

Changing to redundant system state (starting the standby CPU)

1. In the table, select the CPU that is in STOP, or the fault-tolerant system.
2. Select the Restart button (warm restart).

Changing to system status STOP (stopping the running CPU)

1. In the table, select the CPU that is in RUN, or the fault-tolerant system.
2. Select the STOP button.

Note

Any set up access right is not canceled until you stop the SIMATIC Manager. You should reset the access right once again to prevent unauthorized access. You reset the access right in the SIMATIC Manager with the menu command PLC > Access Rights > Cancel.

6.2.6 System status change from the redundant system state

Requirement:

- For CPU access protection with password: You have entered the CPU access password with the menu command PLC > Access Rights > Setup in SIMATIC Manager.
- You have opened the "Operating state" dialog box using the PLC > Diagnostics/Setting > Operating state menu command in SIMATIC Manager.

Changing to STOP system state (stopping the fault-tolerant system)

1. Select the fault-tolerant system in the table.
2. Select the Stop button.

Result

Both CPUs switch to STOP.

Changing to standalone mode (stop of one CPU)

1. In the table, select the CPU that you want to stop.
2. Select the Stop button.

Result:

The selected CPU goes into the STOP state, while the other CPU remains in RUN state; the fault-tolerant system continues operating in standalone mode.

Note

Any set up access right is not canceled until you stop the SIMATIC Manager. You should reset the access right once again to prevent unauthorized access. You reset the access right in the SIMATIC Manager with the menu command PLC > Access Rights > Cancel.

6.2.7 System diagnostics of a fault-tolerant system

The diagnose hardware function identifies the state of the entire fault-tolerant system.

Procedure:

1. Select the desired AS 410H SIS in the SIMATIC Manager.
2. Select the menu command PLC > Diagnostics/Setting >Diagnose hardware.
3. In the "Select CPU" dialog, select the CPU and confirm with OK.

Result:

The operating state of the selected CPU can be identified based on the display of the selected CPU in the "Diagnose hardware" dialog:

CPU icon	Operating state of the respective CPU
	Master CPU is in RUN operating state
	Standby CPU is in RUN operating state
	Master CPU is in STOP operating state
	Standby CPU is in STOP operating state
	Master CPU is in STARTUP operating state
	Master CPU or a module whose parameters it assigned is faulty.
	Standby CPU or a module whose parameters it assigned is faulty
	Maintenance required on master CPU
	Maintenance required on standby CPU

CPU icon	Operating state of the respective CPU
	Maintenance request on master CPU
	Maintenance request on standby CPU

Note

The view is not updated automatically in the Online view. Use the F5 function key to view the current operating state.

6.3 Self-test

Processing the self-test

The CPU executes the complete self-test program after an unbuffered POWER ON, e.g., POWER ON after initial insertion of the CPU or POWER ON without backup battery, and in the ERROR-SEARCH operating state.

The duration of the self-test is approximately 7 minutes.

In a fault-tolerant system, if the CPU calls for a memory reset and a buffered Power Off/On is then carried out, the CPU performs a self-test even though it was buffered.

In RUN the operating system splits the self-test routine into several small program sections ("test slices") which are processed in multiple successive cycles. The cyclic self-test is organized to perform a single, complete pass in a certain time. This time interval is at least 90 minutes and can be extended in the configuration to reduce the impact of the self-test on the runtime of the user program. However, it also extends the time interval in which a possible error is detected.

Response to errors during the self-test

If the self-test returns an error, the following happens:

Table 6-3 Response to errors during the self-test

Type of error	System response
Hardware fault	The faulty CPU switches to DEFECTIVE state. Fault-tolerant system switches to stand-alone operation. The cause of the error is written to the diagnostics buffer.
Hardware fault, which is signaled via a one-sided OB 121 call	The CPU with the one-sided OB 121 switches to ERROR-SEARCH. Fault-tolerant system switches to stand-alone operation (see below).
RAM/PIQ comparison error	The cause of the error is written to the diagnostics buffer. The configured system or operating state is assumed (see below).
Checksum errors	The response depends on the error situation (see below).
Multiple-bit errors	The faulty CPU switches to ERROR-SEARCH operating state.

Hardware fault with one-sided OB 121 call

If a hardware fault occurs that triggers a one-sided OB 121 call and this fault occurs for the first time since the last unbuffered POWER ON, the faulty CPU switches to ERROR SEARCH operating state. The fault-tolerant system switches to stand-alone operation. The cause of the error is written to the diagnostics buffer.

RAM/PIQ comparison error

If the self-test detects a RAM/PIQ comparison error, the fault-tolerant system exits redundant operating state and the standby CPU switches to ERROR SEARCH operating state (default setting). The cause of the error is written to the diagnostics buffer.

The response to a recurring RAM/PIQ comparison error depends on whether the error recurs in the first self-test cycle after troubleshooting or not until later.

Table 6-4 Response to a recurring comparison error

Comparison error recurs ...	Reaction
in the first self-test cycle after troubleshooting	Fault-tolerant system switches to stand-alone operation. Standby CPU switches to ERROR SEARCH and then remains in STOP.
after two or more self-test cycles after troubleshooting	Fault-tolerant system switches to stand-alone operation. Standby CPU switches to ERROR SEARCH.

Checksum errors

When a checksum error occurs for the first time since the last POWER ON without battery backup, the system reacts as follows:

Table 6-5 Reaction to checksum errors

Time of detection	System response
During the startup test after POWER ON	The faulty CPU switches to DEFECTIVE state. Fault-tolerant system remains in stand-alone operation.
In the cyclic self-test (STOP or solo operation)	The error is corrected. The CPU remains in STOP operating state or in solo operation.
In the cyclic self-test (redundant system state)	The error is corrected. The faulty CPU switches to ERROR-SEARCH operating state. Fault-tolerant system switches to stand-alone operation.
In the ERROR-SEARCH operating state	The faulty CPU switches to DEFECTIVE state.

The cause of the error is written to the diagnostics buffer.

In an F-system, the F-program is already signaled at the first occurrence of a checksum error in STOP operating state or in stand-alone operation that the self-test has detected an error.

Hardware fault with one-sided OB 121 call, checksum error, 2nd occurrence

The response of a CPU 410SIS to the second occurrence of hardware faults with one-sided OB 121 call and checksum errors is as shown in the following table for the various operating modes of a CPU 410SIS.

Table 6-6 Hardware fault with one-sided OB 121 call, checksum error, 2nd occurrence

Error	CPU in stand-alone operation/single mode	CPU in redundant operation
Hardware fault with one-sided OB 121 call	OB 121 is executed	The faulty CPU switches to ERROR-SEARCH operating state. The fault-tolerant system switches to stand-alone operation.
Checksum error	The CPU enters the DEFECTIVE state if two errors occur within two successive test cycles (You configure the length of the test cycle in HW Config)	The CPU enters the DEFECTIVE state if a second error triggered by the first error event occurs in ERROR-SEARCH mode.

If a second checksum error occurs in solo or stand-alone operation after twice the test cycle time has expired, the CPU reacts as it did on the first occurrence of the error. If a second error (hardware fault with one-sided OB 121 call, checksum error) occurs in redundant operation after expiration of the troubleshooting operation, the CPU responds the same as to the first occurrence of the error.

Multiple-bit errors

If a multiple-bit error is detected during redundant operation of a fault-tolerant system, the CPU switches to ERROR-SEARCH operating state. When troubleshooting is finished, the CPU can be linked up and updated again, and resume redundant operation. If there is no error on the CPU 410SIS, it switches to RUN and becomes the master. The cause of the error is signaled by the call of OB 84.

There are some rare cases in which multiple-bit and single-bit errors can occur due to very challenging ambient conditions. If they occur only once, they do not interfere with the hardware. If bit errors occur frequently, however, replace the hardware.

Single-bit errors

Single-bit errors are also detected and eliminated outside the self-test. After elimination of the error, the CPU 410SIS calls OB 84.

Influencing the cyclic self-test

SFC 90 "H_CTRL" allows you to influence the scope and execution of the cyclic self-test. For example, you can remove various test components from the overall test and re-introduce them. In addition, you can explicitly call and process specific test components.

For detailed information on SFC 90 "H_CTRL", refer to Manual *System Software for S7-300/400, System and Standard Functions*.

Note

In a fail-safe system, you are not allowed to disable and then re-enable the cyclic self-tests.

6.4 Performing a memory reset

Memory reset process in the CPU

You can perform a memory reset of the CPU from the ES. During a memory reset, the following process occurs on the CPU:

- The CPU deletes the entire user program in the main memory.
- The CPU deletes the user program from the load memory.
- The CPU deletes all counters, bit memories, and timers, but not the time of day.
- The CPU tests its hardware.
- The CPU sets its parameters to default settings.

The LEDs behave as following during the memory reset:

1. The STOP LED flashes for about 1-2 seconds at 2 Hz.
2. All LEDs light up for approximately 10 seconds.
3. The STOP LED flashes for approximately 30 seconds at 2 Hz.
4. The RUN LED and the STOP LED flash for approximately 2 seconds at 0.5 Hz.
   This operation can also take a few seconds longer depending on the utilization level of the memory.
5. The RUN LED and the STOP LED flash for approximately 2 seconds at 0.5 Hz.
   If a large data volume is being deleted, the LEDs may flash longer.
6. The STOP LED lights up permanently.

Data retained after a memory reset...

The following values are retained after a memory reset:

- The content of the diagnostic buffer
- The baud rate of the DP interface
- The parameters of the PN interfaces
  - Name (NameOfStation)
  - IP address of CPU
  - Subnet mask
  - Static SNMP parameters
- The time of day
- The status and value of the operating hours counter

Link-up and update

7

7.1 Effects of link-up and updating

The link-up and update operations are indicated by the REDF LED on both CPUs. During link-up, the LEDs flash at a frequency of 0.5 Hz, and when updating at a frequency of 2 Hz.

Link-up and update have various effects on user program execution and on communication functions.

Table 7-1 Properties of link-up and update functions

Process	Link-up	Update
Execution of the user program	All priority classes (OBs) are processed.	Processing of the priority classes is delayed section by section. All requests are caught up with after the update. For details, refer to the sections below.
Deleting, loading, generating, and compressing of blocks	Blocks cannot be deleted, loaded, created or compressed. When such actions are busy, link-up and update operations are inhibited.	Blocks cannot be deleted, loaded, created or compressed.
Execution of communication functions, ES operation	Communication functions are executed.	Execution of the functions is restricted section by section and delayed. All the delayed functions are caught up with after the update. For details, refer to the sections below.
CPU self-test	Not performed	Not performed
Testing and commissioning functions, such as "Monitor/ modify tag", "Monitor (on/ off)".	No testing and commissioning functions are possible. When such actions are busy, link-up and update operations are inhibited.	No testing and commissioning functions are possible.
Handling of connections on the master CPU	All connections are retained; no new connections can be made.	All connections are retained; no new connections can be made. Interrupted connections are not restored until the update is completed
Handling of connections on the reserve CPU	All the connections are cancelled; no new connections can be made.	All connections are already down. Cancellation takes place during link-up. Connections of the standby are not established until Redundant system state.

7.2 Link-up and update via an ES command

Which commands you can use on the programming device to initiate a link-up and update operation is determined by the current conditions on the master and standby CPU. The following table shows the possible PG commands for the link-up and update in various circumstances.

Table 7-2 PG commands for link-up and update

Link-up and update as PG command:	Firmware version on master and standby CPU	Available sync connections	Hardware version on master and standby CPU
Restart of the standby	Are identical	2	Are identical
Switching to a partner CPU with modified configuration	Are identical	2	Are identical
Switching to a partner CPU with modified operating system	Are different	2	Are identical
Switching to a partner CPU with modified hardware product version	Are identical	2	Are different
Switching to a partner CPU using only one intact redundant link	Are identical	1	Are identical

7.3 Time monitoring

Program execution is interrupted for a certain time during updating. This section is relevant to you if this period is critical in your process. If this is the case, configure one of the monitoring times described below.

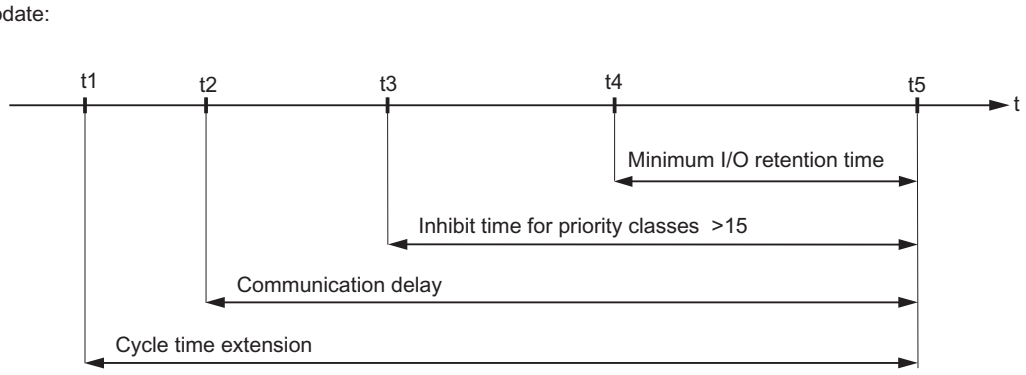
During updating, the fault-tolerant system monitors the cycle time extension, communication delay and inhibit time for priority classes > 15 in order to ensure that their configured maximum values are not exceeded, and that the configured minimum I/O retention time is maintained.

You made allowances for the technological requirements in your configuration of monitoring times.

The monitoring times are described in detail below.

- Maximum cycle time extension
  - Cycle time extension: The time during the update in which neither OB 1 nor any other OBs up to priority class 15 are executed. "Normal" cycle time monitoring is disabled within this time span.
  - Max. cycle time extension: The maximum permissible cycle time extension configured by the user.
- Maximum communication delay
  - Communication delay: The time span during the update during which no communication functions are processed. Note: The master CPU, however, maintains all existing communication links.
  - Maximum communication delay: The maximum permissible communication delay configured by the user.
- Maximum inhibit time for priority classes > 15
  - Inhibit time for priority classes > 15: The time span during an update during which no OBs (and thus no user program) are executed nor any I/O updates are implemented.
  - Maximum inhibit time for priority classes > 15: The maximum permissible inhibit time for priority classes > 15 configured by the user.
- Minimum I/O retention time:
  This represents the interval between copying of the outputs from the master CPU to the standby CPU, and the time of the master/standby changeover (time at which the previous master CPU goes into STOP and the new master CPU goes into RUN). Both CPUs control the outputs within this period, in order to prevent the I/O from going down when the system performs an update with master/standby changeover.
  The minimum I/O retention time is of particular importance when updating with master/standby changeover.

The following figure shows a summary of the relevant times during the update. These times expire when the system enters the redundant system mode or when there is a master/standby changeover, i.e. on the transition of the new master to RUN when the update is completed.



t1: End of current OBs up to priority class 15
t2: Stop all communication functions
t3: End of watchdog interrupt OB with special handling
t4: End of copying of outputs to the standby CPU
t5: Redundant system status, or master/standby changeover

Figure 7-1 Meanings of the times relevant for updates

Response to time-outs

If one of the times monitored exceeds the configured maximum value, the following procedure is started:

1. Cancel update
2. Fault-tolerant system remains in standalone mode, with the previous master CPU in RUN
3. Cause of cancelation is entered in diagnostic buffer
4. Call OB 72 (with corresponding start information)

The standby CPU then reevaluates its system data blocks.
Following this, after at least one minute, the CPU tries again to perform the link-up and update. If still unsuccessful after a total of 10 retries, the CPU abandons the attempt. You yourself will then need to start the link-up and update again.

A monitoring timeout can be caused by:

- High interrupt load (e.g. from I/O modules)
- High communication load causing prolonged execution times for active functions
- In the final update phase, the system needs to copy unusually large amounts of data to the standby CPU.

7.3.1 Time response

Time response during link-up

The influence of link-up operations on your plant's control system should be kept to an absolute minimum. The current load on your automation system is therefore a decisive factor in the increase of link-up times. The time required for link-up is in particular determined by

- the communication load
- the cycle time

Link-up takes about 2 minutes for automation systems without load.

It can take more than one hour when there is a high load on your automation system.

Time response during updating

The transmission time during updating depends on the current changes of the process values and the communication load.

As a simple approximation, we can interpret the maximum inhibit time to be configured for priority classes > 15 as a function of the data volume in the work memory. The volume of code in the work memory is irrelevant.

7.3.2 Determining the monitoring times

Calculation using STEP 7 or formulas

STEP 7 automatically calculates the monitoring times listed below for each new configuration. You can also calculate these times using the formulas and procedures described below. They are equivalent to the formulas provided in STEP 7.

- Maximum cycle time extension
- Maximum communication delay
- Maximum inhibit time for priority classes
- Minimum I/O retention time

The automatic calculation of the monitoring times can also be triggered in HW Config under CPU Properties -> H Parameters

Monitoring time accuracy

Note

The monitoring times determined by STEP 7 or by using formulas merely represent recommended values.

These times are based on a fault-tolerant system with two communication peers and an average communication load.

Your system profile may differ considerably from those scenarios, therefore the following rules must be observed.

- A high communication load can significantly increase cycle time.
- Any modification of the system in operation may lead to a significant increase in cycle times.
- Any increase in the number of programs executed in priority classes > 15 (in particular processing of communication blocks) increases the delay in communication and extends the cycle time.
- You can even undercut the calculated monitoring times in small plants with high-performance requirements.

Configuration of the monitoring times

When configuring monitoring times, always make allowances for the following dependencies; conformity is checked by STEP 7:

Maximum cycle time extension
> maximum communication delay
> (maximum inhibit time for priority classes > 15)
> minimum I/O retention time

If you have configured different monitoring times in the CPUs and perform a link-up and update operation with master/standby changeover, the system always applies the higher of the two values.

Calculating the minimum I/O retention time (T_{PH})

The following applies to the calculation of the minimum I/O retention time:

- With central I/O: T_{PH} = 30 ms
- For distributed I/O (PROFIBUS DP): $T_{PH} = 3 \times T_{TRmax}$
  Where T_{TRmax} = maximum target rotation time
  of all DP master systems of the fault-tolerant station

When using central and distributed I/O, the resultant minimum I/O retention time is:

$T_{PH} = MAX (30 ms, 3 \times T_{TRmax}, T_{wd_max})$

The following figure shows the correlation between the minimum I/O retention time and the maximum inhibit time for priority classes > 15.

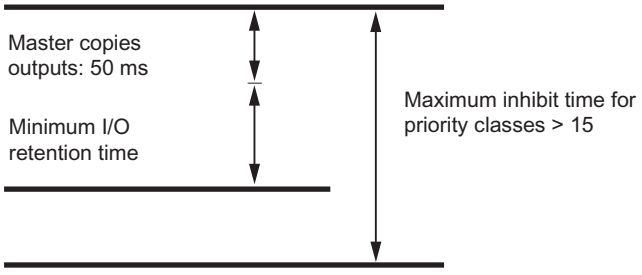


Figure 7-2 Correlation between the minimum I/O retention time and the maximum inhibit time for priority classes > 15

Note the following condition:

50 ms + minimum I/O retention time ≤
(maximum inhibit time for priority classes > 15)

It follows that a high minimum I/O retention time can determine the maximum inhibit time for priority classes > 15.

Calculating the maximum inhibit time for priority classes > 15 (T_{P15})

The maximum inhibit time for priority classes > 15 is determined by 4 main factors:

- As shown in Figure 12-2, all the contents of data blocks modified since last copied to the standby CPU are once again transferred to the standby CPU on completion of the update. **Number and structure of the data blocks**, which you describe in the high-priority priority classes, determine the duration of this operation and thus the maximum inhibit time for priority classes > 15. You receive a notice in the case of the remedies specified below.
- In the last phase of the update, all OBs are delayed or inhibited. To prevent the maximum inhibit time for priority classes > 15 from being extended unnecessarily due to unfavorable programming, you process the most time-critical I/O components in a **selected cyclic interrupt**. This is particularly relevant in fail-safe user programs. You can define this cyclic interrupt in your configuration. It is then executed again right after the start of the maximum inhibit time for priority classes > 15, provided you have assigned it a priority class > 15.

- In link-up and update operations with master/standby changeover (see section Link-up and update (Page 89)), you also need to changeover the active communication channel on the switched DP slaves on completion of the update. This operation prolongs the time within which valid values can neither be read nor output. How long this process takes is determined by your **hardware configuration**.
- The **technological conditions in your process** also decide how long an I/O update can be delayed. This is particularly important in time-monitored processes in fail-safe systems.

Note

For details, refer to Manual *S7-400F and S7-400FH Automation Systems* and Manual *S7-300 Automation Systems, Fail-safe Signal Modules*. This applies in particular to the internal execution times of fail-safe modules.

1. Based on the bus parameters in STEP 7, determine the following for the DP master system:
   - T_{TR} for the DP master system
   - DP changeover time (referred to below as T_{DP_UM})
2. Based on the technical specifications for the switched DP slaves, determine for the DP master system:
   - The maximum changeover time of the active communication channel (referred to below as T_{SLAVE_UM}).
3. Based on the technological specifications of your system, determine the following:
   - Maximum permissible time during which there is no update of your I/O modules (referred to below as T_{PTO}).
4. Based on your user program, determine the following:
   - Cycle time of the highest-priority or selected (see above) cyclic interrupt (T_{WA})
   - Execution time of your program in this cyclic interrupt (T_{PROG})
5. This results in the following for the DP master system:
   T_{P15} (DP master system) = T_{PTO} - (2 x T_{TR} + T_{WA} + T_{PROG} + T_{DP_UM} + T_{SLAVE_UM}) [1]

Note

For T_{P15}(DP master system) < 0, the calculation must be aborted here. Possible remedies are shown below the following example calculation. Make appropriate changes and then restart the calculation at 1.

6. Determine the share of the maximum inhibit time for I/O classes > 15 that is required by the minimum I/O retention time (T_{P15_OD}):
   T_{P15_OD} = 50 ms + min. I/O retention time [2]

Note

For T_{P15_OD} > T_{P15}, stop the calculation here. Possible remedies are shown below the following example calculation. Make appropriate changes and then restart the calculation at 1.

7. Using the information in Chapter Performance values for link-up and update (Page 100), calculate the share of the maximum inhibit time for priority classes > 15 that is required by the user program (T_{P15_AWP}).

Note

For $T_{P15_AWP} > T_{P15}$, stop the calculation here. Possible remedies are shown below the following example calculation. Make appropriate changes and then restart the calculation at 1.

8. The recommended value for the maximum inhibit time for priority classes > 15 is now obtained from:
$T_{P15} = MAX (T_{P15_AWP}, T_{P15_OD})$ [3]

Example of the calculation of T_{P15}

In the next steps, we take an existing system configuration and define the maximum permitted time span of an update, during which the operating system does not execute any programs or I/O updates.

A DP master system is connected to the CPU via the DP interface of the CPU.

1. Based on the bus parameters in STEP 7:
T_{TR_1} = 25 ms
T_{TR_2} = 30 ms
$T_{DP_UM_1}$ = 100 ms
$T_{DP_UM_2}$ = 80 ms
2. Based on the configuration in STEP 7:
T_{max_Akt} = 8 ms
T_{PN_UM} = 110 ms
3. Based on the technical data of the DP slaves used:
$T_{SLAVE_UM_1}$ = 30 ms
$T_{SLAVE_UM_2}$ = 50 ms
4. Based on the technological settings of your system:
T_{PTO_1} = 1250 ms
T_{PTO_2} = 1200 ms
T_{PTO_PN} = 1000 ms
5. Based on the user program:
T_{WA} = 300 ms
T_{PROG} = 50 ms
6. Based on the formula [1]:
T_{P15} (DP master system)
= 1250 ms - (2 x 25 ms + 300 ms + 50 ms + 100 ms + 30 ms) = 720 ms

Check: Since $T_{P15} > 0$, continue with

1. T_{P15} = 720 ms
2. Based on the formula [2]:

$T_{P15_OD} = 50 ms + T_{PH} = 50 ms + 90 ms = 140 ms$

Check: Because T_{P15_OD} = 140 ms < T_{P15_HW} = 720 ms, continue with

1. Based on section Performance values for link-up and update (Page 100) with 170 KB of user program data:
   T_{P15_AWP} = 194 ms

Check: Because T_{P15_AWP} = 194 ms < T_{P15} = 720 ms, continue with

1. Based on formula [3], we obtain the recommended max. inhibit time for priority classes > 15:

T_{P15} = MAX (194 ms, 140 ms)

T_{P15} = 194 ms

This means that by setting a maximum inhibit time of 194 ms for priority classes > 15 in STEP 7, you ensure that any signal changes during the update are detected with a signal duration of 1250 ms or 1200 ms.

Remedies if it is not possible to calculate T_{P15}

If no recommendation results from calculating the maximum inhibit time for priority classes > 15, you can remedy this by taking various measures:

- Reduce the cyclic interrupt cycle of the configured cyclic interrupt.
- Increase the baud rate of the DP master system.
- If you do not expect any significant load caused by interrupts or parameter assignments in a DP master system, you can also reduce the calculated T_{TR} times by around 20% to 30%. However, this increases the risk of a station failure in the distributed I/O.
- The time value T_{P15_AWP} represents a guideline and depends on your program structure. You can reduce it by taking the following measures, for example:
  - Save data that changes often in different DBs than data that does not change as often.
  - Specify a smaller DB sizes in the work memory.

If you reduce the time T_{P15_AWP} without taking the measures described, you run the risk that the update operation will be canceled due to a monitoring timeout.

Calculation of the maximum communication delay

Use the following formula:

Maximum communication delay =
4 x (maximum inhibit time for priority classes > 15)

Decisive factors for determining this time are the process status and the communication load in your system. This can be understood as the absolute load or as the load relative to the size of your user program. You may have to adjust this time.

Calculation of the maximum cycle time extension

Use the following formula:

Maximum cycle time extension =
10 x (maximum inhibit time for priority classes > 15)

Decisive factors for determining this time are the process status and the communication load in your system. This can be understood as the absolute load or as the load relative to the size of your user program. You may have to adjust this time.

7.3.3 Performance values for link-up and update

User program section T_{P15_AWP} of the max. inhibit time for priority classes > 15

You can calculate the user program section T_{P15_AWP} of the max. inhibit time for priority classes > 15 with the following formula:

T_{P15_AWP} in ms = 0.7 x size of the DBs in the work memory in KB + 75

The following table shows the resulting times for some typical values of the working memory data.

Table 7-3 Typical values for the user program section

Work memory data	T_{P15_AWP}
500 KB	220 ms
1 MB	400 ms
2 MB	0.8 s
4 MB	1.6 s

The following assumptions were made for this formula:

- 80% of the data blocks are still changed prior to the delay in the interrupts with priority classes > 15.
  This value must be determined more precisely for fail-safe systems to avoid a timeout of the driver blocks (see section Determining the monitoring times (Page 94)).
- For each MB of memory that is occupied by data blocks, there is still approx. 100 ms of update time for currently running or restarted communication functions.
  Depending on the communication load of your automation system, you need to add or subtract when setting T_{P15_AWP}.

7.3.4 Influences on time response

The period during which no I/O updates take place is primarily determined by the following influencing factors:

- The number and size of data blocks modified during the update
- The number of instances of SFBs in S7 communication and of SFBs for generating block-specific messages
- System modifications during operation
- Expansion of distributed I/Os with PROFIBUS DP (a lower baud rate and higher number of slaves increases the time it takes for I/O updates).

In the worst case, this period is extended by the following amounts:

- Maximum cyclic interrupt used
- Duration of all cyclic interrupt OBs
- Duration of high-priority interrupt OBs executed until the start of interrupt delays

7.4 Special features in link-up and update operations

Requirement for input signals during the update

Any process signals read previously are retained and not included in the update. The CPU only recognizes changes of process signals during the update if the changed signal state remains after the update is completed.

The CPU does not detect pulses (signal transitions "0 → 1 → 0" or "1 → 0 →1") which are generated during the update.

You should therefore ensure that the interval between two signal transitions (pulse period) is always greater than the required update period.

Communication links and functions

Connections on the master CPU are not be shut down. However, associated communication jobs are not executed during updates. They are queued for execution as soon as one of the following cases occurs:

- The update is completed, and the system is in the redundant state.
- The update and master/standby changeover are completed, the system is in solo operation.
- The update was canceled (e.g., due to timeout), and the system has returned to solo operation.

An initial call of communication blocks is not possible during the update.

Memory reset request on cancelation of link-up

If the link-up operation is canceled while the content of load memory is being copied from the master to the standby CPU, the standby CPU requests a memory reset. This indicated in the diagnostics buffer by event ID W#16#6523.

Special functions of the CPU 410SIS

8

8.1 Security functions of the CPU 410SIS

Automation system protection

The CPU 410SIS has various functions that can be used to protect your automation system.

- Signed firmware:
  The firmware of the CPU 410SIS is provided with a signature to detect manipulations on the CPU itself. If firmware with an incorrect signature is loaded, the CPU 410SIS rejects the firmware update.
- Protection level:
  A number of different protection levels regulate access to the CPU. See sectionSecurity levels (Page 104)
- SysLogEvents:
  Security-related changes to the CPU can be sent to one or more SIEM systems as SysLogEvent; see Security event logging (Page 106)
- Field Interface Security:
  If an interface of the CPU is only used for connecting field devices, access can be prevented at the interface for other devices; see section Field Interface Security (Page 108)
- Support of "Block Privacy":
  Blocks can be encrypted with a password using the STEP 7 "Block Privacy". The CPU 410SIS supports this function and can therefore process protected blocks; see section Access-protected blocks (Page 109)

Reference

You can find additional information about Industrial Security in the introduction in Security information (Page 11).

8.2 Security levels

You can define a protection level for your project in order to prevent unauthorized access to the CPU programs. The objective of these protection level settings is to grant a user access to specific programming device functions which are not protected by password, and to allow that user to execute those functions on the CPU.

Setting protection levels

You can set the CPU protection levels 1 to 3 in HW Config.

The following table shows the protection levels of a CPU.

Table 8-1 Protection levels of a CPU

CPU function	Protection level 1	Protection level 2	Protection level 3
Display of list of blocks	Access granted	Access granted	Access granted
Monitor variables	Access granted	Access granted	Access granted
Module status STACKS	Access granted	Access granted	Access granted
Operator control and monitoring functions	Access granted	Access granted	Access granted
S7 communication	Access granted	Access granted	Access granted
Read time of day	Access granted	Access granted	Access granted
Set time of day	Access granted	Access granted	Access granted
Block status	Access granted	Access granted	Password required
Load in PG	Access granted	Access granted	Password required
Controlling selection	Access granted	Password required	Password required
Modify variable	Access granted	Password required	Password required
Breakpoint	Access granted	Password required	Password required
Clear breakpoint	Access granted	Password required	Password required
Stop a CPU or the system	Access granted *	Password required	Password required
Load in CPU	Access granted *	Password required	Password required
Delete blocks	Access granted *	Password required	Password required
Compress memory	Access granted *	Password required	Password required
Memory reset	Access granted *	Password required	Password required
Firmware update	Access granted *	Password required	Password required

* A password is required if the program has a safety program.

Note

Any set up access right is not canceled until you stop the SIMATIC Manager. You should reset the access right once again to prevent unauthorized access. You reset the access right in the SIMATIC Manager with the menu command PLC > Access Rights > Cancel.

Setting the protection level with SFC 109 "PROTECT"

You can set the following protection levels on your CPU with SFC 109:

- SFC 109 call with MODE=0: Setting the protection level 1. If the password legitimization is locked, the lock is canceled by calling SFC 109 with MODE=0.
- SFC 109 call with MODE=1: Setting of protection level 2 with password legitimization. This means you can cancel the write protection set with SFC 109 if you know the valid password. The SFC 109 call with MODE=1 overrides any existing lock of password legitimization.
- SFC 109 call with MODE=2: Setting of protection level 3 without password legitimization. This means you cannot cancel the write and read protection set with SFC 109 even if you know the valid password. If a legitimated connection exists at the time of the SFC 109 call with MODE=2, the SFC 109 call has no effect for this connection.

Note

Setting a lower protection level

With SFC 109 "PROTECT", you cannot set a lower protection level than the one configured in HW Config.

NOTICE
Use SFC 109 only with existing protection level
Only use SFC 109 if you have configured protection levels in HW Config.

Additional aspects

- Both fault-tolerant CPUs of a fault-tolerant system can have different protection levels in STOP.
- The protection level is transferred from the master to the standby during link-up/update operations.
- The set protection levels of both fault-tolerant CPUs are retained if you make modifications to the plant during operation.
- The protection level is transferred to the target CPU in the following cases:
  - Switch to CPU with modified configuration
  - Switching to a CPU with modified operating system
  - Switching to a CPU using only one intact redundant link

8.3 Security event logging

Security events

The CPU 410SIS supports security events according to IEC 62443-3-3. The security events can be sent from the CPU in syslog frames to up to four external SIEM servers (Security Information and Event Management). For the scenario that no external SIEM server is accessible, the CPU 410SIS stores up to 3200 events in the work memory. If more than 3200 security events occur, the oldest events are overwritten.

You can store security events as a text file using Simatic Manager -> PLC -> Save Security Events.

Parameter description

The entries in the saved text file are structured as follows:

CEF parameter	Key name	Meaning
CEF	CEF	0
Manufacturer		Siemens AG
Device		e.g.: CPU 410SIS
Version		e.g.: V8.2.0
Event ID		Corresponds to Security Event ID (see below)
Event		Security Event (textual name of the signature ID)
Priority		1: Alarm (A) This situation requires immediate action. 3: Error (E) Correctable error in general. 5: Note (N) A situation has occurred that could require targeted action. 6: Information (I) Message during runtime
Protection level	protlevel	Set protection level 0 or 1 to 3, CPU-specific
Start time	start	Time stamp for occurrence of the event Format: MMM dd yyyy HH:mm:ss.SSS
Operating mode (optional)	opmod	Operating mode of the CPU (e.g. STOP)
Reason (optional)	reason	Byte-encoded origin of the event

CEF parameter	Key name	Meaning
Connection parameters (optional)		The following parameters are summarized under the term "Connection parameters": • Connection_id, Session ID • Protocol • Application protocol • Connection type • Gateway session ID • Source addresses – Source IP address – Source MAC address – SourcePort – Source tsap id – Source subnet id – Source Profibus address – Source C-bus rack number – Source C-bus slot number • Destination addresses – Destination IP address – Destination MAC address – Destination port – Destination tsap id – Destination subnet id – Destination Profibus address – Destination K bus rack number – Destination C-bus slot number
Status (optional)	status	Contains the number of overwritten unsent security events

Note

You can request the details of specific encodings from Customer Support.

Events

The following table provides an overview of the individual events.

Security event ID	Event	Security Event Severity meaning
3	SE_NETWORK_SUCCESSFUL_LOGON	Connection established with correct authentication
4	SE_NETWORK_UNSUCCESSFUL_LOGON	Error occurred during logon. Incorrect password or logon not currently possible (due to AaA)
5	SE_LOGOFF	Cancel logon
11	SE_ACCESS_PWD_ENSABLED	Password protection was set up

Security event ID	Event	Security Event Severity meaning
12	SE_ACCESS_PWD_DISABLED	Password protection was revoked
13	SE_ACCESS_PWD_CHANGED	Password has been changed.
20	SE_ACCESS_DENIED	A connection setup from the outside is rejected because Field Interface Security is activated for this interface
71	SE_SOFTWARE_INTEGRI-TY_CHECK_FAILED	An attempt was made to install invalid firmware.
75	SE_SESSION_CLOSED	Connection closed
94	SE_SECURITY_CONFIGURA-TION_CHANGED	The CPU security settings have been changed.
95	SE_SESSION_ESTABLISHED	Connection established
96	SE_CFG_DATA_CHANGED	A configuration change was made
97	SE_USER_PROGRAM_CHANGED	A SIS compact user program change has been transferred
98	SE_OPMOD_CHANGED	Operating state changed
99	SE_FIRMWARE_LOADED	A firmware change has been downloaded.
100	SE_FIRMWARE_ACTIVATED	The previously downloaded firmware change has been activa-ted.
101	SE_SYSTEMTIME_CHANGED	The time of day has been reset.

Note

You can request the details of specific encodings from Customer Support.

Procedure

You can configure the sending of security events in HW Config as follows:

- Send Yes/No, common switch for all messages
- IP address of the SIEM server. You can specify two different IP addresses.
- The port number on the SIEM server
- You can assign a maximum of 4 IP addresses per station and assign all 4 IP addresses to one interface (X5, X8).

8.4 Field Interface Security

Activating additional protection at the PROFIBUS or PROFINET interface

If want to prevent access to the CPU over the PROFIBUS or PROFINET interface, you can block that access.

To achieve the greatest possible protection from unauthorized access, you can disable all functions that are not required for the actual automation task. For the interfaces (PROFIBUS and PROFINET), this means that all incoming connection requests are rejected.

You can prevent an incoming connection attempt for each interface with the setting "Activate additional protection at the interface (Field Interface Security)" in HW Config. This prevents any connections being established by external bus nodes. All requests are then rejected. The connections required for IO operation are still established from the CPU

Features of disable

- If you have set a disable for a specific interface, connections that have already been established passively over this interface will be terminated. This applies for all connection types.
- If an incoming connection is rejected because a disable is set, a security event (SysLog) is generated.
- The receipt of UDP message frames (TURCV, both active and passive) is not possible at a blocked interface. TURCV is canceled and an error output.
- The disable applies irrespective of the CPU protective levels.
- For configured H connections with individual partial connections both over X5 and over X8, the partial connections are terminated.

8.5 Access-protected blocks

S7-Block Privacy

The STEP 7 add-on package S7-Block Privacy can be used to protect the functions and function blocks against unauthorized access.

Observe the following information when using S7-Block Privacy:

- S7-Block Privacy is operated by means of shortcut menus. To view a specific menu help, press the "F1" function key.
- You can no longer edit protected blocks in STEP 7. Moreover, testing and commissioning functions such as "Monitor blocks" or breakpoints are no longer available. Only the interfaces of the protected block remain visible.
- Protected blocks can only be released again for editing if you have the correct key and the corresponding decompilation information included in your package. Make sure that the key is always kept in a safe place.
- If your project contains sources, you can use these to restore the protected blocks by means of compilation. The S7-Block Privacy sources can be removed from the project.

Note

Memory requirements

Each protected block with decompilation information occupies 232 additional bytes in load memory.

Each protected block without decompilation information occupies 160 additional bytes in load memory.

Note

Extended runtimes

The startup time of the CPU at power on, the loading time of blocks and the startup after a system modification at runtime may be significantly prolonged.

To optimize additional time requirements, it is best practice to protect one large block instead of many small blocks.

Additional information

For additional information, refer to "S7 block privacy" in the STEP 7 Online Help.

8.6 Retentive load memory

Retentivity of the user program

The load memory is retentive, all blocks are also available after power off/on even if you are not using a back-up battery.

As a result, the user program is retained in the CPU after an unbuffered Power Off. Power failures are ridden through. The user program, the configuration and the parameters set in data blocks retain their state at the last complete download.

Note

If you want to operate the CPU 410SIS without a backup battery, you must switch off the buffer monitoring at the power supply. Otherwise, the CPU remains in STOP when powering up after Power On and does not switch automatically to RUN.

Without a backup battery, the following data is not buffered:

- Diagnostics buffer
- Security event buffer
- Date and time
- Process image
- Data blocks that were not backed up to the load memory with CFC
- Data blocks created by the program (CREATE_DB instruction)
- Operating hours counter
- Bit memory
- Timers
- Counters

CAUTION

Caution when replacing a CPU

If you reuse a CPU that has previously been used at a different location, ensure that the contents backed up in the load memory cannot pose a hazard at the new point of use.

Reset the CPU to factory settings if its previous use is unknown.

Buffering with a battery

If you are using one or two backup batteries in the power supply module and the power supply module is switched off or the supply voltage in the CPU and configurable modules fails, the set parameters and the memory content (RAM) will be buffered via the backplane bus as long as there is still battery capacity.

8.7 Type update with interface change in RUN

Overview

The AS 410 SIS supports the type update with interface change in RUN mode.

Gives you the option to update the instances at block types after an interface change and download the update to the PLC in RUN.

You will find more detailed information on this topic in the *Process Control System PCS 7, CFC for SIMATIC S7* manual.

8.8 Resetting the CPU 410SIS to delivery condition (reset to factory setting)

CPU factory settings

A general memory reset is performed when you reset the CPU to its factory settings and the properties of the CPU are set to the following values:

Table 8-2 CPU properties in the factory settings

Properties	Value
Contents of the diagnostics buffer	Empty
IP parameters	None
SNMP parameters	Default values
Operating hours counter	0 without battery backup
Contents of the load memory	Empty

Procedure

Proceed as follows to reset a CPU to its factory settings:

1. Switch off the line voltage.
2. Switch on the line voltage while pressing and holding down the Reset button.
3. Wait until LED lamp image 1 from the subsequent overview is displayed. In this lamp pattern, INTF flashes at 0.5 Hz. EXTF, BUSxF, MAINT, IFMxF, RUN, and STOP remain unlit.
4. Wait until LED lamp image 2 from the subsequent overview is displayed. In this LED pattern, INTF is lit. EXTF, BUSxF, MAINT, IFMxF, RUN, and STOP remain unlit.
5. The CPU performs a memory reset and the STOP LED flashes at 2 Hz.

The CPU is now reset to its factory settings. It starts up and switches to STOP operating state or links up. The event "Reset to factory setting" is entered in the diagnostics buffer.

LED patterns during CPU reset

While you are resetting the CPU to its factory settings, the LEDs light up consecutively in the following LED patterns:

Table 8-3 LED patterns

LED	LED pattern 1	LED pattern 2
INTF	Flashes at 0.5 Hz	Lit
EXTF	Dark	Dark
BUSxF	Dark	Dark
MAINT	Dark	Dark
IFMxF	Dark	Dark

LED	LED pattern 1	LED pattern 2
RUN	Dark	Dark
STOP	Dark	Dark

8.9 Reset during operation

CPU operating state

The following procedure references the RED or RUN RED operating state.

Note

If you perform a reset to prevent a malfunction of the CPU, you should read out the diagnostics buffer and the service data before the reset with the menu command "PLC -> Save service data".

Reset procedure during operation

Press and hold down the Reset button for 5 seconds. The CPU generates the current service data and writes the event W#16#4308 ("Memory reset started by switch operation") to the diagnostics buffer. The CPU then switches back to RUN.

8.10 Response to fault detection

Response to fault detection

To ensure high reliability, especially in the H system, the CPU 410SIS has extensive self-diagnostics capabilities. Faults can thus be detected and eliminated at an early stage. In the rare instance that a fault occurs that cannot be eliminated by the firmware, the current service data is saved internally for further evaluation by SIEMENS specialists. An automatic reboot is then started. This behavior reduces the downtime of the CPU to a minimum. Access to the process is restored as soon as possible.

CPU response following reboot

The CPU operating system tries to switch back to RUN by rebooting the CPU.

The CPU responds as follows to a reboot:

1. The CPU writes the cause of the error to the diagnostics buffer.
2. The CPU generates the current service data.

3. The CPU checks if a reboot is possible.
   A reboot is not possible in the following cases:
   - The user data is inconsistent.
   - A reboot has already been carried out within the previous 24 hours.
   - The event that led to the defect is preventing an automatic reboot.
4. The CPU records the automatic reboot in the diagnostics buffers (event W#16#4309 "Memory reset launched automatically" or W#16#452B "CPU REBOOT for clearing data inconsistency").
5. The CPU runs internal tests.
6. In a redundant system, the standby CPU links up to the master in operation.
7. In stand-alone operation and solo mode, the CPU loads the backed up user program and executes a warm restart.

8.11 Reading service data

Application case

If you need to contact Customer Support due to a service event, the department may require specific diagnostic information on the CPU status of your system. This information is stored in the diagnostic buffer and in the service data.

Select the "PLC -> Save service data" command to read this information and save the data to two files. You can then send these to Customer Support.

Note the following:

- If possible, read out the service data immediately after the CPU goes into STOP or immediately after the synchronization of a fault-tolerant system has been lost.
- Always read out the service data of both CPUs in a fault-tolerant system.

Procedure

1. Select the "PLC > Save service data" command.
   In the dialog box that opens up, select the file path and the file names.
2. Save the files.
3. Forward these files to Customer Support on request.

Note

Customer Support may also request a readout of the security events for diagnostic purposes in the service case. You can store the security events as a text file with:

>Simatic Manager - PLC - Save Security Events

See also Security event logging (Page 106)

8.12 Updating firmware in stand-alone operation

Basic procedure

To update the firmware of a CPU, you will receive several files (*.UPD) containing the current firmware. You download these files to the CPU. You can update the firmware in a single work step or you can first download it to the CPU and then activate it at a later time.

Requirement

The CPU whose firmware you want to update must be accessible online, e.g., via PROFIBUS or Industrial Ethernet. The files containing the current firmware versions must be downloaded into the programming device/PC file system. A folder may contain only the files of one firmware version. If the CPU is protected with a password, you need the respective password for the update.

Note any information posted in the firmware download area.

Note

Checking the firmware update files (*.UPD)

The CPU checks the firmware update files (*.UPD) during the update process. If an error is detected, the old firmware remains active and the new firmware is rejected.

For CPU access protection with password: in SIMATIC Manager, select a CPU of the fault-tolerant system, then select "PLC > Access Rights > Setup" from the menu. Enter the CPU access password.

Firmware update in two stages

The advantage of updating the firmware in two stages is that the automation system only switches to STOP during the actual activation of the new firmware. The firmware is loaded in RUN. This allows you to carry out the longer process of loading the firmware beforehand in RUN at a suitable time, and launch the quicker activation process later.

Proceed as follows to update the firmware of a CPU:

1. Open the station containing the CPU you want to update in HW Config.
2. Select the CPU.
3. Select the "PLC -> Update firmware" menu command.
4. In the "Update firmware" dialog, select the path to the firmware update files (*.UPD) using the "Browse" button.
   After you have selected a file, the information in the bottom boxes of the "Update firmware" dialog box will indicate the modules for which the file is suitable and as of which firmware version.
5. Select "Only load firmware".
   The firmware will be loaded to the CPU.

Proceed as follows to activate the loaded firmware at a later time:

1. Open the station containing the CPU you want to update in HW Config.
2. Select the CPU.
3. Select the "PLC -> Update firmware" menu command.
4. Select "Activate loaded firmware" and click "Execute".
5. Acknowledge the security prompt with "OK".
   The firmware update will run automatically.
6. Acknowledge the final message with "Yes".

The CPU is now in RUN again.

Firmware update in one stage

Proceed as follows to update the firmware of a CPU:

1. Open the station containing the CPU you want to update in HW Config.
2. Select the CPU.
3. Select the "PLC -> Update Firmware" menu command.
4. In the "Update Firmware" dialog, select the path to the firmware update files (*.UPD) using the "Browse" button.
   After you have selected a file, the information in the bottom boxes of the "Update Firmware" dialog box indicate the modules for which the file is suitable and from which firmware version.
5. Select "Load and activate firmware" and click "Execute".
6. Acknowledge the security prompt with "OK".
   The firmware update will run automatically.
7. Acknowledge the final message with "Yes".

The CPU is now in RUN again.

Values retained after a firmware update

The following values are retained after a firmware update:

- IP address of the CPU
- Device name (NameOfStation)
- Subnet mask
- Static SNMP parameters
- Contents of the load memory

8.13 Updating firmware in redundant mode

Requirement

You are operating the CPU 410SIS in an H system. Both Sync links exist and are working. There are no redundancy losses. The REDF LED is not lit and both CPUs are in redundant mode.

Note any information posted in the firmware download area.

Note

Checking the firmware update files (*.UPD)

The CPU checks the firmware update files (*.UPD) during the update process. If an error is detected, the old firmware remains active and the new firmware is rejected.

For CPU access protection with password: in SIMATIC Manager, select a CPU of the fault-tolerant system, then select "PLC > Access Rights > Setup" from the menu. Enter the CPU access password.

Note

Redundancy error

There must not be a redundancy error, e.g. a faulty IM153-2, because the update may otherwise lead to station failures.

Firmware update in two stages

The advantage of updating the firmware in two stages is that the fault-tolerant system only operates in solo mode during the actual activation of the new firmware. The firmware is loaded in redundant mode. This allows you to carry out the longer process of loading the firmware beforehand in redundant mode at a suitable time, and launch the quicker activation process later.

Proceed as follows to update the firmware of the CPUs of a fault-tolerant system in RUN:

1. Open the station containing the CPU you want to update in HW Config.
2. Select the CPU.
3. Select the "PLC -> Update firmware" menu command.
4. In the "Update firmware" dialog, select the path to the firmware update files (*.UPD) using the "Browse" button.
   After you have selected a file, the information in the bottom boxes of the "Update firmware" dialog box will indicate the modules for which the file is suitable and as of which firmware version.
5. Select "Only load firmware" and click "Execute".
   The firmware will be loaded to both CPUs. Both CPUs remain in redundant mode. Loading can take several minutes.

Proceed as follows to activate the loaded firmware at a later time:

1. Open the station containing the CPU you want to update in HW Config.
2. Select the CPU.
3. Select the "PLC -> Update firmware" menu command.
4. Make sure that the same firmware version as the loaded firmware has been loaded to both CPUs.
   The version of the loaded firmware is displayed in the "Update firmware" dialog.
5. Select "Activate loaded firmware" and click "Execute".
   The CPU in rack 1 is switched to STOP
   The new firmware is activated in the CPU in rack 1
6. Click "Continue".
   The system switches to the CPU with the new firmware.
   The new firmware is activated in the CPU in rack 0.
   The CPU in rack 0 is started.
   The CPU in rack 0 is linked up and updated.

Both CPUs have updated firmware (operating system) and are in the redundant operating state.

Firmware update in one stage

Proceed as follows to update the firmware of the CPUs of a fault-tolerant system in RUN:

1. For CPU access protection with password: Select a CPU of the fault-tolerant system in SIMATIC Manager and select menu command
   PLC > Access Authorization > Setup. Enter the CPU access password.
2. Select the CPU.
3. Open the station containing the CPU you want to update in HW Config.
4. Select the "PLC -> Update firmware" menu command.
5. In the "Update Firmware" dialog, select the path to the firmware update files (*.UPD) using the "Browse" button.
   After you have selected a file, the information in the bottom boxes of the "Update Firmware" dialog box indicates the modules for which the file is suitable and as of which firmware version.
6. Select "Load and activate firmware".
7. Click "Execute".
   The CPU in rack 1 is switched to STOP.
   The new firmware is loaded to and activated in the CPU in rack 1.
8. Click "Continue".
   The system switches to the CPU with the new firmware.
   The new firmware is loaded to and activated in the CPU in rack 0.
   The CPU in rack 0 is started.
   The CPU in rack 0 is linked up and updated.

Both CPUs have updated firmware (operating system) and are in the redundant operating state.

Note

Only the third number of the firmware versions of the master and standby CPU may differ by 1. You can only update to the newer version.

The constraints described in Chapter System and operating states of the CPU 410SIS (Page 71) also apply to a firmware update in RUN.

Any set up access right is not canceled until you stop the SIMATIC Manager. You should reset the access right once again to prevent unauthorized access. You reset the access right in the SIMATIC Manager with the menu command PLC > Access Rights > Cancel.

Values retained after a firmware update

The following values are retained after a firmware update:

- IP address of the CPU
- Device name (NameOfStation)
- Subnet mask
- Static SNMP parameters
- Contents of the load memory

Time synchronization and time stamping

9

Definition of time synchronization

Time synchronization refers to the process in which various S7 stations receive or retrieve their local time from a central time source (central time transmitter/time server).

Time-of-day synchronization is required when the time sequence of events from different stations is to be evaluated.

Interfaces

Time-of-day synchronization is possible across all interfaces of the CPU 410SIS:

- PROFINET interface via Industrial Ethernet
  Time-of-day synchronization using the NTP method; the CPU is the client.
  Time-of-day synchronization using the SIMATIC method as master or slave.
- Within the station (in the AS) using the S7-400 backplane bus
  You can configure the CPU as a time master or a time slave.
- PROFIBUS DP interface
  You can configure the CPU as a time master or a time slave.

Time-of-day synchronization via the PROFINET interface

Time-of-day synchronization is possible via the PROFINET interface using both the NTP method and the SIMATIC method. The CPU 410SIS is the client in this case.

You can configure up to four NTP servers. You can set an update interval of between 10 seconds and 1 day. An NTP request of the CPU 410SIS always occurs every 90 minutes for time settings greater than 90 minutes.

If you synchronize the CPU 410SIS in the NTP method, you should use SICLOCK or an NTP server on the OS.

Time-of-day synchronization is also possible via Ethernet MMS (Simatic method on Ethernet) as master or slave. NTP can in this case be combined with the SIMATIC method.

CPU 410SIS as time slave

If the CPU 410SIS is a time slave on the S7-400 backplane bus, synchronization is via the CP by a central clock connected to the LAN.

You can use a CP to forward the time to the S7-400 station. If the CP supports a direction filter, the CP must be configured for time forwarding with the "from LAN to station" option.

CPU 410SIS as time master

If you configure the CPU 410SIS as the time master, you must specify a synchronization interval. You can select any interval between 1 s and 24 h.

Select a synchronization interval of 10 s if the CPU 410SIS is the time master on the S7-400 backplane bus.

The time master does not send time frames until its time of day has been set. You can set the of day with STEP 7 or with an interface as time slave (NTP client / slave).

Definition of time stamping

Time stamping refers to the assignment of an event to its acquisition time. The more precise this assignment is, the more precisely the acquisition time corresponds to the event.

For time stamping the DP master sends its time of day to the DP line.

The DP slave receives this time of day and uses this time information for time stamping.

In this case, one refers to "high-precision time stamping" in the context of SIMATIC SIS compact.

Relationship between time synchronization and time stamping

To examine the chronological relationship between time stamped events from different S7 stations, the S7 stations must be time synchronized.

The synchronism among the individual systems is dependent on the selected time synchronization method, the topology and the utilized interface in the S7 station.

Precision

The precision of the time stamping is the maximum difference of the time stamps that result from signals that were recorded simultaneously by digital input modules.

The precision depends on the hardware used and the configuration of the plant.

Resolution

The resolution is the smallest possible time difference between two different time stamps.

Additional information

You can find additional information about time-of-day synchronization and time stamping in the following manuals:

- Process Control System PCS 7, High-precision Time Stamping (V9.0)
- Process Control System PCS 7, Time Synchronization (V9.0)

Plant changes in RUN - CiR 10

10.1 Motivation for CiR via PROFINET DP

There are plants that must not be shut down during operation. This may be the case, for example, due to the complexity of the automated process or due to high restart costs. Nevertheless, it may be necessary to expand or modify a configuration.

With the help of a plant change during operation using CiR, certain configuration changes can be made in RUN. In so doing, processing is stopped for a brief time interval. The upper limit of this time interval is 60 ms. Process inputs retain their last value during this time.

Note

The term "CiR" stands for "Configuration in RUN". It refers to the method described in this documentation for modifying a plant during operation. The requirements listed below must be met for this.

Hardware requirements for PROFIBUS DP

The following hardware and firmware requirements must be met for plant changes in RUN using CiR:

- If you want to add modules for ET 200M, you must also configure the ET 200M with active bus elements and sufficient free space for the planned expansion. You may not integrate the ET 200M as DPV0 slave (with a GSD file).
- If you want to add additional electronic modules to the ET 200iSP: Configure the ET 200iSP with standby modules. You replace the standby modules when you install electronic modules later.
- If you want to add entire stations: Stock the corresponding bus connectors, repeaters, etc.
- Use of the CR2 rack is not permitted.

Note

You can combine components that support system changes during operation using CiR with those that do not support this function as desired. However, you can only make plant changes to components that have CiR capability.

The following configuration changes in RUN are then permitted:

- Adding and removing electronic modules in ET 200M.
- Adding and removing electronic modules in ET 200iSP.

Configuration requirements for PROFIBUS DP

You need to select saving on the CPU for all modules within the station for which you can choose whether the configuration data is saved on the module itself or on the CPU.

Software requirements

The user program must meet the following requirement if you are to make a configuration change in RUN: It must be written in such a way that station failures or module faults, for example, do not result in a CPU STOP.

The following OBs must be available in your CPU:

- Hardware interrupt OBs (OB 40 to OB 47)
- Cycle time error OB (OB 80)
- Diagnostic interrupt OB (OB 82)
- Remove/insert interrupt OB (OB 83)
- Program execution error OB (OB 85)
- Rack failure OB (OB 86)
- I/O access error OB (OB 122)

Note

SIMATIC SIS compact always meets all these requirements.

10.2 Permitted changes over PROFIBUS DP

Permitted configuration changes: Overview

The method presented here supports the following modifications in your automation system:

- Addition of modules for a modular DP slave, provided you have not integrated it as a DPV0 slave (via a GSD file).
- Reassignment of module parameters, e.g. selection of different alarm limits or use of previously unused channels
- Replacement of standby modules with future electronic modules of the ET 200iSP
- Reassignment of parameters of ET 200iSP modules
- Addition of DP slaves to an existing DP master system
- Assignment of added modules to a process image partition
- Modification of the process image partition assignment for existing modules or compact slaves

- Reassignment of parameters of existing modules in DP stations (standard modules and fail-safe signal modules in standard operation)
- Undoing of modifications (undo functionality): Added modules and DP slaves can be removed again.

All modifications that are not expressly permitted above are not permitted as part of a plant change during operation and are not further discussed here. These include, for example,

- Change of CPU-properties.
- Change of properties of centrally inserted I/O modules.
- Change of properties of existing DP master systems including bus parameters.
- Change of the following parameters of a DP slave: bus address, assignment of DP master, parameter assignment data, diagnostic address.
- Reassignment of parameters of fail-safe signal modules in safety operation.
- Addition and removal of DP master systems.
- Removal of any modules from modular DP slaves, see undoing of previously made changes.
- Removal of any DP slaves from an existing DP master system, see undoing of previously made changes.

Recommendations for plant changes in RUN using CiR

Some tips are given below for Configuration in RUN.

- Create a backup copy of your current plant configuration after each configuration change. Further processing of the project without loss of CiR capability is only possible with this backup version.
- If possible, change the configuration in multiple steps and make only a few changes in each step. This approach will help you to keep things under control.

10.3 CiR objects and CiR modules for PROFINET DP

10.3.1 Basic Requirements

Overview

A system modification during RUN via CiR is based on the provisions you have made in your initial configuration for an expansion of your PLC hardware. Define suitable CiR-compatible elements that you can later replace step-by-step in RUN mode with real objects (slaves and/or modules). You can then download such a modified configuration to the CPU during runtime.

Procedure

The table below shows the procedures required for modification of the program and of the configuration, as well as the corresponding system phase.

Step	Action	CPU mode	System status
1	Configuration of your current (real) system configuration	STOP	Offline configuration
2	Defining CiR Elements	STOP	Offline configuration
3	Configuration download	STOP	Commissioning
4	System modifications are only possible on master systems which contain a CiR object or on ET 200M stations which are equipped with a CiR module.	RUN	Continuous operation

If required, execute several passes of the CiR sequence (step 4 of the table above). You merely have to provide a sufficient number of slaves or adequate I/O volume for all of your system expansions before you switch to continuous operation.

10.3.2 Types of CiR Elements

Overview

The following CiR elements are available:

Component	CiR element
Existing DP master system	CiR object It contains the number of additional I/O modules and you can edit it.
Modular DP slave of type ET 200M / ET 200iSP	CiR module If contains the additional I/O volume and you can edit it.

Note

STEP 7 takes into account both the configured slaves and the CiR elements when the bus parameters are determined. When CiR elements are converted into real slaves and/or modules while the CPU is in RUN, the bus parameters therefore remain unchanged.

You can add CiR elements either automatically or individually.

CiR objects

You specify the following properties for a CiR object:

- Number of slaves that you are guaranteed to be able to add (default setting: 15 on DP master system)
- Number of input bytes and output bytes for future use (default setting: 1220 each on DP master system) This relates to future user data addresses. You can configure diagnostic addresses independent of this.

CiR modules

For the modular ET 200M / ET 200iSP I/O device, you specify an additional I/O volume with the help of a CiR module by defining the total number of additional input bytes and output bytes. This relates to future user data addresses. You can configure diagnostic addresses independent of this.

The additional user data volume does not have to be used up completely at any given time. However, the user data volume currently still available may never be exceeded. This is ensured by STEP 7.

See also

Defining CiR Elements (Page 129)

10.3.3 CiR Elements and I/O Address Areas

CiR objects

The following rule applies to a DP master system: The total of the number of configured real slaves and the guaranteed number of slaves of the CiR object in the associated DP master system may not exceed the quantity structure of the associated DP master.

Compliance with this rule is monitored directly by HW Config during definition of the CiR objects.

I/O volume for CiR objects and CiR modules that can be used in the future

The following rules apply to the DP master with respect to the input and output bytes that can be used in the future:

I/O	Rule 1
Inputs	The total of configured real user addresses for inputs and input bytes that can be used in the future must not be greater than the quantity structure of the DP master.
Outputs	The total of configured real user addresses for outputs and output bytes that can be used in the future may not be greater than the quantity structure of the DP master.

Compliance with these rules is monitored by HW Config directly during the definition of the CiR elements of the DP master system.

To use the CiR elements as flexibly as possible, however, the following applies from the CPU perspective:

I/O	Rule 2
Inputs	The total of configured real inputs and input bytes that can be used in the future can be greater than the quantity structure of the CPU.
Outputs	The total configured real outputs and output bytes that can be used in the future can be greater than the quantity structure of the CPU.

HW Config does not check whether the added slaves and/or modules fit into the available address space of the CPU until the CiR elements are used.

10.4 Procedure for PROFIBUS DP

10.4.1 Basic Procedures in STOP Mode

10.4.1.1 Overview

Note

Back up your current configuration after each download of the station configuration from HW Config (regardless of the operating state of the CPU). This is the only way for you to ensure that you can continue working with the backed up project in case of an error (loss of data) without loss of the CiR capability.

Overview

The following basic operating steps are available in STOP state:

- Defining CiR elements
- Deleting CiR elements
- Editing CiR elements
- Downloading the configuration

Defining CiR elements

You can define CiR objects for previously configured DP master systems and CiR modules for modular DP slaves of type ET 200M / ET 200iSP. For the exact procedure, see Defining CiR elements.

The "Activate CiR capability" function is additionally available for DP master systems. If you select this function, a CiR object is created on the selected DP master system. A CiR module

is inserted on each CiR-capable modular slave of type ET 200M / ET 200iSP on the selected DP master system.

Note

The "Activate CiR capability" function is only possible on DP master systems on which a CiR object is not yet defined.

Deleting CiR elements

In STOP operating state, you can delete CiR objects on DP master systems or CiR modules on modular DP slaves of type ET 200M / ET 200iSP that you have defined previously.

If you want to delete all CiR elements in a DP master system, you can easily do this using the "Deactivate CiR capability" function.

Note

The "Deactivate CiR capability" function is only possible for DP master systems on which a CiR object is defined.

Downloading the configuration

After defining new CiR elements or redefining existing CiR elements, you download the configuration with the CPU in STOP operating state.

A large number of modules can be used in the S7-410 automation system. To ensure that none of the modules you are using will prevent a future CiR action, you must adhere to the following procedure: Once you have downloaded the configuration in STOP operating state of the CPU, immediately download it again to the CPU, but this time with the CPU in RUN operating state. When this is done, STEP 7 and the CPU will check the CiR capability. With older modules or modules from third-party manufacturers, this is not yet possible offline.

10.4.1.2 Defining CiR Elements

Adding CiR elements automatically

Note

The automatic addition of CiR elements is only possible if a CiR object is not yet present on the selected DP master system.

If you want to automatically add CiR elements in an existing DP master system, proceed as follows:

1. Select the relevant DP master system in the upper part of the station window.
2. In the Edit menu, select the "Master System > Activate CiR capability" command.
   STEP 7 then adds the following CiR elements on the selected DP master system:
   - A CiR module on each CiR-capable modular slave (if slots are still available).
     This CiR module contains so many input and output bytes that a reasonable number is available for later use on the modular slave.
   - A CiR object on the selected DP master system.
     STEP 7 attempts to guarantee 15 slaves and to make available 1220 input bytes and 1220 output bytes for this CiR object. If the largest address up to now on this master system is greater than 110, correspondingly fewer slaves can be guaranteed. If fewer than 1220 input bytes and 1220 output bytes are available, the number is reduced accordingly.
3. The default settings of the CiR objects are the same for all CPUs. For this reason, after activation of CiR capability of a master system, you should check each associated CiR object to determine whether the CiR synchronization time of the master system specified in the properties window of the CiR object is compatible with the CiR synchronization time of the CPU.

Adding a CiR object on the DP master system

If you want to add a CiR object in a DP master system, follow these steps:

1. Select the relevant master system in the upper part of the station window.
2. Open the "Hardware catalog" window.
3. Using drag-and-drop, move the associated CiR object from the hardware catalog onto the master system. The CiR object then appears in the upper part of the station window as a placeholder slave. The CiR object has the following default values:
   - Number of guaranteed additional slaves: 15 on DP master system
   - Maximum number of additional slaves: 45 DP slaves
   - Number of input bytes: 1220 for a DP master system
   - Number of output bytes: 1220 for a DP master system

4. The default settings of the CiR objects are the same for all CPUs. For this reason, after definition of a CiR object, you should check whether the CiR synchronization time of the associated master system specified in the properties window of the CiR object is compatible with the CiR synchronization time of the CPU.
5. If you want to change the number of additional slaves and/or the number of input/output bytes, proceed as follows:
   Open the properties window of the CiR object (double-click the CiR object or select CiR object, right-click and select "Object properties ..." or select CiR object and "Edit > Object properties ...").
   You can change the guaranteed number of additional slaves. The lower part of the station window displays the resulting bus parameters: Target Rotation Time, Typical Target Rotation Time and watchdog time.
   You can also change the number of input bytes and output bytes. To do so, select the "Advanced settings" check box.

Adding a CiR module in a modular slave of type ET 200M / ET 200iSP

For a modular slave, proceed as follows:

1. Select the relevant slave in the upper part of the station window.
2. Open the "Hardware catalog" window.
3. Using drag-and-drop, move the CiR module from the hardware catalog onto the slot directly after the last configured module of the DP slave in the lower part of the station window. (If you automatically add CiR elements, this rule is automatically taken into account.) The CiR module then appears in the lower part of the station window as a placeholder module. The number of input bytes and output bytes are displayed in the properties window of the CiR module.
4. For ET 200M stations, this is determined as follows:
   - Number of input bytes = Number of free slots * 16
     In an ET 200M station that contains only a CiR module, this value is thus 128 (if the CiR object on the DP master system still has a sufficient number of free input and output bytes).
   - Number of output bytes = Number of free slots * 16
     In an ET 200M station that contains only a CiR module, this value is thus 128 (if the CiR object on the DP master system still has a sufficient number of free input and output bytes).

Note

For ET 200iSP, a maximum of 244 input bytes and output bytes are available. You can find the input and output bytes of the individual electronic modules in the ET 200iSP manual.

Downloading the configuration

After defining the CiR elements you download them with the CPU in STOP operating state.

A large number of modules can be used in the S7-400 automation system. To ensure that none of the modules you are using will prevent a future CiR action, you must adhere to the following procedure: Once you have downloaded the configuration in STOP operating state of

the CPU, immediately download it again to the CPU, but this time with the CPU in RUN operating state. When this is done, STEP 7 and the CPU will check the CiR capability. With older modules or modules from third-party manufacturers, this is not yet possible offline.

10.4.1.3 Deleting CiR Elements

Deleting all CiR elements

Note

The deletion of all CiR elements is only possible if a CiR object is present on the selected DP master system.

If you want to delete all CiR elements in an existing DP master system, proceed as follows:

1. Select the relevant DP master system in the upper part of the station window.
2. In the Edit menu, select the "Master System > Deactivate CiR capability" command.

STEP 7 then deletes

- all CiR modules in modular slaves
- the CiR object on the selected DP master system

Deleting an individual CiR element

If you want to delete the CiR module in a modular DP slave of type ET 200M / ET 200iSP, proceed as follows:

1. Select the CiR element to be deleted.
2. Select the **Delete** command in the shortcut menu or Edit menu.

If a DP master system has no more CiR elements besides the CiR object on this DP master system, you can delete this CiR object with the same procedure.

10.4.2 Basic Procedure in RUN Mode

10.4.2.1 Overview

Overview

The following basic operating steps are available in RUN:

- Add slaves or modules
- Rebuild hardware when adding a slave
- Change process image partition assignment

- Re-configure existing modules in ET 200M/ET 200iSP stations
- Undo previously made changes (Undo functionality)
- Replace slaves or modules

Note

All plant changes listed below require a CiR object in the DP master system. This also applies for adding and removing slave slots.

Back up your current configuration after each download of the station configuration from HW Config (regardless of the CPU mode). This is the only way to ensure that you can continue working with the backed up project in the event of an error (loss of data) without losing CiR capability.

10.4.2.2 add slaves or modules

Procedure

Adding slaves or modules in RUN mode involves the following steps:

1. Expand and download the configuration with HW Config.
2. Rebuild the hardware.
3. Expand, test and download the user program.

You must adhere to this order of steps.

Rules

You must comply with the following rules when adding components:

- Within a modular DP slave of the type ET 200M / ET 200iSP, you may only add a CiR module in the slot directly after the last configured module. (This rule is observed automatically if you add CiR elements automatically.)
- Within a master system, a slave added must be assigned a PROFIBUS address that is higher than the highest assigned so far.
- With the ET 200iSP, you can only ever add or remove one module per station and download.

10.4.2.3 Reconfigure the hardware when adding a slave

Procedure

1. Terminate both ends of PROFIBUS DP bus cables using active bus terminating elements in order to ensure proper termination of the cables while you are reconfiguring the system.
2. When adding a slave to a master system, make sure that no bus cables become disconnected.
   - One method of achieving this is to provide and connect additional bus connectors at the future mounting positions for the master systems to be expanded. Connect the new slave to these bus connectors, if necessary.
   - Another method is to provide repeaters or diagnostic repeaters. In this case, follow these steps when adding a slave:
     Turn off the repeater function.
     Connect the new slave on the previously unused end of the repeater. In doing so, observe the applicable installation guidelines (see *Installation manual: S7-400 and M7-400 Programmable Controllers Hardware and Installation)*.
     Turn on the repeater function again.

10.4.2.4 change process image partition assignment

Procedure

You can change the assignment of a process image partition of an existing module or compact slave as follows:

1. Open the properties window of the module or slave. Specify the new process image partition in the "Addresses" tab.
2. Download the new configuration with HW Config.

10.4.2.5 reconfigure existing modules in ET200M / ET200iSP stations

Procedure

The procedure for using previously free channels is described under Using a Previously Unused Channel.

The procedure for reconfiguring already used channels of ET200M / ET200iSP modules is described under Reconfiguring a Previously Used Channel or under Removing a Previously Used Channel.

See also

Reconfiguring an already used channel. (Page 141)

Delete an already used channel. (Page 142)

10.4.2.6 Undo previous changes (Undo function):

Procedure

Undoing changes in RUN involves the following steps:

1. Undo the changes previously made in the user program (if necessary) and then download the user program.
2. Remove added slaves and modules from the configuration and download this configuration in RUN.
3. Rebuild the hardware, if necessary.

Rules

You must comply with the following rules when undoing changes:

- Within a modular DP slave of the type ET 200M / ET 200iSP, you may only remove the modules from the bottom (i.e. starting with the highest slot number).
- Within a master system, you must start at the highest PROFIBUS address of the slaves you want to remove. You can then continue with the slaves with lower addresses if required.

Note

You can remove slaves or modules that you have added in the course of multiple downloads in just one download.

By removing a slave or a module from a configuration, you increase the available I/O volume. The guaranteed number and the maximum number of slaves that can be used in the future may increase.

10.4.2.7 Replacing Slaves or Modules

Principle

The following rule applies: You can either remove or add slaves by downloading a configuration.

Replacement of slaves / modules by means of a download operation is therefore not supported.

10.4.2.8 Using CiR Elements in RUN Mode

Introduction

This section describes how to expand and then load an existing configuration.

Note

If you run invalid operations when adding real slaves or modules for configuration, an error message is not output until you load the configuration.

You should check for CiR capability after each plant change ("Station > Check CiR Capability" or the shortcut CTRL+ALT+F).

Adding a DP slave

To add a DP slave, follow these steps:

1. Open the "Hardware catalog" window.
2. Drag and drop the slave from the hardware catalog to the CiR object in the upper part of the station window.
   The slave added appears in the upper part of the station window. The name of the slave added is displayed on an orange background to indicate that it has been created from a CiR object.

   Note

   When a slave is added, STEP 7 updates the guaranteed and maximum number of slaves and the number of input and output bytes of the corresponding CiR object.

   We recommend selecting the station number of the added DP slave as follows:

   Station number of the DP slave added = highest station number of all DP slaves previously configured + 1

   If you select a higher station number for the added DP slave, the guaranteed number and maximum number of DP slaves that can still be added may be reduced by more than 1 under unfavorable circumstances.

   If you add a CiR-capable modular DP slave of the type ET 200M / ET 200iSP, it will be assigned a CiR module from the outset.

Adding modules in a modular slave of the type ET 200M / ET 200iSP

Proceed as follows to add components to an ET 200M / ET 200iSP modular slave:

1. Open the "Hardware catalog" window.
2. Drag and drop the module to be added to the CiR module in the bottom part of the station window.
   The module added then appears in the bottom part of the station window in the position that was occupied by the CiR module. The CiR module is moved down a slot.

Note

When you add a module to an ET 200M / ET 200iSP station, STEP 7 updates the number of input and output bytes of the corresponding CiR module.

Loading the configuration in RUN

A modified configuration is loaded in RUN in the following two steps:

1. Check that the current configuration can be loaded ("Station > Check CiR Capability").
2. Download the configuration to the CPU ("PLC > Download to module ...").

Note

When the configuration is loaded to the CPU, the INTF LED goes and off again and the EXTF LED comes on permanently. You cannot start added the real stations or modules until the INTF LED has gone out. The EXTF LED then goes out again (see "Behavior of the CPU after download of the configuration in RUN").

Back up your current configuration after each download of the station configuration from HW Config (regardless of the CPU mode). This is the only way to ensure that you can continue working with the backed up project in the event of an error (loss of data) without losing CiR capability.

10.4.2.9 Undoing Previous Changes

Principle

You can undo any previous configuration changes that you downloaded to the CPU by removing the slaves or modules you added at that time.

The following rules apply:

- When removing slaves within the DP master system, you must start with the slave at the highest PROFIBUS address. You then continue with the slave with the next-highest PROFIBUS address.
- Within a modular DP slave of the type ET 200M / ET 200iSP, you must start with the highest slot number of the modules you want to remove. In the HW Config view, this is the module at the very bottom. STEP 7 offers the following support for this step: The module that you can remove next is entered in the bottom part of the station window in standard font; all other modules are shown in italics.
  You then continue with the module with the next-highest slot number.

Procedure

1. Select the object you want to remove.
2. Select the "Delete" command in the shortcut menu or in the "Edit" menu.
3. Repeat steps 1 and 2 for the remaining objects you want to remove.
4. Download the modified configuration to your CPU.

Note

When you delete a slave, STEP 7 updates the guaranteed and the maximum number of slaves as well as the number of input and output bytes of the associated CiR object.

When you delete a module in a modular slave of the type ET 200M / ET 200iSP, STEP 7 updates the number of input and output bytes of the associated CiR module.

10.5 Reconfigure existing modules in ET200M / ET200iSP stations

10.5.1 Requirements for Reconfiguration

Note

You can use previously unused channels as well as re-configure previously used channels.

The addresses of existing modules may not be changed using CiR.

Requirement for configuration

Re-configuration requires an existing CiR object in the respective DP master system.

Hardware requirements

The modules (signal modules and function modules) of the ET 200M / ET 200iSP that can be re-configured in RUN mode of the CPU are listed in the info text in the "Hardware catalog" window.

The maximum number of modules that can be re-configured is 100.

10.5.2 Module Response During a Reconfiguration

Principle

During reconfiguration the input modules can respond in one of the three following ways:

- Channels not affected will continue to return the actual process value.
- Channels not affected will return the process value which was valid prior to the reconfiguration.
- All channels will return the value "0" (applies to digital modules and FMs) or W#16#7FFF (applies to analog modules).

Please refer to the technical data of the specific modules for information on their response.

Output modules respond as follows during reconfiguration:

The respective channels output the initial value which was valid before the parameter assignment.

10.5.3 CPU response during reconfiguration

Re-configuration sequence

Once you have made the parameter changes in HW Config and have downloaded them to the CPU in RUN mode, the CPU runs the tests described in "Behavior of the CPU after download of the configuration in RUN". The input and output values have the status "OK" after successful re-configuration.

You may only access those values in the process image that belong to the process image partition of the OB currently being processed.

The DP master marks the modules as available in the module status data if data record transfer was successful and as unavailable if data record transfer was not successful. In the latter case, access to the module triggers an I/O access error (in the event of input process image updates, transmission of the output process image to the module or direct access to the module. Depending on the type of access, OB 85 or OB 122 is started).

The input or output data of the modules behaves in the same way as after a remove module interrupt, which means it may not yet be correct (because the module may not yet have evaluated its data records). However, the restriction that data record SFCs for the modules can no longer be active no longer applies.

Note

If the re-configuration of a module involves disabling the diagnostic interrupt, for example, the module may still subsequently send an interrupt that it has already prepared.

Possible fault scenarios during re-configuration

The following error scenarios are possible:

- The module receives the parameter data records but cannot evaluate them.
- Serious errors (in particular protocol errors on the DP bus) may cause the DP master to completely suspend the corresponding DP slave, causing all modules of this station to fail.

Re-configuration dependency on CPU modes

Re-configuration takes place after SDB evaluation (see Behavior of the CPU after download of the configuration in RUN) in RUN mode. The INTF-LED is on during re-configuration.

The re-configuration process is interrupted during transition to HOLD. The process is continued when the CPU changes to STOP or RUN. In STOP, only the calls of OB83 are stopped.

Re-configuration is aborted if there is a power failure. Once power is restored, all existing DP stations are re-configured.

Coordination between master systems

The sequence

- OB 83 start (start event W#16#3367)
- Data record transmission
- OB 83 start (start event W#16#3267 or 3968)

may run in parallel in the master systems in question.

OB calls in re-configuration

Once the CPU has run the tests described in "Behavior of the CPU after download of the configuration in RUN", it starts OB 80 with the event W#16#350A. It then starts OB 83 with the start event W#16#3367. This means that as of now the input or output data of the I/O modules in question may no longer be correct. You may now no longer call any SFCs that trigger new jobs for sending data records to the modules involved (for example SFC 57 "PARM_MOD"), otherwise a conflict could occur between the data records sent by the system and those sent by the user.

Once the CPU has completed OB 83, it sends the parameter data records, with each module involved receiving the total number of data records (regardless of how many data records are affected by your change).

Another OB 83 start follows (start event W#16#3267 if sending was successful, W#16#3968 if it was not). No other priority class is interrupted by this processing of OB 83.

10.5.4 Reconfiguration Procedure

10.5.4.1 Using a Previously Unused Channel

Procedure

1. Change the hardware configuration and download it to the CPU.
2. Save your project.
3. Make the change to the wiring.
4. Change the user program and download it to the CPU.

10.5.4.2 Reconfiguring an already used channel.

Introduction

The procedure depends on whether or not changes to the user program and the associated hardware are necessary due to the re-configuration. The individual cases are described below.

Procedure without change

The user program need not be changed as a result of re-configuration. This is the case, for example, when you change an alarm limit or when you disable the diagnostic interrupt.

- Change the hardware configuration and download it to the CPU.

Procedure for changing the user program

The user program need not be changed as a result of the re-configuration. This is the case, for example, when you change the measuring range for a channel of an analog input module and when you compare the associated analog value with a constant in your program. The constant must be adapted in this case.

1. Set the values of the channel being re-configured to simulation (in the associated driver).
2. Change the hardware configuration and download it to the CPU.
3. Save your project.
4. If necessary, adapt the user program to the changed channel and download it to the CPU. Cancel the simulation for the re-configured channel (in the corresponding driver).

Procedure for changing the user program and the hardware

The user program and the hardware must be changed as a result of the re-configuration. This is the case, for example, when you re-configure an input channel from "0 to 20 mA" to "0 to 10 V".

1. Set the values of the channel being re-configured to simulation (in the associated driver).
2. Change the associated hardware.
3. Change the hardware configuration and download it to the CPU.
4. Save your project.
5. If necessary, adapt the user program to the changed channel and download it to the CPU. Cancel the simulation for the re-configured channel (in the corresponding driver).

Procedure for changing the address area of the ET 200iSP electronic module

This is the case, for example, when you use IEEE values of a HART electronic module.

Follow these steps:

1. Set the values of the module being re-configured to simulation (in the associated driver).
2. Delete the module in the hardware configuration and download it to the CPU.
3. Insert the module once again and configure it for your configuration as needed.
4. Download the hardware configuration to the CPU.
5. Save your project.
6. If necessary, adapt the user program to the changed module and download it to the CPU.
7. Cancel the simulation for the re-configured module (at the associated driver).

10.5.4.3 Delete an already used channel.

Procedure

You do not need to change the hardware configuration if you no longer need a channel previously used.

1. Change the user program so that the channel to be removed is no longer evaluated, and download it to the CPU.
2. Change the hardware configuration and download it to the CPU.
3. Save your project.
4. Change the corresponding hardware (remove sensor or actuator, etc.).

10.6 Notes on Reconfiguration in RUN Mode Depending on the I/O

10.6.1 DP slaves

Principle

If you are planning system changes in RUN using CiR, you must ensure the following when planning the system:

- Provide a sufficient number of branching points for spur lines or isolating points (spur lines are not permitted when using a transmission rate of 12 Mbit/s).
- You must configure ET 200M stations with an active backplane bus. Fit all the bus modules required if possible, since bus modules must not be inserted or removed during operation.
- You must fit all the terminal modules required for the ET 200iSP. Then fit all the standby modules required for all terminal modules assigned to the standby area.
- Terminate both ends of PROFIBUS DP bus cables using active bus terminating elements in order to ensure proper termination of the cables while you are reconfiguring the system.

Rules for CiR

The station number you assign to a newly added DP slave must be higher than the station number of all previously configured DP slaves.

Because the sum of the station number of the added DP slave and the number of the slaves that can still be added cannot exceed 125, we recommend selecting the station number of the added DP slave as follows:

Station number of the added DP slave = highest station number of all previously configured slaves + 1

If you select a higher station number for the added DP slave, the guaranteed number and maximum number of DP slaves that can still be added may be reduced by more than 1 under unfavorable circumstances. The following example will illustrate this:

The maximum station number of all previously configured slaves is 115. The maximum number of slaves that can still be added is 10. If you assign the station number 118 to the added slave, the maximum number of slaves that can still be added is then 7.

10.6.2 Modules in ET 200M Modular Slaves

Principle

When you are planning systems during operation via CiR, you must observe the following already at the planning stages:

- Install the ET 200M station with an active backplane bus.
- Always try to equip the station with the maximum number of bus modules, as you can not insert or remove a bus module during runtime.

Rules for System Modification During Runtime

- You may only add or remove modules immediately after the last existing module. Always avoid gaps between modules.
- In order to replace a module with a module of a different type in an existing CPU configuration, you must perform at least two downloads to the CPU: First, download the CPU configuration that no longer contains the modules you are going to remove. Secondly, download the configuration that contains the new modules.

10.6.3 Modules in ET200iSP Modular Slaves

Principle

When you are planning systems during operation via CiR, you must observe the following already at the planning stages of the ET200iSP stations:

- Install the ET200iSP station completely with terminal modules and end module.
- Equip the ET200iSP from the interface module, starting with the necessary electronics modules. Equip the remaining slots right up to the end module with the reserve modules.

Rules for System Modification During Runtime

Replace the reserve modules with the intended electronics modules. Start with the first reserve module that is located on the lowest slot (right next to the last electronics module). In doing so a gap may appear in each case, i.e. always replace just one reserve module with the electronics module.

10.7 Effects on the process when re-configuring in RUN

10.7.1 Effects on Operating System Functions During the CiR Synchronization Time

Principle

Operating system function	Effects
Process image update	locked. The process images of the inputs and outputs are held at their last value.
User program processing	All priority classes are locked, which means no OBs are processed. However, all outputs are kept at their current value. Any existing interrupt requirements are retained. Currently occurring interrupts are only received by the CPU once the SDB evaluation is complete.
Time system	The timers continue running. The cycles for time-of-day interrupt, cyclic interrupt and time-delay interrupt continue running but the interrupts themselves are locked. They are only received after the SDB evaluation. This means, for example, that only one interrupt can be added for each cyclic interrupt.
Programming device operation	Only the STOP command can be operated from the programming device. This means data record jobs are not possible.
External SSL information	Information functions are processed with a time delay.

10.7.2 Behavior of the CPU after download of the configuration in RUN

10.7.2.1 Overview

Sequence after download of the configuration in RUN

Once a modified configuration has been downloaded, CPU first checks whether your changes are admissible. If they are, it evaluates the relevant system data.

This evaluation affects operating system functions such as process image updates and user program processing. The details of these effects are set out below.

The fixed time for interpretation of system data by the CPU is referred to below as CiR synchronization time.

The CPU enters the event W#16#4318 in the diagnostic buffer at the start and the event W#16#4319 in the diagnostic buffer at the end of system data evaluation.

Note

If a Power Off occurs or the CPU switches to STOP during system data evaluation, only a warm restart or cold restart is then possible.

The CPU then starts OB 80 with the event W#16#350A and enters the duration of evaluation in the OB start information. This allows you to use this time in the control algorithms in your cyclic interrupt OBs, for example.

10.7.2.2 Error displays

LED Displays during Reconfiguration

The INTF LED is lit from the start of the consistency check until completion of SDB evaluation. The light will remain on if module parameters are being changed.

After the CiR operation, the preset configuration and the actual configuration will differ (the preset configuration is changed after you have downloaded a configuration change to the CPU) and the EXTF LED is lit. If your modified configuration includes added slaves, the BUS1F LED or the BUS2F LED will also flash. The BUS1F LED, BUS2F LED and EXTF LED will be switched off after you have made the corresponding hardware changes.

Plant changes during redundant operation - H-CiR 11

11.1 The H-CiR wizard

The H-CiR wizard helps you with plant changes during redundant operation. It allows you to download a modified configuration without interrupting operation.

Note

Using the H-CiR wizard

Use the H-CiR wizard for H-CiR operations. This minimizes the risk of inconsistencies and avoids bumps during a plant change.

You can open the H-CiR wizard in HW Config.

Proceed as follows:

1. Make the desired changes/extensions and update the configuration accordingly in HW Config.
2. In HW Config, click on the "Download to module" button.
3. Select "Download station configuration in RUN mode".
4. Select one of the redundant CPUs.
5. Select "Automatically continue".
   This runs the first steps in the plant change process automatically.
6. Click "Continue".
   - The CPU is selected
   - The standby CPU may be switched to RUN by a warm restart.
   - The required system data blocks are generated.
   - The selected CPU is switched to RUN.
   - The new hardware configuration is downloaded to the CPU.
7. Click "Continue".
   - The system switches to the CPU with the modified configuration.
   - The current standby CPU is switched to RUN.
8. Close the dialog box.

Note

Keep changes to a manageable level and do not make changes to multiple interfaces at the same time.

11.2 Replacing central components

Which central components can be modified?

The following changes can be made to the hardware configuration during operation:

- Changing certain CPU parameters
- Re-configuring a module
- Assigning a module to another process image partition
- Upgrading the CPU version
- Upgrading to a higher product level or a current version of the components used.
- Add or remove modules in the central controllers.

For all changes, please observe the rules for the assembly of an H station.

Changes to the hardware configuration

With a few exceptions, all elements of the configuration can be modified during operation. Configuration changes will usually also affect the user program.

The following must not be changed by means of system modifications during runtime:

- Certain CPU parameters (for details, please refer to the relevant sections)
- The transmission rate (baud rate) of redundant DP master systems
- S7 and S7 H connections

Note

With switched I/O: Complete all changes to one of the redundant DP master systems before you make changes to the second DP master system.

11.3 Motivation for H-CiR via PROFIBUS DP

In addition to the options described in section Replacement of failed components during redundant operation (Page 165) for replacing failed components during operation, a system change can also be performed in redundant operation for the CPU 410SIS without having to interrupt the active program.

The procedure and scope depend on the operating mode of the CPU.

The procedures described below for making changes during operation are each created in such a way that they start from the redundant system state (see Chapter The system states of the AS 410H SIS (Page 79)) and have as their objective a return to redundant system state.

Note

Keep strictly to the rules described in this section with regard to modifications of the system in runtime. If you contravene one or more rules, the response of the fault-tolerant system can result in its availability being restricted or even failure of the entire automation system.

Only perform a plant change in runtime if there is no redundancy error, i.e. if the REDF LED is not on. The automation system may otherwise fail.

The cause of a redundancy error is listed in the diagnostics buffer.

Safety-related components are not taken into account in this description. For more information on handling fail-safe systems refer to the *S7 F/FH Systems - Configuring and Programming* manual.

Requirements

For switched I/O to be expanded during operation, the following points must be taken into account already at the system planning stage:

- In both cables of a redundant DP master system, sufficient numbers of branching points are to be provided for spur lines or isolating points (spur lines are not permitted for transmission rates of 12 Mbit/s). These branching points can be spaced or implemented at any points that can be accessed easily.
- Both cables must be uniquely identified so that the line which is currently active is not accidentally cut off. This identification should be visible not only at the end points of a line, but also at each possible new connection point. Different colored cables are especially suitable for this.
- Modular DP slave stations (ET 200M) and Y links must always be installed with an active backplane bus and fitted with all the bus modules required wherever possible, because bus modules are not permitted to be installed and removed during operation.
- The configuration of the terminal modules with the ET200iSP should have sufficient reserves and be fitted with unconfigured standby modules.
- Always terminate both ends of PROFIBUS DP bus cables using active bus terminating elements in order to ensure proper termination of the cables while you are reconfiguring the system.

Modifications to the user program and the connection configuration

The modifications to the user program and connection configuration are loaded into the target system in redundant system state. More detailed information can be found in the *PCS 7, Configuration Manual*.

See also

Modifying the System during Operation via CiR (https://support.industry.siemens.com/cs/ww/en/view/14044916)

11.4 Permitted changes over PROFIBUS DP

How is hardware modified?

If the hardware components concerned can be unplugged or plugging in live, the hardware modification can be carried out in the redundant system state. However, the fault-tolerant system must be temporarily switched to solo mode as downloading a modified hardware configuration in the redundant system state would cause the fault-tolerant system to stop. In solo operation, the process is then controlled by only one CPU while the desired configuration changes are made to the other CPU.

Note

You can either remove or add modules during a hardware change. If you want to alter your fault-tolerant system by removing some modules and adding others, you will need to make two hardware changes.

Note

Always download configuration changes to the CPU using the "Configure hardware" function.

Synchronization link

Following all hardware changes, ensure that the synchronization link between both CPUs is restored **before** you start or switch on the standby CPU. When the power supplies of the CPUs are switched on, the IFM1F and IFM2F LEDs, which are used to indicate module interface errors, must **go out** on both CPUs.

Which distributed components can be modified?

The following changes can be made to the hardware configuration during operation:

- Adding or removing components of the distributed I/O such as
  - DP slaves with redundant interface module (e.g. ET 200M, ET 200iSP and Y link)
  - One-sided DP slaves
  - Modules in modular DP slaves (ET 200M and ET 200iSP)
- Upgrading to a higher product version or a current version of components used such as DP-IMs.

Special features

When you use an IM 153-2, active bus modules can only be plugged in if the power supply is off.

Preparations

To minimize the time during which the fault-tolerant system has to run in solo mode, please note the following **before** starting a hardware change:

Modules which are plugged but not configured yet do not have any unwanted influence on the process.

See also

Rules for assembly of an AS 410H SIS (Page 19)

Connection of two-channel I/O to the PROFIBUS DP interface (Page 53)

11.5 Adding components

Starting situation

You have ensured that the CPU parameters (for example the monitoring times) are compatible with the planned new program. You may first need to modify the CPU parameters (see Editing CPU parameters (Page 159)).

The AS 410H SIS operates in redundant system state.

Procedure

To add hardware components to an AS 410H SIS under SIMATIC SIS compact, follow the steps listed below. Details of each step are described in a section.

Step	What has to be done?	See section
1	Modify hardware	Modify hardware (Page 152)
2	Change hardware configuration offline	Change hardware configuration offline (Page 152)
3	Access H-CiR wizard	Opening the H-CiR wizard (Page 153)
4	Modify and download the user program	Modify and download the user program (Page 154)

Exceptions

This overall procedure for changing a plant does not apply in the following case:

- For use of free channels on an existing module

11.5.1 Modify hardware

Starting situation

The fault-tolerant system is operating in the redundant system state.

Procedure

1. Add the new components to the system.
   - Insert new central modules in the rack.
   - Insert new modules in existing modular DP stations
   - Add new DP stations to existing DP master systems.
2. Connect the required sensors and actuators to the new components.

Result

Inserting modules that are not yet configured does not affect the user program. The same applies to the addition of DP stations.

The fault-tolerant system continues to operate in the redundant system state.

New components are not yet addressed.

11.5.2 Change hardware configuration offline

Starting situation

The fault-tolerant system is operating in redundant system state.

Procedure

1. Perform all changes to the hardware configuration related to the added hardware offline. Assign appropriate symbols for the new channels to be used.
2. Compile the new hardware configuration but do **not yet** download it to the PLC.

Result

The changed hardware configuration is on the programming device / ES. The target system continues operation with the old configuration in redundant system state.

11.5.3 Opening the H-CiR wizard

The next steps, except for changing and loading the user program, are performed by the H-CiR wizard.

Reaction of the I/O to the new master CPU

While the previous master CPU is still in STOP, the I/O reacts to the new master CPU as follows:

Type of I/O	One-sided I/O of the previous master CPU	One-sided I/O of the new master CPU	Switched I/O
Added I/O modules	Not yet accessed by the CPU.	Configured and updated by the CPU. Driver blocks are not yet available. Any occurring process or diagnostic alarms are detected, but not reported.	
I/O modules still available	No longer accessed by the CPU. Output modules have the configured substitute or holding values.	Newly configured and updated by the CPU.	Continue working without interruption.
Added DP stations	Not yet accessed by the CPU.	like I/O modules to be added (see above)	

Reaction of the I/O to entering redundant mode

The fault-tolerant system is in redundant mode with the new configuration. The I/O reacts as follows:

Type of I/O	One-sided I/O of the reserve CPU	One-sided I/O of the master CPU	Switched I/O
Added I/O modules	Configured and updated by the CPU. Driver blocks are not yet available. Any occurring alarms are not reported.	Updated by the CPU. Driver blocks are not yet available. Any occurring process or diagnostic alarms are detected, but not reported.	
I/O modules still available	Newly configured and updated by the CPU.	Continue working without interruption.	
Added DP stations	like I/O modules to be added (see above)	Driver blocks are not yet available. Any occurring alarms are not reported.	

Reaction to exceeding the monitoring times

When one of the monitored timers exceeds the configured maximum value, the update is aborted and no master switchover is performed. The H system remains in solo mode with the previous master CPU and attempts to later perform the master switchover under certain conditions. For details, refer to the section Time monitoring (Page 90).

11.5.4 Modify and download the user program

Starting situation

The H system is operating with the new hardware configuration in redundant system state.

Note

The following program changes are not possible in redundant system state and result in a switch to STOP system state (both CPUs in STOP):

- Structural modifications to global DBs.
- Compression of the CFC user program

Before the entire program is recompiled and reloaded due to such modifications the parameter values must be read back into the CFC, otherwise the modifications to the block parameters could be lost. You will find more detailed information on this topic in the *CFC for S7, Continuous Function Chart* manual.

Procedure

1. Adapt the program to the new hardware configuration. You can add the following components:
   - CFCs
   - Blocks in existing charts
   - Connections and parameter settings
2. Configure the added channel drivers and connect them to the newly assigned symbols (see section Change hardware configuration offline (Page 152)).
3. In SIMATIC Manager, select the charts folder and choose the "Options > Charts > Generate Module Drivers" menu command.
4. Compile only the modifications in the charts and download them to the target system.

Result

The H system operates all plant hardware with the new user program in redundant system state.

11.5.5 Use of free channels on an existing module

The use of previously free channels of an I/O module depends mainly on the fact if the module can be configured or not.

Non-configurable modules

Free channels can be switched and used in the user program at any time in case of non-configurable modules.

Configurable modules

The hardware configuration first has to be matched to the used sensors or actuators for configurable modules. This step usually requires a new configuration of the entire module in most cases.

This means an uninterrupted operation of the respective modules is no longer possible:

- One-sided output modules briefly output 0 during this time (instead of the configured substitute or hold values).
- Modules in switched DP stations are not reconfigured when you switch over to the CPU with the modified configuration.

Proceed as follows to change the channel use:

- First, the affected module is completely removed from the hardware configuration and the user program. But it can remain inserted in the DP station. The module drivers must not be removed.
- After this, the module with the modified use is added again to the hardware configuration and the user program.

Note

Between these two switchover actions, affected modules are not accessed; affected output modules have a value of 0. The existing channel drivers in the user program hold their signals.

If this behavior is unacceptable for the process to be controlled, there is no other way to use previously free channels. In this case you must install additional modules to expand the system.

11.6 Removal of components

Starting situation

You have ensured that the CPU parameters (for example the monitoring times) are compatible with the planned new program. You may first need to modify the CPU parameters (see Editing CPU parameters (Page 159)).

The modules to be removed and their connected sensors and actuators are no longer of any significance to the process being controlled. The AS 410H SIS operates in redundant system state.

Procedure

To remove hardware components from an AS 410H SIS under SIMATIC SIS compact, following the steps listed below. Details of each step are described in a subsection.

Step	What to do?	See section
1	Change hardware configuration offline	Change hardware configuration offline (Page 156)
2	Modify and download the user program	Modify and download the user program (Page 157)
3	Access H-CiR wizard	Opening the H-CiR wizard (Page 157)
4	Modify hardware	Modify hardware (Page 158)

11.6.1 Change hardware configuration offline

Starting situation

The fault-tolerant system is operating in the redundant system state.

Procedure

1. Perform offline only the configuration modifications relating to the hardware being removed. As you do, delete the icons to the channels that are no longer used.
2. Compile the new hardware configuration but do **not yet** download it to the PLC.

Result

The modified hardware configuration is available in the PG/ES. The target system continues operation with the old configuration in redundant system mode.

11.6.2 Modify and download the user program

Starting situation

The fault-tolerant system is operating in redundant system mode.

⚠ CAUTION

The following program modifications are not possible in redundant system mode and result in the system mode Stop (both CPUs in STOP mode):

- Structural modifications to an FB interface or the FB instance data.
- Structural modifications to global DBs.
- Compression of the CFC user program.

Before the entire program is recompiled and reloaded due to such modifications the parameter values must be read back into the CFC, otherwise the modifications to the block parameters could be lost. You will find more detailed information on this topic in the *CFC for S7, Continuous Function Chart* manual.

Procedure

1. Edit only the program elements related to the hardware removal. You can delete the following components:
   - CFCs and SFCs
   - Blocks in existing charts
   - Channel drivers, interconnections and parameter settings
2. In SIMATIC Manager, select the charts folder and choose the "Options > Charts > Generate Module Drivers" menu command.
   This removes the driver blocks that are no longer required.
3. Compile only the modifications in the charts and download them to the target system.

Note

Until an FC is called the first time, the value of its output is undefined. This must be taken into account in the interconnection of the FC outputs.

Result

The fault-tolerant system continues to operate in redundant system mode. The modified user program will no longer attempt to access the hardware being removed.

11.6.3 Opening the H-CiR wizard

The next steps, except for the conversion of the hardware, are performed by the H-CiR wizard.

Reaction of the I/O to the new master CPU

While the previous master CPU is still in STOP, the I/O reacts to the new master CPU as follows:

Type of I/O	One-sided I/O of the previous master CPU	One-sided I/O of the new master CPU	Switched I/O
The I/O modules to be removed[1)]	No longer accessed by the CPU. Driver blocks are no longer available.		
I/O modules still available	No longer accessed by the CPU. Output modules have the configured substitute or holding values.	Newly configured and updated by the CPU.	Continue working without interruption.
The DP stations to be removed	like I/O modules to be removed (see above)		
1) No longer included in the hardware configuration, but still plugged			

Reaction of the I/O to entering redundant mode

The fault-tolerant system is in redundant mode with the new configuration. The I/O reacts as follows:

Type of I/O	One-sided I/O of the reserve CPU	One-sided I/O of the master CPU	Switched I/O
The I/O modules to be removed[1)]	No longer accessed by the CPU. Driver blocks are no longer available.		
I/O modules still available	Newly configured and updated by the CPU.	Continue working without interruption.	
The DP stations to be removed	like I/O modules to be removed (see above)		
1) No longer included in the hardware configuration, but still plugged			

Reaction to exceeding the monitoring times

When one of the monitored timers exceeds the configured maximum value, the update is aborted and no master switchover is performed. The H system remains in solo mode with the previous master CPU and attempts to later perform the master switchover under certain conditions. For details, refer to the section Time monitoring (Page 90).

11.6.4 Modify hardware

Starting situation

The fault-tolerant system is operating with the new hardware configuration in the redundant system state.

Procedure

1. Disconnect all the sensors and actuators from the components you want to remove.
2. Unplug modules of the one-sided I/Os that are no longer required from the racks.
3. Unplug components that are no longer required from the modular DP stations.
4. Remove DP stations that are no longer required from the DP master systems.

Note

With switched I/O: Complete all changes to **one** line of the redundant DP master system before you make changes to the second line.

Result

Unplugging modules and I/O modules that have been removed from the configuration does not affect the user program. The same applies to removal of DP stations.

The fault-tolerant system continues to operate in the redundant system state.

11.7 Editing CPU parameters

11.7.1 Editing CPU parameters

Only certain CPU parameters (object properties) can be edited in operation. These are highlighted in the screen forms by blue text. If you have set blue as the color for dialog box text on the Windows Control Panel, the editable parameters are indicated in black characters.

Note

If you edit any protected parameters, the system will reject any attempt to changeover to the CPU containing those modified parameters. The event W#16#5966 is written to the diagnostic buffer. and you will then have to restore the wrongly changed parameters in the parameter configuration to their last valid values.

Table 11-1 Modifiable CPU parameters

Tab	Editable parameter
Startup	Monitoring time for signaling readiness by modules
	Monitoring time for transferring parameters to modules
Cycle/clock memory	Cycle load due to communication
Memory	Local data for the individual priority classes
Time-of-day interrupts (for each time-of-day interrupt OB)	"Active" checkbox
	"Execution" list box

Tab	Editable parameter
	Starting date
	Time
Watchdog interrupt (for each watchdog interrupt OB)	Execution
	Phase offset
Diagnostics/clock	Correction factor
Security	Security level and password
H parameter	Test cycle time
	Maximum cycle time extension
	Maximum communication delay
	Maximum inhibit time for priority classes > 15
	Minimum I/O retention time

The selected new values should match both the currently loaded and the planned new user program.

Starting situation

The fault-tolerant system is operating in redundant system mode.

Procedure

To edit the CPU parameters of a fault-tolerant system, follow the steps outlined below. Details of each step are described in a subsection.

Step	What to do?	See section
1	Editing CPU parameters offline	Changing CPU parameters offline (Page 160)
2	Open the H-CiR wizard	Opening the H-CiR wizard (Page 161)

11.7.2 Changing CPU parameters offline

Starting situation

The fault-tolerant system is operating in redundant system mode.

Procedure

1. Edit the relevant CPU properties offline in HW Config.
2. Compile the new hardware configuration, but do **not** load it into the target system just yet.

Result

The modified hardware configuration is in the PG/ES. The target system continues operation with the old configuration in redundant system mode.

11.7.3 Opening the H-CiR wizard

The H-CiR wizard takes over the next step.

Reaction of the I/O to the new master CPU

While the previous master CPU is still in STOP, the I/O reacts to the new master CPU as follows:

Type of I/O	One-sided I/O of the previous master CPU	One-sided I/O of the new master CPU	Switched I/O
I/O modules	No longer accessed by the CPU. Output modules have the configured substitute or holding values.	Newly configured and updated by the CPU.	Continue working without interruption.

Reaction of the I/O to entering redundant mode

The fault-tolerant system is in redundant mode with the new configuration. The I/O reacts as follows:

Type of I/O	One-sided I/O of the reserve CPU	One-sided I/O of the master CPU	Switched I/O
I/O modules	Newly configured and updated by the CPU.	Continue working without interruption.	

Reaction to exceeding the monitoring times

When one of the monitored timers exceeds the configured maximum value, the update is aborted and no master switchover is performed. The H system remains in solo mode with the previous master CPU and attempts to later perform the master switchover under certain conditions. For details, refer to the section Time monitoring (Page 90).

11.8 Re-parameterization of a module

11.8.1 Re-parameterization of a module

Refer to the information text in the "Hardware Catalog" window to determine which modules can be reconfigured during operation. The specific reactions of individual modules are described in the respective technical documentation.

Note

If you edit any protected parameters, the system will reject any attempt to changeover to the CPU containing those modified parameters. In this case, the event W#16#5966 is entered in the diagnostic buffer for PROFIBUS DP, and you will then have to restore the wrongly changed parameters in the parameter configuration to their last valid values.

The selected new values must match the current and the planned user program.

Starting situation

The fault-tolerant system is operating in the redundant system state.

Procedure

To change the parameters of modules of an H system, perform the steps listed below. Details of each step are described in a subsection.

Step	What to do?	See section
1	Editing parameters offline	Editing parameters offline (Page 162)
2	Access H-CiR wizard	Opening the H-CiR wizard (Page 163)

11.8.2 Editing parameters offline

Starting situation

The fault-tolerant system is operating in redundant system mode.

Procedure

1. Edit the module parameters offline in HW Config.
2. Compile the new hardware configuration, but do **not** load it into the target system just yet.

Result

The modified hardware configuration is in the PG/ES. The target system continues operation with the old configuration in redundant system mode.

11.8.3 Opening the H-CiR wizard

The H-CiR wizard takes over the next step.

Reaction of the I/O to the new master CPU

While the previous master CPU is still in STOP, the I/O reacts to the new master CPU as follows:

Type of I/O	One-sided I/O of the previous master CPU	One-sided I/O of the new master CPU	Switched I/O
I/O modules	No longer accessed by the CPU. Output modules have the configured substitute or holding values.	Newly configured and updated by the CPU.	Continue working without interruption.

Reaction of the I/O to entering redundant mode

The fault-tolerant system is in redundant mode with the new configuration. The I/O reacts as follows:

Type of I/O	One-sided I/O of the reserve CPU	One-sided I/O of the master CPU	Switched I/O
I/O modules	Newly configured and updated by the CPU.	Continue working without interruption.	

Reaction to exceeding the monitoring times

When one of the monitored timers exceeds the configured maximum value, the update is aborted and no master switchover is performed. The H system remains in solo mode with the previous master CPU and attempts to later perform the master switchover under certain conditions. For details, refer to the section Time monitoring (Page 90).

Replacement of failed components during redundant operation

12

Note

Components in redundant mode

Only components with the same product version, the same article number and the same version can be operated redundantly.
If a component is no longer available as spare part, you must replace both components so that this condition is met once again.

12.1 Replacement of central components

12.1.1 Replacement of a CPU during redundant operation

Starting situation for replacement of the CPU

Failure	How does the system react?
The S7-400H is in redundant system mode and a **CPU** fails.	• The partner CPU switches to single mode. • The partner CPU reports the event in the diagnostic buffer and in OB 72.

Requirements for replacement

The module replacement described below is possible only if the "new" CPU

- has the same operating system version as the failed CPU and
- if it is equipped with the same system expansion card as the failed CPU.

Note

New CPUs are always shipped with the latest operating system version. If this differs from the version of the operating system of the remaining CPU, you will have to equip the new CPU with the same version of the operating system. Download the required operating system via HW Config with "PLC -> Update Firmware", see section Updating firmware in stand-alone operation (Page 116).

CAUTION

Caution when replacing a CPU

If you reuse a CPU that has previously been used at a different location, ensure that the contents backed up in the load memory cannot pose a hazard at the new point of use. Reset the CPU to factory settings if its previous use is unknown.

See Resetting the CPU 410SIS to delivery condition (reset to factory setting) (Page 112)

Procedure

Note

Replacing an SEC

You can replace an SEC by following the same procedure as described above. Here you do not replace the CPU in step 2, but replace the SEC with an SEC of the same size and then reinstall the CPU.

Follow the steps below to **replace a CPU**:

Step	What to do?	How does the system react?
1	Turn off the power supply module.	• The entire subsystem is switched off (system operates in single mode).
2	Ensure that an SEC E4MB is inserted into the new CPU.	-
3	Replace the CPU. Make sure the rack number is set correctly on the CPU.	–
4	Insert the synchronization modules.	–
5	Plug in the fiber-optic cable connections of the synchronization modules.	–
6	Switch the power supply module on again.	• CPU runs the self-tests and changes to STOP.
7	Perform a CPU memory reset on the replaced CPU.	–
8	Start the replaced CPU (for example, STOP-RUN or Start using the PG).	• The CPU performs an automatic LINK-UP and UPDATE. • The CPU changes to RUN and operates as the standby CPU.

⚠ CAUTION

Wiring synchronization modules crosswise

If you wire synchronization modules crosswise, i.e. the IF1 interface of the first CPU with the IF2 interface of the second CPU and vice versa, the two CPUs take over the master role and the system will now function properly. The LEDs IFM 1 and IFM 2 are lit on both CPUs.

Make sure that you connect the IF1 interface of the first CPU with the IF1 interface of the second CPU and the IF2 interface of the first CPU with the IF2 interface of the second CPU when you replace the CPU. Mark the fiber-optic cables before the replacement, if necessary.

12.1.2 Replacement of a power supply module

Starting situation

Both CPUs are in RUN.

Failure	How does the system react?
The S7-400H is in redundant system mode and a power supply module fails.	• The partner CPU switches to single mode. • The partner CPU reports the event in the diagnostic buffer and in OB 72.

Procedure

If you are replacing a power module in the central controller, follow these steps:

Step	What to do?	How does the system react?
1	Turn off the power supply (24 V DC for PS 405 or 120/230 V AC for PS 407).	• The entire subsystem is switched off (system operates in single mode).
2	Replace the module.	–
3	Switch the power supply module on again.	• The CPU executes the self-tests. • The CPU performs an automatic LINK-UP and UPDATE. • The CPU changes to RUN (redundant system mode) and operates as reserve CPU.

Note

Redundant power supply

If you use a redundant power supply with two PS 407 10A R or PS 405 10A R, two power supply modules are assigned to one CPU 410H SIS. The associated CPU continues to run if one of the redundant power supply modules fails. The defective part can be replaced during operation.

Other power supply modules

If the failure involves a power module in the I/O device, the failure is signaled as a station failure (distributed). In this case, simply switch off the power supply to the power supply module concerned.

12.1.3 Replacement of synchronization module or fiber-optic cable

In this section, you will see three different error scenarios:

- Failure of a synchronization module or fiber-optic cable
- Successive failure of both synchronization modules or fiber-optic cables
- Simultaneous failure of both fiber-optic cables

The CPU indicates by means of LEDs and diagnostics whether the lower or upper redundant link has failed. After the defective parts (fiber-optic cable or synchronization module) have been replaced, LEDs IFM1F and IFM2F must go out.

If one of the IFM LEDs continues to be lit even after you have replaced the relevant synchronization modules, the synchronization cables and even the standby CPU, there is an error in the master CPU. In this case, you can, however, switch to the standby CPU by selecting the "via only one intact redundancy link" option in the "Switch" STEP 7 dialog box.

Starting situation

Failure	How does the system react?
Failure of a fiber-optic cable or synchronization module: The S7-400H is in the redundant system state and a fiber-optic cable or synchronization module fails. See also chapter Synchronization modules for the CPU 410SIS. (Page 175).	• Master CPU reports the event in the diagnostic buffer and through OB 72 or OB 82. • The standby CPU switches to ERROR-SEARCH operating state for a few minutes. If the error is eliminated during this time, the standby CPU switches to redundant system mode, otherwise it switches to STOP. • One of the two LEDs Link1 OK or Link2 OK is lit One of the two LEDs IFM1F or IFM2F is lit

Procedure

Follow the steps below to replace a fiber-optic cable:

Step	What to do?	How does the system react?
1	Look for the cause of the error along the path for which the IFMxF LEDs are lit on both CPUs: IFM1F: Upper sync modules in CPU rack 0 or rack 1 or corresponding synchronization cable. IFM2F: Lower sync modules in CPU rack 0 or rack 1 or corresponding synchronization cable. First, check the fiber-optic cable.	-
2	If the fiber-optic cable is defective, replace it.	The IFMxF LEDs on both CPUs go out.

Follow the steps below to replace a synchronization module:

Step	What to do?	How does the system react?
1	Replace the synchronization module on the CPU on which the LED Linkx-OK is still lit.	-
2	Plug in the fiber-optic cable connections of the synchronization modules.	• The LEDs IFMxF go out. If the LED should not go out, you must replace the synchronization module on the other CPU. • Both CPUs report the event in the diagnostic buffer
3	Start the standby CPU	The system status now changes to Redundant mode.

Starting situation

Failure	How does the system react?
Simultaneous failure of both fiber-optic cables The S7-400H is in the redundant system state and **both** fiber-optic cables fail.	• Both CPUs report the event in the diagnostic buffer and via OB 72. • Both CPUs become master CPU and remain in RUN. • The LEDs IFM1F and IFM2F are lit on both CPUs.

Procedure

The described double failure results in loss of redundancy and partial or complete failure of switched DP I/O. In this event proceed as follows:

Step	What to do?	How does the system react?
1	Switch off one subsystem.	-
2	Replace the faulty components.	-

Step	What to do?	How does the system react?
3	Turn the subsystem back on.	• LEDs IFM1F and IFMF2F go off. The LED MSTR of the switched on subsystem goes out.
4	Start the CPU.	• The CPU performs an automatic LINK-UP and UPDATE. • The CPU switches to RUN (redundant system state) and operates as standby CPU.

12.2 Replacement of components of the distributed I/O on PROFIBUS DP

Which components can be replaced?

The following components of the distributed I/Os can be replaced during operation:

- PROFIBUS DP interface module IM 153-2
- PROFIBUS DP slave
- PROFIBUS DP cable
- Signal modules in a distributed station

Replacing signal modules

To replace signal modules, follow these steps:

Step	What to do?	How does the system react?
1	Disconnect the module from its load current supply.	
2	Remove the failed module (in RUN mode).	• Both CPUs generate a remove/insert interrupt and enter the event in the diagnostic buffer and the system status list.
3	Disconnect the front connector and wiring.	-
4	Plug the front connector into the new module.	-
5	Insert the new module.	• Both CPUs generate a remove/insert interrupt and enter the event in the diagnostic buffer and the system status list. • Parameters are assigned automatically to the module by the CPU concerned and the module is addressed again.

12.2.1 Replacement of a redundant PROFIBUS DP interface module

Starting situation

Failure	How does the system react?
The S7-400H is in redundant system state, and a PROFIBUS DP interface module IM 153-2 fails.	Both CPUs report the event in the diagnostic buffer and via OB 70.

Replacement procedure

Proceed as follows to replace the PROFIBUS DP interface module:

Step	What has to be done?	How does the system react?
1	Turn off the supply for the affected DP interface module.	–
2	Remove the bus connector.	–
3	Insert the new PROFIBUS DP interface module and turn the power supply back on.	–
4	Plug the bus connector back in.	• The CPUs process the I/O redundancy error OB 70 (outgoing event) synchronized with each other. • Redundant access to the station by the system is now possible again.

12.2.2 Replacement of a PROFIBUS DP slave

Starting situation

Failure	How does the system react?
The S7-400H is in redundant system state and a DP slave fails.	Both CPUs signal the event in the diagnostics buffer and via a corresponding OB 86.

Procedure

Proceed as follows to replace a DP slave:

Step	What to do?	How does the system react?
1	Turn off the supply for the DP slave.	With one-sided I/O: OB 86 and OB85 are called for access errors during the PA update. With switched I/O: OB70 is called (incoming event), the LED REDF lights up.
2	Remove the bus connector.	–

Step	What to do?	How does the system react?
3	Replace the DP slave.	–
4	Plug the bus connector back in and turn the power supply back on.	• The CPUs process the rack failure OB 86 synchronously (outgoing event). • With switched I/O: OB70 is called (outgoing event), the LED REDF goes out. • The associated DP master can address the DP slave.

12.2.3 Replacement of PROFIBUS DP cables

Starting situation

Failure	How does the system react?
The S7-400H is in redundant system mode and the PROFIBUS DP cable is defective.	• With single-channel one-sided I/O: Rack failure OB (OB 86) is started (incoming event). The DP master can no longer process connected DP slaves (station failure). The LED BUS1F flashes. • With switched I/O: I/O redundancy error OB (OB 70) is started (incoming event). DP slaves are addressed via the DP master of the partner. The LED BUS1F and the LED REDF are flashing.

Replacement procedure

Proceed as follows to replace PROFIBUS DP cables:

Step	What to do?	How does the system react?
1	Check the cabling and localize the interrupted PROFIBUS DP cable.	–
2	Replace the defective cable.	The CPUs process the error OBs synchronized with each other • With one-sided I/O: Rack failure OB 86 (outgoing event) The LED BUS1F goes out. The DP slaves can be addressed via the DP master system. • With switched I/O: I/O redundancy error OB 70 (outgoing event). The DP slaves can be addressed via both DP master systems. The LED BUS1F and the LED REDF go out.

Synchronization modules 13

13.1 Synchronization modules for the CPU 410SIS.

Function of the synchronization modules

Synchronization modules are used for the synchronization connection of two redundant CPUs 410SIS. You need two synchronization modules per CPU, which you connect in pairs using fiber-optic cable.

The system supports hot-swapping of synchronization modules, and so allows you to influence the repair response of the fault-tolerant systems and to control the failure of the redundant connection without stopping the plant.

The diagnostics process for synchronization modules is based in parts on the maintenance concept familiar from PROFINET IO. Required maintenance is not signaled.

If you remove a synchronization module in redundant system mode, there is a loss of synchronization. The standby CPU switches to ERROR-SEARCH operating state for a few minutes. If the new synchronization module is inserted and the redundant link is reestablished during this time, the standby CPU then switches to redundant system mode; otherwise it switches to STOP.

Once you have inserted the new synchronization module and reestablished the redundant link, you must restart the standby CPU, if necessary.

Distance between the S7–400H CPUs

The following types of synchronization modules are available:

Article No.	Maximum distance between the CPUs
6ES7 960–1AA06–0XA0	10 m
6ES7 960-1AA08-0XA0	10 m, use up to 70°C possible
6ES7 960–1AB06–0XA0	10 km

The synchronization set with article number 6ES7 656-7XX30-0XE0 includes 4 synchronization modules 6ES7 960–1AA06–0XA0 (10m) and 2 fiber-optic cables each 1m long.

Long synchronization cables may increase cycle times. This extension can have the factor 2 - 5 with a cable length of 10 km.

Note

You must use 4 synchronization modules of the same type in a fault-tolerant system.

Mechanical configuration

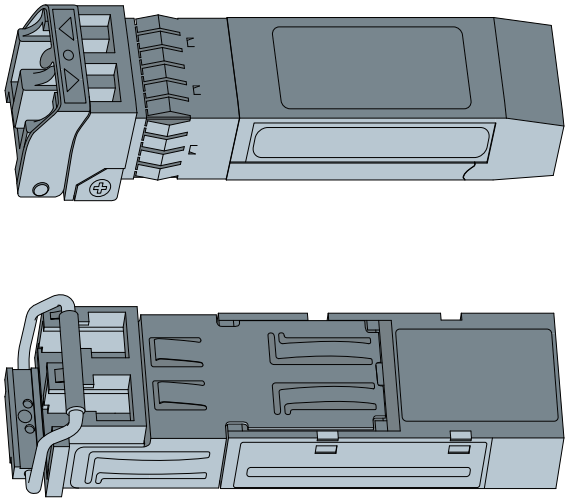


Figure 13-1 Synchronization modules 6ES7 960-1AA08-0XA0 and 6ES7 960-1Ax06-0xA0

CAUTION

Risk of injury.

The synchronization module is equipped with a laser system and is classified as a "CLASS 1 LASER PRODUCT" according to IEC 60825–1.

Avoid direct contact with the laser beam. Do not open the housing. Always observe the information provided in this manual, and keep the manual to hand as a reference.



OB 82

In redundant mode, the operating system of the CPU calls OB82 in case of a Snyc link fault.

You can display the following channel-specific diagnostic data in the Module state tab dialog for the selected synchronization module:

- Overtemperature
  The synchronization module is too hot.
- Fiber-optic error
  The sender of the electro-optical component has reached the end of its service life.
- Violation of lower limit
  The sent or received optical performance is low or too low.

- Violation of upper limit
  The sent or received optical performance is high or too high.
- Functional error of the network component
  The quality of the redundancy link between the CPUs (transmission distance including synchronization modules and fiber-optic cables) is reduced so that transmission errors are occurring frequently.

In redundant mode the OB82 is also called at Power Off/On or at a firmware update of the partner CPU. This does not indicate any problem with the synchronization link but is instead due to the fact that the synchronization modules are not emitting any light at this moment.

Fiber-optic interfaces of unused modules

Fiber-optic interfaces of unused modules must be blanked off during storage to protect the optical equipment. The plugs are in the synchronization module when shipped.

NOTICE
Reduced optical performance due to dirt Even small amounts of dirt in a fiber-optic interface adversely affect the quality of the signal transmission. This can lead to synchronization losses during operation. Protect the fiber-optic interfaces against dirt during storage and installation of the synchronization modules.

Wiring and inserting the synchronization module

1. Remove the dummy plug of the synchronization module.
2. Fold back the clip completely against the synchronization module.
3. Insert the synchronization module into the IF1 interface of the first fault-tolerant CPU until it snaps into place.
4. Insert the end of the fiber-optic cable into the synchronization module until it snaps into place.
5. Repeat steps 1 to 4 for the second synchronization module.
6. Repeat the process for the second fault-tolerant CPU.
   Connect the IF1 interface of the first CPU with the IF1 interface of the second CPU and the IF2 interface of the first CPU with the IF2 interface of the second CPU.

Note

Wiring synchronization modules crosswise

If you wire synchronization modules crosswise, i.e. the IF1 interface of the first CPU with the IF2 interface of the second CPU and vice versa, the two CPUs take over the master role and the system will now function properly. The LEDs IFM 1 and IFM 2 are lit on both CPUs.

Make sure that you connect the IF1 interface of the first CPU with the IF1 interface of the second CPU and the IF2 interface of the first CPU with the IF2 interface of the second CPU.

Removing the synchronization module

1. Slightly press the release of the fiber-optic cable and remove it from the synchronization module.
2. Fold the clip of the synchronization module to the front and remove the synchronization module from the fault-tolerant CPU interface.
3. Place the dummy plug on the synchronization module.
4. Repeat this procedure for all interfaces and both fault-tolerant CPUs.

Technical specifications

Technical specifications	6ES7960–1AA08–0XA0
Maximum distance between the CPUs	10 m
Supply voltage	3.3 V, supplied by the CPU
Current consumption	220 mA
Power loss	0.77 W
Wavelength of the optical transceivers	850 nm
Maximal permitted attenuation of the fiber-optic cable	7.5 dB
Maximum permitted difference in cable lengths	9 m
Dimensions W x H x D (mm)	13 x 14 x 58
Weight	0.014 kg

13.2 Installation of fiber-optic cables

Introduction

Fiber-optic cables may only be installed by trained and qualified personnel. Always observe the applicable rules and statutory regulations. The installation must be carried out with meticulous care, because faulty installations represent the most common source of error. Causes are:

- Kinking of the fiber-optic cable due to an insufficient bending radius.
- Crushing of the cable as a result of excess forces caused by persons treading on the cable, or by pinching, or by the load of other heavy cables.
- Overstretching due to high tensile forces.
- Damage on sharp edges etc.

Permitted bending radius for prefabricated cables

The following bending radii must not be undershot when installing the cables (6ES7960–1AA04–5xA0) prefabricated by SIEMENS.

- During installation: 88 mm (repeated)
- After installation: 59 mm (one-time)

Permitted bending radii for prefabricated cables

When you install self-assembled cables make sure to comply with the bending radii specified by the manufacturer. Note that approx. 50 mm of space is available for the connector and the fiber-optic cable under the front cover of the CPU and that no tight bending radius of a fiber-optic cable is therefore possible in the proximity of the connector.

Points to observe when installing the fiber-optic cables for the S7-400H synchronization link

Always route the two fiber-optic cables separately. This increases availability and protects the fiber-optic cables from potential double errors caused, for example, by interrupting both cables at the same time.

Always make sure the fiber-optic cables are connected to both CPUs before switching on the power supply or the system, otherwise the CPUs may process the user program as the master CPU.

If you are using fiber-optic cables that were not stored with blanking plugs at the connectors, note the following:

Clean the connectors, especially the optical surfaces, with a soft, clean and lint-free cloth before you use them.

Local quality assurance

Check the points outlined below before you install the fiber-optic cables:

- Does the delivered package contain the correct fiber-optic cables?
- Any visible transport damage to the product?
- Have you organized a suitable intermediate on-site storage for the fiber-optic cables?
- Does the category of the cables match the connecting components?

Check the attenuation of the fiber-optic cables after installation.

Storage of the fiber-optic cables

if you do not install the fiber-optic cable immediately after you received the package, it is advisable to store it in a dry location where it is protected from mechanical and thermal influences. Observe the permitted storage temperatures specified in the data sheet of the fiber-optic cable. You should not remove the fiber-optic cables from the original packaging until you are going to install them.

NOTICE
Reduced optical performance due to dirt Even slight amounts of dirt at the end of a fiber-optic cable will adversely affect its optical performance and thus the quality of the signal transmission. This can lead to synchronization losses during operation. Protect the ends of the fiber-optic cables against dirt during storing and installation. If the ends of the fiber-optic cable are covered when delivered, do not remove these covers.

Open installation, wall breakthroughs, cable ducts:

Note the points outlined below when you install fiber-optic cables:

- The fiber-optic cables may be installed in open locations, provided you can safely exclude any damage in those areas (vertical risers, connecting shafts, telecommunications switchboard rooms, etc.).
- Fiber-optic cables should be mounted on mounting rails (cable trays, wire mesh ducts) using cable ties. Take care not to crush the cable when you fasten it (see Pressure).
- Always deburr or round the edges of the breakthrough before you install the fiber-optic cable, in order to prevent damage to the sheathing when you pull in and fasten the cable.
- The bending radii must not be smaller than the value specified in the manufacturer's data sheet.
- The branching radii of the cable ducts must correspond to the specified bending radius of the fiber-optic cable.

Cable pull-in

Note the points below when pulling-in fiber-optic cables:

- Always observe the information on pull forces in the data sheet of the corresponding fiber-optic cable.
- Do not reel off any greater lengths when you pull in the cables.
- Install the fiber-optic cable directly from the cable drum wherever possible.
- Do not spool the fiber-optic cable sideways off the drum flange (risk of twisting).
- You should use a cable pulling sleeve to pull in the fiber-optic cable.

- Always observe the specified bending radii.
- Do not use any grease or oil-based lubricants.
  You may use the lubricants listed below to support the pulling-in of fiber-optic cables.
  - Yellow compound (Wire-Pulling, lubricant from Klein Tools; 51000)
  - Soft soap
  - Dishwashing liquid
  - Talcum powder
  - Detergent

Pressure

Do not exert any pressure on the cable, for example, by the inappropriate use of clamps (cable quick-mount) or cable ties. Your installation should also prevent anyone from stepping onto the cable.

Influence of heat

Fiber-optic cables are highly sensitive to direct heat, which means the cables must not be worked on using hot-air guns or gas burners as used in heat-shrink tubing technology.

13.3 Selecting fiber-optic cables

Check or make allowance for the following conditions and situations when selecting a suitable fiber-optic cable:

- Required cable lengths
- Indoor or outdoor installation
- Any particular protection against mechanical stress required?
- Any particular protection against rodents required?
- Can an outside cable be routed directly underground?
- Does the fiber-optic cable need to be water-proof?
- Which temperatures influence the installed fiber-optic cable?

Cable length up to 10 m

The synchronization module 6ES7 960–1AA06–0XA0 can be operated in pairs with fiber-optic cables up to a length of 10 m.

Select cables with the following specification for lengths up to 10 m:

- Multimode fiber 50/125 µ or 62.5/125 µ
- Patch cable for indoor applications

- 2 x duplex cables per fault-tolerant system, cross-over
- Connector type LC–LC

Such cables are available in the following length as accessories for fault-tolerant systems:

Table 13-1 Accessory fiber-optic cable

Length	Article No.
1 m	6ES7960–1AA04–5AA0
2 m	6ES7960–1AA04–5BA0
10 m	6ES7960–1AA04–5KA0

Cable length up to 10 km

The synchronization module 6ES7 960-1AB06-0XA0 can be operated in pairs with fiber-optic cables up to a length of 10 km.

The following rules apply:

- Make sure of adequate strain relief on the modules if you use fiber-optic cables longer than 10 m.
- Keep to the specified environmental conditions of the fiber-optic cables used (bending radii, pressure, temperature...)
- Observe the technical specifications of the fiber-optic cable (attenuation, bandwidth...)

Fiber-optic cables with lengths above 10 m usually have to be custom-made. First, select the following specification:

- Single-mode fiber (mono-mode fiber) 9/125 µ
  In exceptional situations, you may also use the lengths up to 10 m available as accessories for short distances when testing and commissioning. However, only the use of specified cables with single-mode fibers is allowed for continuous operation.

Note

Cable up to 10 m length on the synchronization module 6ES7 960-1AB06-0XA0

Cables up to a length of 10 m are available on order as accessories. If you use one of these cables on the synchronization module 6ES7 960-1AB06-0XA0 , you may see the error message "Optical performance too high" at the call of OB 82.

The table below shows the further specifications, based on your application:

Table 13-2 Specification of fiber-optic cables for indoor applications

Cabling	Components required	Specification
The entire cabling is routed within a building No cable junction is required between the indoor and outdoor area The necessary cable length is available in one piece. There is no need to connect several cable segments by means of distribution boxes. Convenient and complete installation using patch cables	Patch cables	2 x duplex cables per system Connector type LC–LC Crossed cores Further specifications you may need to observe for your plant, e.g.: UL approval Halogen-free materials
	Assembled patch cable	Multicore cables, 4 cores per system Connector type LC–LC Crossed cores Further specifications you may need to observe for your plant, e.g.: UL approval Halogen-free materials
The entire cabling is routed within a building No cable junction is required between the indoor and outdoor area The necessary cable length is available in one piece. There is no need to connect several cable segments by means of distribution boxes. Convenient and complete installation using patch cables	including patch cables for indoor applications as required	1 cable with 4 cores per fault-tolerant system Both interfaces in one cable 1 or 2 cables with several shared cores Separate installation of the interfaces in order to increase availability (reduction of common cause factor) Connector type ST or SC, for example, to match other components; see below Further specifications you may need to observe for your plant: UL approval Halogen-free materials Avoid splicing cables in the field. Use prefabricated cables with pulling protection/aids in whiplash or breakout design, including measuring log.
	Patch cable for indoor applications	Connector type LC on ST or SC, for example, to match other components
Installation using distribution boxes, see Fig. 12-2	One distribution/junction box per branch Installation and patch cables are connected via the distribution box. Either ST or SC plug-in connections can be used, for example. Check the cross-over installation when you wire the CPUs.	Connector type ST or SC, for example, to match other components

Table 13-3 Specification of fiber-optic cables for outdoor applications

Cabling	Components required	Specification
A cable junction is required between the indoor and outdoor area see Figure 12-2	• Installation cables for outdoor applications	Installation cables for outdoor applications • 1 cable with 4 cores per fault-tolerant system Both interfaces in one cable • 1 or 2 cables with several shared cores Separate installation of the interfaces in order to increase availability (reduction of common cause factor) • Connector type ST or SC, for example, to match other components; see below Further specifications you may need to observe for your plant: • UL approval • Halogen-free materials Further specifications you may need to observe for your plant: • Protection against increased mechanical stress • Protection against rodents • Water-proofing • Suitable for direct underground installation • Suitable for the given temperature ranges Avoid splicing cables in the field. Use prefabricated cables with pulling protection/aids in whiplash design, including measuring log.
	• including patch cables for indoor applications as required	• 1 cable with 4 cores per fault-tolerant system Both interfaces in one cable • 1 or 2 cables with several shared cores Separate installation of the interfaces in order to increase availability (reduction of common cause factor) • Connector type ST or SC, for example, to match other components; see below Further specifications you may need to observe for your plant: • UL approval • Halogen-free materials Avoid splicing cables in the field. Use prefabricated cables with pulling protection/aids in whiplash or breakout design, including measuring log.
	• Patch cable for indoor applications	• Connector type LC on ST or SC, for example, to match other components

Cabling	Components required	Specification
A cable junction is required between the indoor and outdoor area see Figure 12-2	• One distribution/junction box per branch Installation and patch cables are connected via the distribution box. Either ST or SC plug-in connections can be used, for example Check the cross-over installation when you wire the CPUs.	• Connector type ST or SC, for example, to match other components

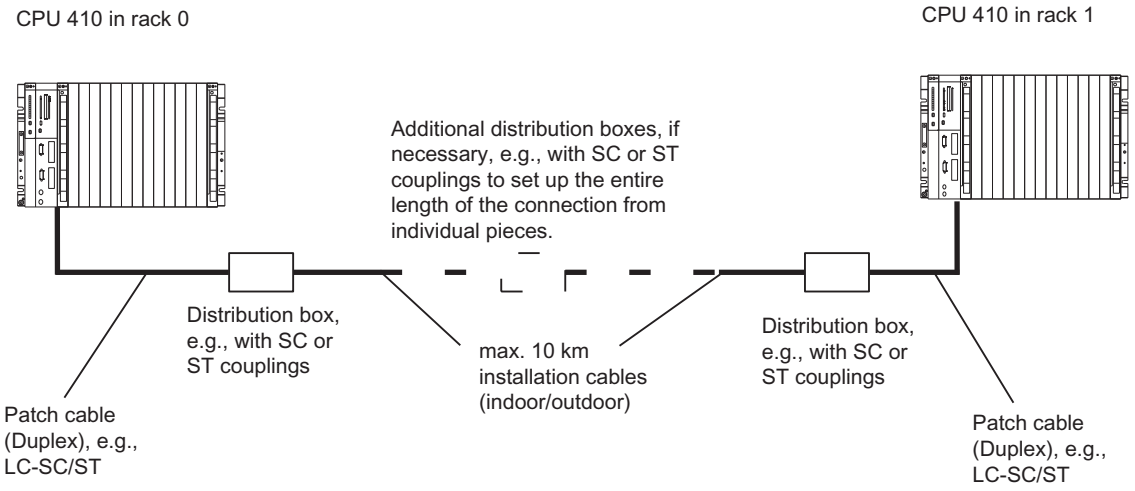


Figure 13-2 Fiber-optic cables, installation using distribution boxes

System expansion card

14

Use of the system expansion card

The SEC E4MB is plugged into a slot located at the back of the CPU.

SEC E4MB provides a maximum of 4 MB work memory for CPU 410SIS, 2 MB of which is for the program and 2 MB for data.

Without the SEC E4MB, it is not possible to operate the CPU 410SIS. If no valid SEC is detected, the CPU is not running.

If an error occurs in redundant mode during access to the SEC of a CPU, this triggers a loss of synchronization and a startup block prevents another automatic link-up.

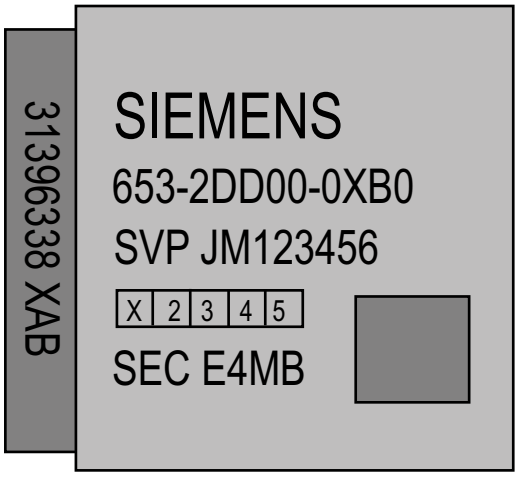


Figure 14-1 SEC E4MB

Enabling R1 redundancy

You can enable the R1 redundancy of a distributed I/O module by transferring the corresponding license key. You can find information about this in the documentation *SIMATIC Process Control System PCS 7, Service Support and Diagnostics* (V9.0)

See also

Licensing (Page 21)

Technical data

15

15.1 Technical specifications of CPU 410SIS (6ES7410-5FM08-0AB0)

Article number	6ES7410-5FM08-0AB0
General information	
Product type designation	CPU 410SIS SAFETY CONTROLLER
Hardware product version	1
Firmware version	V8.2
Design of PLC basic unit	With Conformal Coating (ISA-S71.04 severity level G1; G2; G3) and operating temperature to 70 °C
Product function	
• SysLog	Yes; via TCP; up to 4 receivers can be parameterized; buffer capacity max. 3 200 entries
• Field interface security	Yes
Engineering with	
• Programming package	SIMATIC SIS COMPACT V9.0 or higher
CiR – Configuration in RUN	
CiR synchronization time, basic load	60 ms
CiR synchronization time, time per I/O byte	0 µs
Input current	
from backplane bus 5 V DC, typ.	2 A
from backplane bus 5 V DC, max.	2.4 A
from backplane bus 24 V DC, max.	150 mA; DP interface
from interface 5 V DC, max.	90 mA; At the DP interface
Power loss	
Power loss, typ.	10 W
Memory	
Work memory	
• integrated	4 Mbyte
• integrated (for program)	2 Mbyte
• integrated (for data)	2 Mbyte
• expandable	No
Load memory	
• integrated RAM, max.	48 Mbyte
• expandable RAM	No
Backup	
• present	Yes
• with battery	Yes; all data
• without battery	Yes; Program and data of the load memory
Battery	

Article number	6ES7410-5FM08-0AB0
Backup battery	
• Backup current, typ.	370 µA; Valid up to 40°C
• Backup current, max.	2.1 mA
• Backup time, max.	Dealt with in the module data manual with the secondary conditions and the factors of influence
• Feeding of external backup voltage to CPU	No
CPU processing times	
CPU speed	450 MHz; Multi-processor system
Process tasks, max.	9; Individually adjustable from 10 ms to 5 s
CPU-blocks	
DB	
• Number, max.	16 000; Number range: 1 to 16 000 (= Instances)
FB	
• Number, max.	8 000; Number range: 0 to 7999
FC	
• Number, max.	8 000; Number range: 0 to 7999
OB	
• Size, max.	64 kbyte
• Number of free cycle OBs	1; OB 1
• Number of time alarm OBs	8; OB 10-17
• Number of delay alarm OBs	4; OB 20-23
• Number of cyclic interrupt OBs	9; OB 30-38 (= Process Tasks)
• Number of process alarm OBs	8; OB 40-47
• Number of DPV1 alarm OBs	3; OB 55-57
• Number of startup OBs	2; OB 100, 102
• Number of asynchronous error OBs	9; OB 80-88
• Number of synchronous error OBs	2; OB 121, 122
Counters, timers and their retentivity	
S7 counter	
• Number	2 048
Retentivity	
– adjustable	Yes
S7 times	
• Number	2 048
Data areas and their retentivity	
retentive data area in total	Total working and load memory (with backup battery)
Address area	
I/O address area	
• Inputs	2 048 byte
• Outputs	2 048 byte
of which distributed	
– DP interface, inputs	1 536 byte

Article number	6ES7410-5FM08-0AB0
– DP interface, outputs	1 536 byte
Hardware configuration	
connectable OPs	119
Multicomputing	No
Number of DP masters	
• integrated	1
• via CP	0
Number of IO Controllers	
• integrated	0
• via CP	0
Slots	
• required slots	2
Time of day	
Clock	
• Hardware clock (real-time)	Yes
• retentive and synchronizable	Yes
• Resolution	1 ms
• Deviation per day (buffered), max.	1.7 s; Power off
• Deviation per day (unbuffered), max.	8.6 s; Power on
Operating hours counter	
• Number	16
• Number/Number range	0 to 15
• Range of values	SFCs 2, 3 and 4: 0 to 32767 hours SFC 101: 0 to 2^31 - 1 hours
• Granularity	1 hour
• retentive	Yes
Clock synchronization	
• supported	Yes
• to DP, master	Yes
• to DP, slave	Yes
• in AS, master	Yes
• in AS, slave	Yes
• on Ethernet via NTP	Possible as client and master/slave via SIMATIC process
Interfaces	
Number of industrial Ethernet interfaces	2
Number of PROFINET interfaces	0
Number of RS 485 interfaces	1; PROFIBUS DP
Number of other interfaces	2; 2x synchronization
1. Interface	
Interface type	Integrated
Physics	RS 485 / PROFIBUS
Isolated	Yes

Article number	6ES7410-5FM08-0AB0
Power supply to interface (15 to 30 V DC), max.	150 mA
Number of connection resources	16
Functionality	
• PROFIBUS DP master	Yes
• PROFIBUS DP slave	No
DP master	
• Number of connections, max.	16
• Transmission rate, max.	12 Mbit/s
• Number of DP slaves, max.	96
• Number of slots per interface, max.	1 632
Services	
– PG/OP communication	Yes
– Routing	Yes; S7 routing
– Global data communication	No
– S7 basic communication	No
– S7 communication	Yes
– S7 communication, as client	Yes
– S7 communication, as server	Yes
– Equidistance	No
– Isochronous mode	No
– SYNC/FREEZE	No
– Activation/deactivation of DP slaves	Yes; Single mode only
– Direct data exchange (slave-to-slave communication)	No
– DPV1	Yes
Address area	
– Inputs, max.	1 536 byte
– Outputs, max.	1 536 byte
User data per DP slave	
– User data per DP slave, max.	244 byte
– Inputs, max.	244 byte
– Outputs, max.	244 byte
– Slots, max.	244
– per slot, max.	128 byte
2. Interface	
Interface type	Integrated Ethernet interface
Physics	Ethernet RJ45
Isolated	Yes
automatic detection of transmission rate	Yes; Autosensing
Autonegotiation	Yes
Autocrossing	Yes
Change of IP address at runtime, supported	No

Article number	6ES7410-5FM08-0AB0
Number of connection resources	120
Interface types	
• Number of ports	2
• integrated switch	Yes
Media redundancy	
• supported	Yes
• Switchover time on line break, typ.	< 200 ms
• Number of stations in the ring, max.	50
Functionality	
• PROFINET IO Controller	No
• PROFINET IO Device	No
• PROFINET CBA	No
• Open IE communication	Yes
• Web server	No
Open IE communication	
• Number of connections, max.	118
• Local port numbers used at the system end	0, 20, 21, 25, 102, 135, 161, 34962, 34963, 34964, 65532, 65533, 65534, 65535
• Keep-alive function, supported	Yes
3. Interface	
Interface type	Integrated Ethernet interface
Physics	Ethernet RJ45
Isolated	Yes
automatic detection of transmission rate	Yes; Autosensing
Autonegotiation	Yes
Autocrossing	Yes
Number of connection resources	120
Interface types	
• Number of ports	2
• integrated switch	Yes
Media redundancy	
• supported	Yes
• Switchover time on line break, typ.	< 200 ms
• Number of stations in the ring, max.	50
Functionality	
• PROFINET IO Controller	No
• PROFINET IO Device	No
• PROFINET CBA	No
• Open IE communication	Yes
• Web server	No
Open IE communication	
• Number of connections, max.	118

Article number	6ES7410-5FM08-0AB0
• Local port numbers used at the system end	0, 20, 21, 25, 102, 135, 161, 34962, 34963, 34964, 65532, 65533, 65534, 65535
• Keep-alive function, supported	Yes
4. Interface	
Interface type	Pluggable synchronization submodule (FO)
Plug-in interface modules	Synchronization module 6ES7960-1AA06-0XA0, 6ES7960-1AB06-0XA0 or 6ES7960-1AA08-0XA0
5. Interface	
Interface type	Pluggable synchronization submodule (FO)
Plug-in interface modules	Synchronization module 6ES7960-1AA06-0XA0, 6ES7960-1AB06-0XA0 or 6ES7960-1AA08-0XA0
Protocols	
Supports protocol for PROFINET IO	No
PROFINET CBA	No
PROFIsafe	Yes
PROFIBUS	Yes
AS-Interface	Yes; Via add-on
Protocols (Ethernet)	
• TCP/IP	Yes
Open IE communication	
• TCP/IP	
– Number of connections, max.	118
– Data length, max.	32 kbyte
– several passive connections per port, supported	Yes
• ISO-on-TCP (RFC1006)	Yes
– Number of connections, max.	118
– Data length, max.	32 kbyte
• UDP	
– Number of connections, max.	118
– Data length, max.	1 472 byte
Further protocols	
• MODBUS	Yes; Via add-on
Communication functions	
PG/OP communication	Yes
• Number of connectable OPs without message processing	119
• Number of connectable OPs with message processing	119; When using Alarm_S/SQ and Alarm_D/DQ
Data record routing	Yes
S7 routing	Yes
S7 communication	
• supported	Yes
• as server	Yes

Article number	6ES7410-5FM08-0AB0
• as client	Yes
• User data per job, max.	64 kbyte
• User data per job (of which consistent), max.	462 byte; 1 variable
Open IE communication	
• TCP/IP	Yes
• UDP	Yes
Number of connections	
• overall	120
S7 message functions	
Number of login stations for message functions, max.	119; Max. 119 with Alarm_S and Alarm_D (OPs); max. 12 with Alarm_8 and Alarm_P (e.g. WinCC)
Alarm 8-blocks	Yes
• Number of instances for alarm 8 and S7 communication blocks, max.	10 000
• preset, max.	10 000
Process control messages	Yes
Test commissioning functions	
Status block	Yes
Single step	Yes
Number of breakpoints	4
Status/control	
• Status/control variable	Yes
• Variables	Inputs/outputs, memory bits, DBs, distributed I/Os, timers, counters
• Number of variables, max.	70
Diagnostic buffer	
• present	Yes
• Number of entries, max.	3 200
Service data	
• can be read out	Yes
Standards, approvals, certificates	
CE mark	Yes
CSA approval	Yes
UL approval	Yes
cULus	Yes
FM approval	Yes
RCM (formerly C-TICK)	Yes
KC approval	Yes
EAC (formerly Gost-R)	Yes
Use in hazardous areas	
• ATEX	ATEX II 3G Ex nA IIC T4 Gc
Ambient conditions	
Ambient temperature during operation	

Article number	6ES7410-5FM08-0AB0
• min.	0 °C
• max.	70 °C
Air pressure acc. to IEC 60068-2-13	
• Installation altitude above sea level, max.	2 000 m
Configuration	
Know-how protection	
• User program protection/password protection	Yes
• Block encryption	Yes; With S7 block Privacy
Dimensions	
Width	50 mm
Height	290 mm
Depth	219 mm
Weights	
Weight, approx.	1.1 kg

15.2 Technical specifications of the system expansion card

Article number	6ES7653-2DD00-0XB0
General information	
Product type designation	CPU 410 System Expansion Card E4MB
Hardware product version	3
Firmware version	V2.0
Design of PLC basic unit	With Conformal Coating (ISA-S71.04 severity level G1; G2; G3) and operating temperature to 70 °C
Memory	
Work memory	
• integrated	Use of max. 4 MB work memory in the CPU 410SIS
• integrated (for program)	Use of 2 MB in the CPU 410SIS
• integrated (for data)	Use of 2 MB in the CPU 410SIS
• expandable	No
Address area	
I/O address area	
• Inputs	Use of 2 048 bytes in the CPU 410SIS
• Outputs	Use of 2 048 bytes in the CPU 410SIS
of which distributed	
– DP interface, inputs	1 536 byte; max.
– DP interface, outputs	1 536 byte; max.
Standards, approvals, certificates	
CE mark	Yes
CSA approval	Yes
UL approval	Yes
cULus	Yes
FM approval	Yes
RCM (formerly C-TICK)	Yes
KC approval	Yes
EAC (formerly Gost-R)	Yes
Use in hazardous areas	
• ATEX	ATEX II 3G Ex nA IIC T4 Gc
Ambient conditions	
Ambient temperature during operation	
• min.	0 °C
• max.	70 °C
Dimensions	
Width	8 mm
Height	16 mm
Depth	25 mm
Weights	
Weight, approx.	20 g

Supplementary information 16

16.1 Configuring

16.1.1 Rules for assembling an AS 410H SIS

There are rules for an AS 410H SIS in addition to the rules that generally apply to the arrangement of modules in a rack:

- Insert the CPUs into the same slots.
- Redundantly used CPUs must be identical, which means they must have the same article number, product version and firmware version. It is not the marking on the front side that is decisive for the product version, but the revision of the "Hardware" component ("Module status" dialog mask) to be read using HW Config.
- Redundantly used other modules must be identical, which means they must have the same article number, product version and - if available - firmware version.

Additional I/O expansion

For use of distributed I/O, you can connect a DP master system to the integrated interface of the CPU in each of the two subsystems.

16.1.2 Configuring hardware

You can use the SIMATIC SIS compact wizards to create the AS bundle configurations.

Another way of achieving a redundant hardware configuration is to initially assemble **one** rack with all components to be implemented redundantly and to assign parameters to them. The entire rack must then be copied and inserted. You adjust the network parameters appropriately in the subsequent dialogs.

Specific aspects of the hardware configuration display

To enable fast identification of a redundant DP master system, it is represented by two closely adjoining lines.

16.1.3 Assigning parameters to modules in an H system

Procedure

Assign all parameters of the redundant components identically, with the exception of communication addresses.

The special case of CPUs

You can only set the CPU0 parameters (CPU on rack 0). Any values that you specify are automatically allocated to CPU1 (CPU on rack 1). You can set the following values for CPU1:

- Parameters of the DP interface (X1)
- Addresses of sync modules

16.1.4 Recommendations for setting CPU parameters, fixed settings

Monitoring time for transferring parameters to modules

You specify this monitoring time on the "Startup" tab. This depends on the size of the H system. If the monitoring time is too short, the CPU enters the W#16#6547 event in the diagnostics buffer.

For some slaves (e.g., IM 153-2) these parameters are packed in system data blocks. The transmission time of the parameters depends on the following factors:

- Baud rate of the bus system (high baud rate => short transmission time)
- Size of the parameters and the system data blocks (long parameter => long transmission time)
- Load on the bus system (many slaves => slow transmission rate);
  Note: The bus load is at its peak during restart of the DP master, for example, following Power OFF/ON

Recommended setting (default setting of the CPU 410SIS): 600 corresponds to 60 s.

Note

The fault-tolerant-specific CPU parameters, and thus also the monitoring times, are calculated automatically. The work memory allocation of all data blocks is based on a CPU-specific default value. If your fault-tolerant system does not link up, check the data memory allocation (HW Config > CPU Properties > H Parameters > Work memory used for all data blocks).

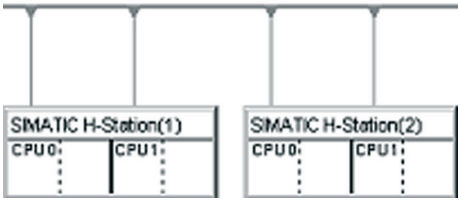
16.1.5 Networking configuration

The fault-tolerant S7 connection is a separate connection type of the "Configure Networks" application. It permits that the following communication peers can communicate with each other:

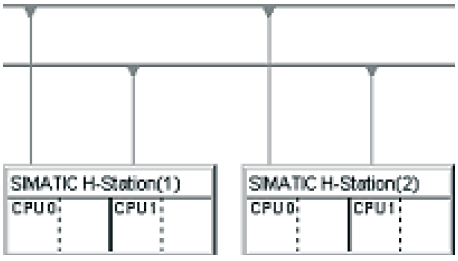
- S7–400 fault-tolerant station (with 2 fault-tolerant CPUs)->S7–400 fault-tolerant station (with 2 fault-tolerant CPUs)
- S7–400 station (with 1 fault-tolerant CPU)->S7–400 fault-tolerant station (with 2 fault-tolerant CPUs)
- S7–400 station (with 1 fault-tolerant CPU)->S7–400 station (with 1 fault-tolerant CPU)
- SIMATIC PC stations > S7–400 fault-tolerant station (with 2 fault-tolerant CPUs)

When this connection type is configured, the application automatically determines the number of possible subconnections:

- If two independent but identical subnets are available and they are suitable for a fault-tolerant S7 connection, two subconnections are used. In practice, they are usually electrical networks, one network connection in each subnet:



- If only one subnet is available, four subconnectors are used for a connection between two fault-tolerant stations. All network connections are located in this subnet:



Within a high-availability S7 connection, the integrated Profinet interfaces are used exclusively for sub-connections within a station. But multiple fault-tolerant stations in one subnet may have different interfaces; they only have to be identical within the station.

Downloading the network configuration into a fault-tolerant station

The complete network configuration can be downloaded into the fault-tolerant station in one operation. The same requirements that apply for downloads into standard stations must be met.

16.2 PG functions

Display in SIMATIC Manager

In order to do justice to the special features of a fault-tolerant station, the way in which the system is visualized and edited in SIMATIC Manager differs from that of a S7-400 standard station as follows:

- In the offline view, the S7 program appears only under CPU0 of the fault-tolerant station. No S7 program is visible under CPU1.
- In the online view, the S7 program appears under both CPUs and can be selected in both locations.

Communication functions

For programming device (PG) functions that establish online connections (e.g., downloading charts), one of the two CPUs has to be selected even if the function affects the entire system over the redundant link.

- Data which is modified in one of the central processing units in redundant operation affect the other CPUs over the redundant link.
- Data which is modified when there is no redundant link (i.e. in single mode) initially affects only the processed CPU. The blocks are applied by the master CPU to the reserve CPU during the next link-up and update. Exception: No new blocks are applied after changing the configuration. Loading the blocks is then the responsibility of the user.

16.3 Communication services

16.3.1 Overview of communication services

Overview

Table 16-1 Communication services of the CPUs

Communication service	Functionality	Allocation of S7 connection resources	Via PROFI-BUS	Via PROFI-NET
PG communication	Commissioning, testing, diagnostics	Yes	Yes	Yes
OP communication	Operator control and monitoring	Yes	Yes	Yes
S7 communication	Data exchange via configured connections	Yes	Yes	Yes
Routing of PG functions	For example, testing, diagnostics beyond network boundaries	Yes	Yes	Yes
PROFIBUS DP	Data exchange between master and slave	No	Yes	No

Communication service	Functionality	Allocation of S7 connection resources	Via PROFI-BUS	Via PROFI-NET
SNMP (Simple Network Management Protocol)	Standard protocol for network diagnostics and parameter assignment	No	No	Yes
Open communication over TCP/IP	Data exchange over Industrial Ethernet with TCP/IP protocol (with loadable FBs)	Yes	No	Yes
Open communication over ISO on TCP	Data exchange over Industrial Ethernet with ISO on TCP protocol (with loadable FBs)	Yes	No	Yes
Open communication over UDP	Data exchange over Industrial Ethernet with UDP protocol (with loadable FBs)	Yes	No	Yes
Data record routing	For example, parameter assignment and diagnostics of field devices on PROFIBUS DP with PDM.	Yes	Yes	Yes

Note

Communication via a PROFINET interface

If you want to use a PROFINET interface of the module for communication during operation, you must also connect this in Step 7 / HW Config / Netpro.

Availability of connection resources

Table 16-2 Availability of connection resources

CPU	Total number of connection resources	Can be used for S7-H connections	Reserved from the total number for	
			PG communication	OP communication
CPU 410SIS	120	62	1	1

Free S7 connections can be used for any of the above communication services.

Note

Communication service via the PROFIBUS DP interface

A fixed default timeout of 40 s is specified for communication services using S7 connection resources. If you operate those communication services via a PROFIBUS DP interface at a low baud rate, operation in configurations with a Ttr (Target Rotation Time) < 20 s is ensured.

16.3.2 PG communication

Properties

Programming device communication is used to exchange data between engineering stations (PG, PC, for example) and SIMATIC modules which are capable of communication. This service is available via PROFIBUS and Industrial Ethernet subnets. Routing between subnets is also supported.

You can use the programming device communication for the following actions:

- Loading programs and configuration data
- Performing tests
- Evaluating diagnostic information

These functions are integrated in the operating system of SIMATIC S7 modules.

A CPU can maintain several simultaneous online connections to one or multiple programming devices.

16.3.3 OP communication

Properties

OP communication is used to exchange data between HMI stations, such as WinCC, OP, TP and SIMATIC modules which are capable of communication. This service is available via PROFIBUS and Industrial Ethernet subnets.

You can use the OP communication for operator control, monitoring and alarms. These functions are integrated in the operating system of SIMATIC S7 modules. A CPU can maintain several simultaneous connections to one or several OPs.

16.3.4 S7 routing

Properties

You can access your S7 stations beyond subnet boundaries using the programming device / PC. You can use them for the following actions:

- Downloading user programs
- Downloading a hardware configurations
- Performing test and diagnostic functions

Requirements

- The network configuration does not exceed project limits.
- The modules have loaded the configuration data containing the latest "knowledge" of the entire network configuration of the project.
  Reason: All modules connected to the network gateway must receive routing information which defines the paths to other subnets.
- In your network configuration, the PG/PC you want to use to set up a connection via gateway must be assigned to the network to which it is physically connected.
- The CPU must be configured as the master.

S7 routing gateways: PROFINET - PROFIBUS

Gateways between subnets are routed in a SIMATIC station that is equipped with interfaces to the respective subnets. The following figure shows CPU 1 (DP master) acting as router for subnets 1 and 2.

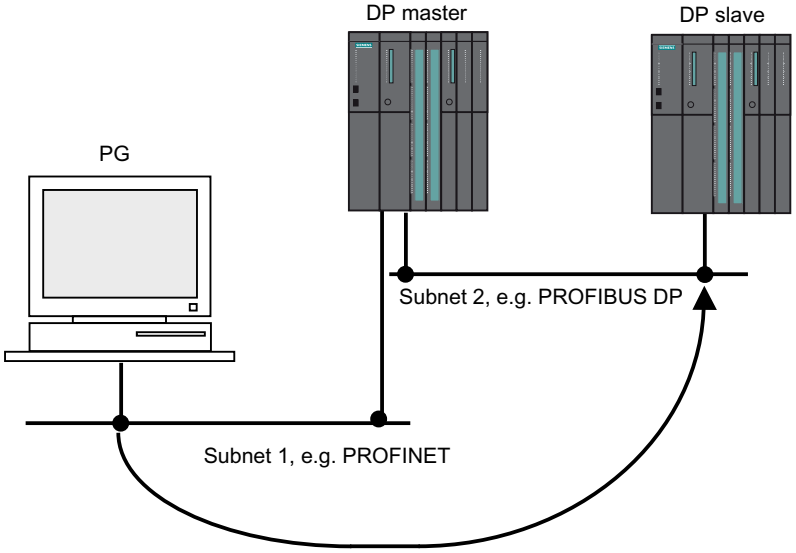


Figure 16-1 S7 routing

S7 routing gateways: PROFINET-PROFIBUS-PROFINET

The following figure shows the access from PROFINET to PROFINET via PROFIBUS. CPU 1 is the router between subnet 1 and subnet 2; CPU 2 is the router between subnet 2 and subnet 3.

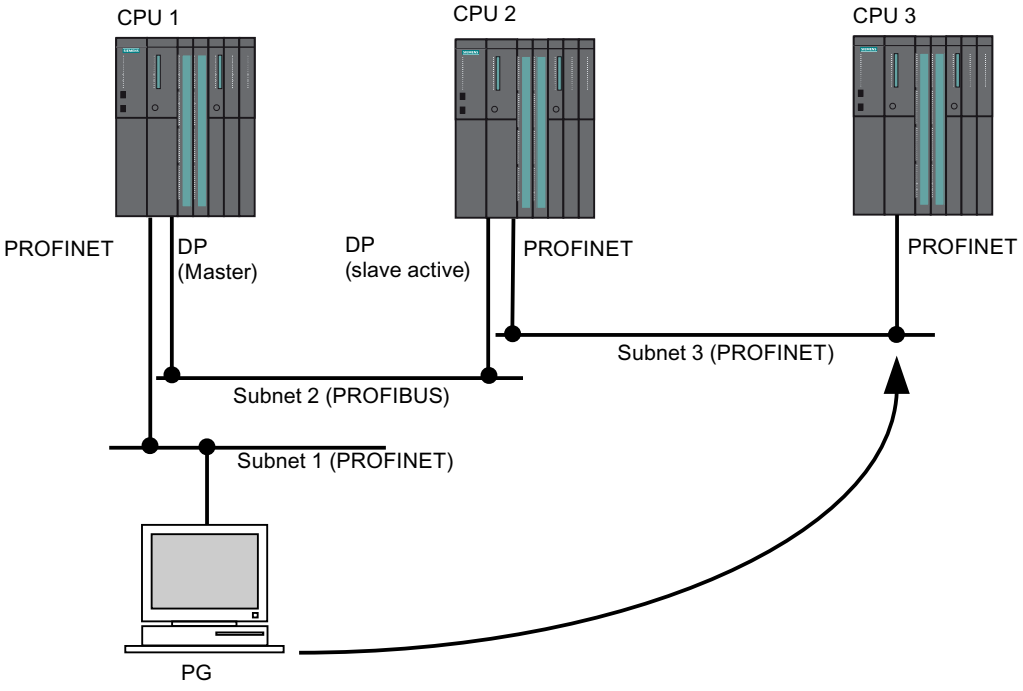


Figure 16-2 S7 routing gateways: PROFINET DP - PROFINET

S7 routing: TeleService application example

The following figure shows an application example of the remote maintenance of an S7 station using a PG. The connection to other subnets is set up via modem.

The bottom of the figure shows how this can be configured in STEP 7.

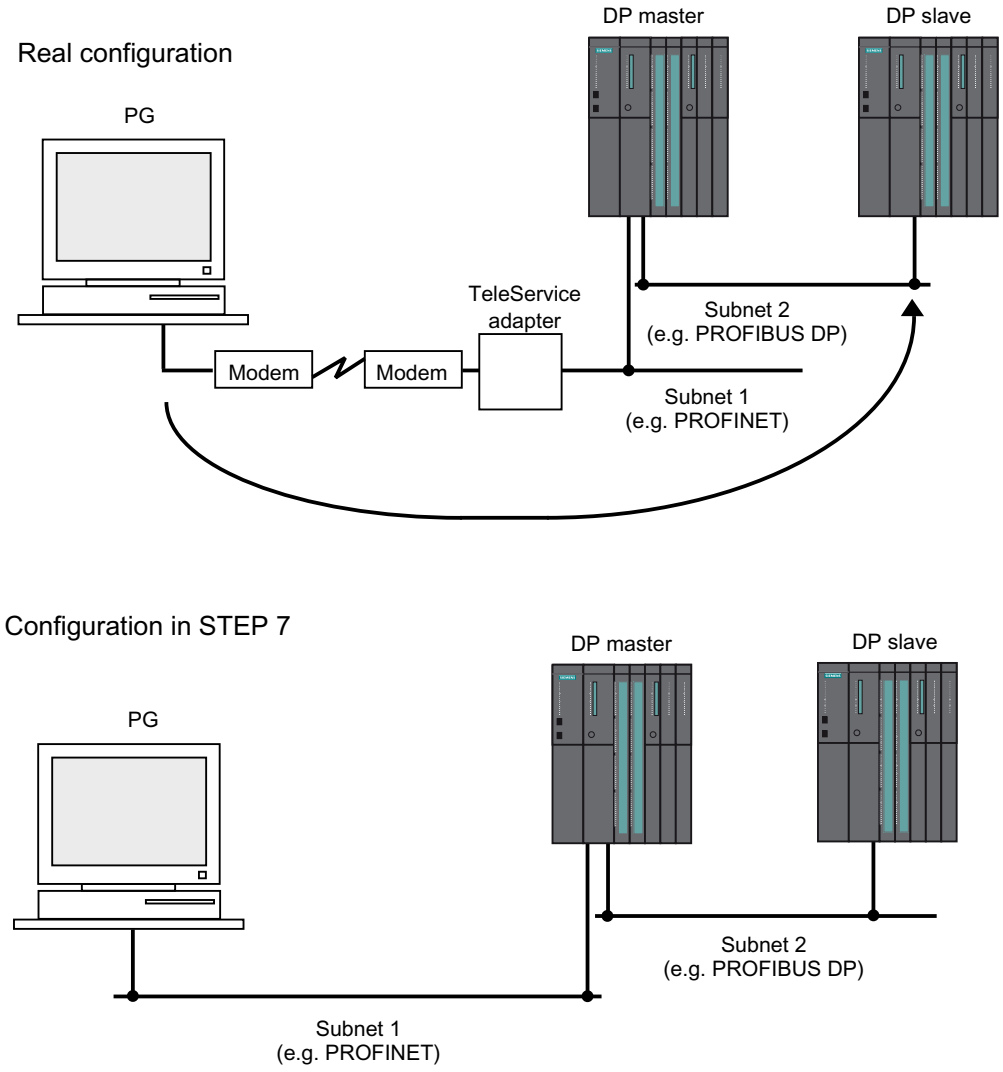


Figure 16-3 S7 routing: TeleService application example

Reference

- Further information on configuration with STEP 7 can be found in Manual Configuring hardware and communication connections with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/45531110).
- More basic information is available in Manual Communication with SIMATIC (https://support.industry.siemens.com/cs/ww/en/view/1254686).
- For more information about the TeleService adapter, refer to Manual TS Adapter (https://support.industry.siemens.com/cs/ww/en/view/20983182)
- For additional information about SFCs, refer to the Instructions list. (https://support.industry.siemens.com/cs/ww/en/view/44395684)
  For a detailed description, refer to the *STEP 7 online help* or Manual System and Standard Functions (https://support.industry.siemens.com/cs/ww/en/view/44240604).

16.3.5 Data set routing

Routing and data set routing

Routing is the transfer of data beyond network boundaries. You can send information from a transmitter to a receiver across several networks.
Data set routing is an expansion of S7 routing and is used, for example, in SIMATIC PDM. The data sent through data record routing include the parameter assignments of the participating communication devices and device-specific information (for example, setpoint values, limit values, etc.). The structure of the destination address for data set routing depends on the data content, in other words, it is determined by the device for which the data is intended. The field device itself does not have to support data set routing, since these devices do not forward the received information.

Data set routing

The following figure shows the engineering station accessing a variety of field devices. The engineering station is connected to the CPU via Industrial Ethernet in this scenario. The CPU communicates with the field devices via the PROFIBUS.

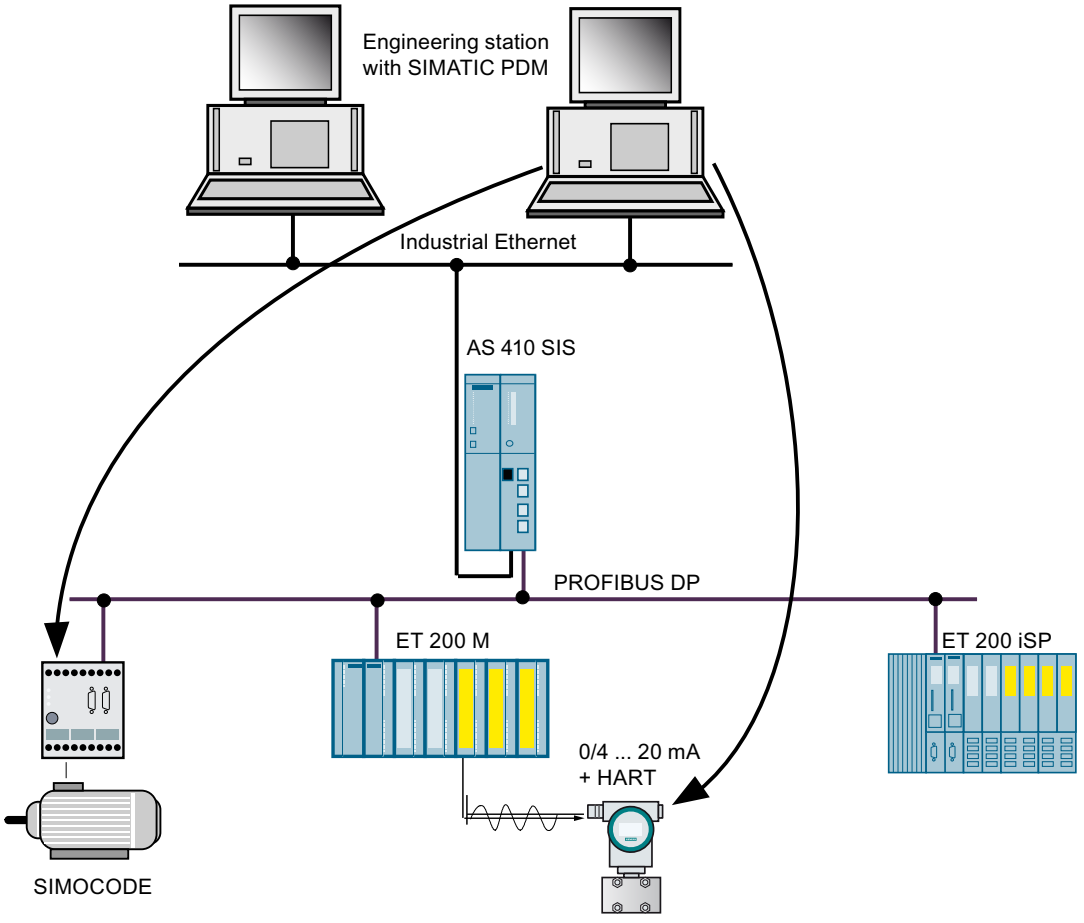


Figure 16-4 Data set routing

See also

For more information on SIMATIC PDM, refer to Manual *The Process Device Manager*.

16.3.6 SNMP network protocol

Properties

SNMP (Simple Network Management Protocol) is the standardized protocol for diagnostics of the Ethernet network infrastructure. In the office setting and in automation engineering, devices from many different manufacturers support SNMP on the Ethernet. Applications based on SNMP can be operated parallel to applications with PROFINET on the same network.

Configuration of the SNMP OPC server is integrated in the STEP 7 Hardware Configuration application. Already configured S7 modules from the STEP 7 project can be transferred directly. As an alternative to STEP 7, you can also perform the configuration with the NCM PC (included on the SIMATIC NET CD). All Ethernet devices can be detected by means of their IP address and/or the SNMP protocol (SNMP V1) and transferred to the configuration.

Use the profile MIB_II_V10.

Applications based on SNMP can be operated parallel to applications with PROFINET on the same network.

Note

MAC addresses

During SNMP diagnostics, the following MAC addresses are shown for the ifPhysAddress parameter:

Interface 1 (PROFINET interface) = MAC address (indicated on the front panel of the CPU)

Interface 2 (port 1) = MAC address + 1

Interface 3 (port 2) = MAC address + 2

Diagnostics with SNMP OPC Server in SIMATIC NET

The SNMP OPC server software enables diagnostics and parameter assignment of any SNMP devices. The OPC server uses the SNMP protocol to perform data exchange with SNMP devices.

All information can be integrated in OPC-compatible systems, such as the WinCC HMI system. This enables process and network diagnostics to be combined in the HMI system.

Reference

For further information on the SNMP communication service and diagnostics with SNMP, refer to the *PROFINET System Description.*

16.4 Basics and terminology of fault-tolerant communication

Overview

When more stringent requirements for overall plant availability exist, it is necessary to increase the reliability of the communication, i.e., by configuring the communication redundantly as well.

Below you will find an overview of the fundamentals and basic concepts which you ought to know with regard to using fault-tolerant communications.

Redundant communication system

The availability of the communication system can be increased by duplicating subcomponents, duplicating all bus components, or using a fiber-optic ring.

Monitoring and synchronization mechanisms ensure that standby components take over communication if one components fails.

A redundant communication system is required for the user of fault-tolerant S7 connections.

Fault-tolerant communication

Fault-tolerant communication is the use of S7 communication SFBs over fault-tolerance S7 connections.

A fault-tolerant S7 connection consists of at least two and a maximum of four partial connections depending on networking. Two partial connections are established for fault-tolerant communication; the two others are configuration standbys.

Fault-tolerant S7 connections require a redundant communication system.

Redundancy nodes

Redundancy nodes represent extreme reliability of communication between two fault-tolerant systems. A system with multi-channel components is represented by redundancy nodes. Redundancy nodes are independent when the failure of a component within the node does not result in any reliability impairment in other nodes.

Even with fault-tolerant communication, only single errors/faults can be tolerated. If more than one error occurs between two communication end points, communication can no longer be guaranteed.

Connection (S7 connection)

A connection represents the logical assignment of two communication peers for executing a communication service. Every connection has two end points containing the information required for addressing the communication peer as well as other attributes for establishing the connection.

An S7 connection is the communication connection between two standard CPUs or between a standard CPU and a CPU of a fault-tolerant system.

Unlike a fault-tolerant S7 connection, which contains at least two partial connections, an S7 connection does only consist of one connection. If that connection fails, communication is terminated.

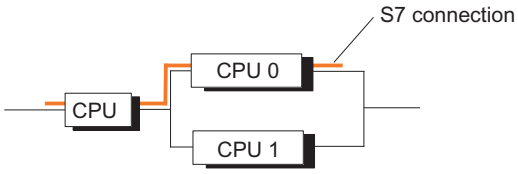


Figure 16-5 Example of an S7 connection

Note

"Connection" in this manual refers in general to a "configured S7 connection". For other types of connection, refer to Manuals *SIMATIC NET NCM S7 for PROFIBUS* and *SIMATIC NET NCM S7 for Industrial Ethernet*.

Fault-tolerant S7 connections

The requirement for higher availability with communication components (for example CPs and buses) means that redundant communication connections are necessary between the systems involved.

Unlike an S7 connection, a fault-tolerant S7 connection consists of at least two subordinate partial connections. For the user program, configuration and connection diagnostics, a fault-tolerant S7 connection and its subordinate partial connections are represented by precisely one ID (like an S7 connection). Depending on the configuration, it can consist of a maximum of four subconnections. To maintain communication in the event of an error, two of the four subconnections are always connected (active) at any given time. The number of subconnections depends on the possible alternative paths (see figure below) and is determined automatically. Within an S7-H connection, only sub-connections over the integrated CPU interface are used in the configuration.

The following examples and the possible configurations in STEP 7 are based on a maximum of 2 subnets in the redundant H system. Configurations with a higher number of networks are not supported by STEP 7.

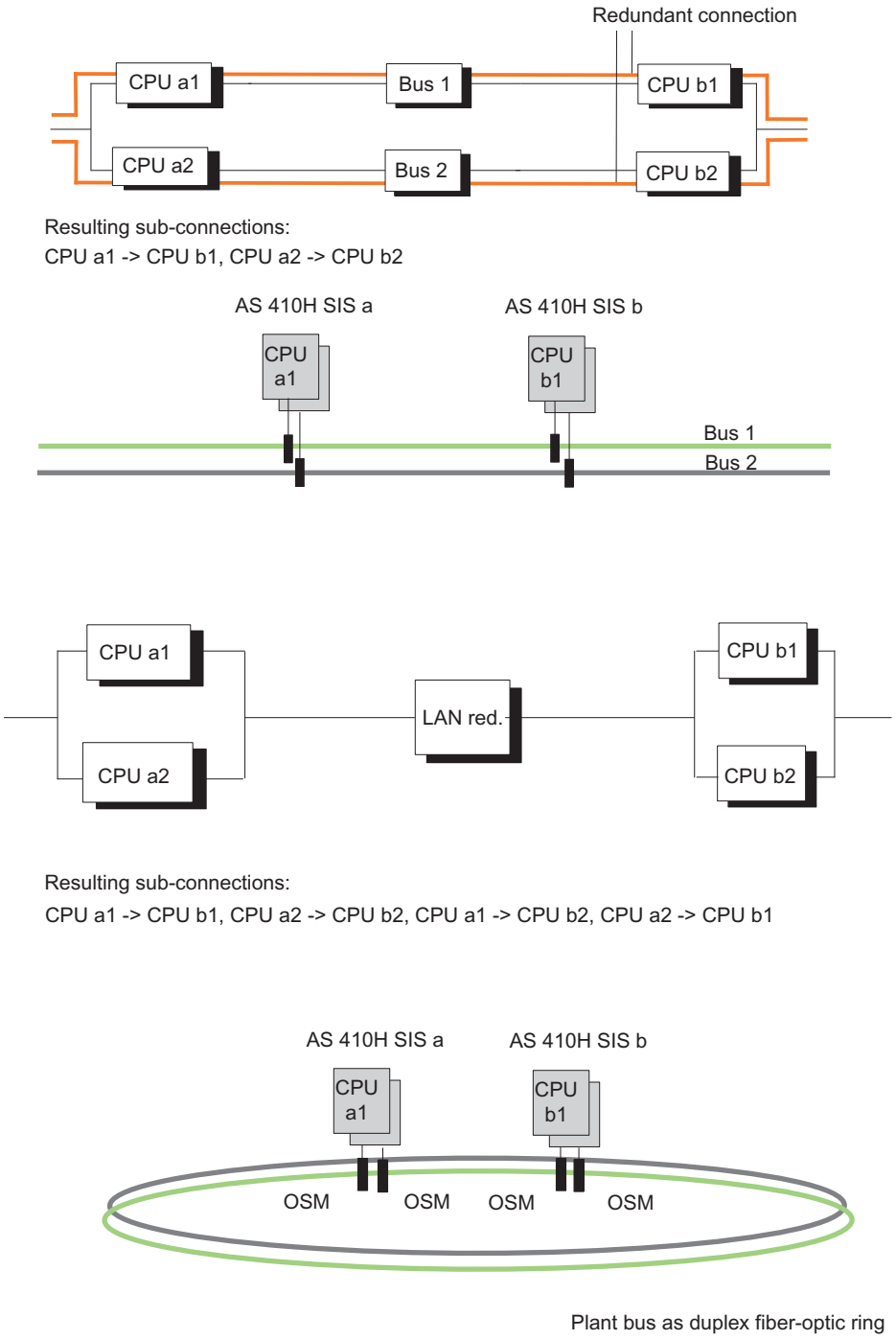


Figure 16-6 Example that shows that the number of resulting partial connections depends on the configuration

If the active subconnection fails, the already established second subconnection automatically takes over communication.

Resource requirements for fault-tolerant S7 connections

The H-CPU enables the operation of 62 (see Technical specifications) fault-tolerant S7 connections. Each connection needs a connection resource on the CPU; subconnections do not need any additional connection resources. On the CP, on the other hand, each subconnection needs a connection resource.

Note

If you have configured multiple fault-tolerant S7 connections for an H station, it may take a considerable time for them to be established. If the configured maximum communication delay was set too short, link-up and updating is canceled and the redundant system state is no longer achieved (see Chapter Time monitoring (Page 90)).

16.5 Usable networks

Your choice of the physical transmission medium depends on the required expansion, targeted fault tolerance, and transfer rate. The following bus systems are used for communication with fault-tolerant systems:

- Industrial Ethernet
- PROFIBUS

Additional information on the networks that can be used is available in the relevant SIMATIC NET documentation on PROFIBUS and Ethernet.

16.6 Communication via S7 connections

Configuration

S7 connections are configured in STEP 7.

Programming

If S7 communication is used on a fault-tolerant system, all communication functions can be used for this.

The communication SFBs are used in STEP 7 to program communication.

Note

The START and STOP communication functions act on exactly one CPU or on all CPUs of the fault-tolerant system. More detailed information is available in Reference Manual *System Software for S7-300/400 System and Standard Functions*.

Note

Downloading the connection configuration during operation

If you download a connection configuration during operation, established connections may be terminated.

16.6.1 Custom connection to single-channel systems

Connection via PC as gateway

Fault-tolerant systems and single-channel systems can also be via a gateway (no connection redundancy). The gateway is connected to the system bus by one or two CPs, depending on availability requirements. Fault-tolerant connections can be configured between the gateway and the fault-tolerant systems. The gateway allows you to link any type of single-channel system (e.g., TCP/IP with a manufacturer-specific protocol).

A user-programmed software instance in the gateway implements the single-channel transition to the fault-tolerant systems, and so allows any single-channel systems to be linked to a fault-tolerant system.

Configuring connections

Redundant connections between the gateway CP and the single-channel system are not required.

The gateway CP is located on a PC system which has fault-tolerant connections to the fault-tolerant system.

To configure fault-tolerant S7 connections between fault-tolerant system A and the gateway, you first need to install S7-REDCONNECT on the gateway. The functions for preparing data for their transfer via the single-channel link must be implemented in the user program.

For additional information, refer to the "*Industrial Communications IK10*" Catalog.

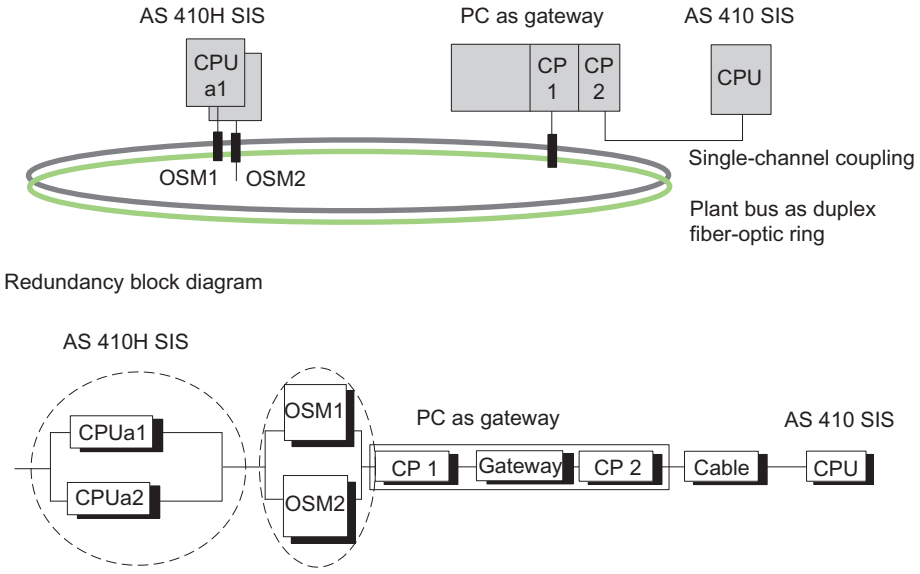


Figure 16-7 Example of linking a fault-tolerant system to a single-channel third-party system

16.7 Communication via fault-tolerant S7 connections

Availability of communicating systems

High-availability communication expands the overall SIMATIC system with additional redundant communication components, for example, bus lines. To illustrate the actual availability of communicating systems when using an optical or electrical network, a description is given below of the possibilities for communication redundancy.

Requirement

The essential requirement for the configuration of fault-tolerant connections with STEP 7 is a configured hardware installation.

The hardware configuration in both subsystems of a fault-tolerant system **must** be identical. This applies in particular to the slots.

High-availability S7 connections via Industrial Ethernet with ISO-on-TCP are supported over the integrated PN interfaces.

Only Industrial Ethernet is supported for connecting to PC stations using fault-tolerant S7 connections. To be able to use fault-tolerant S7 connections between a fault-tolerant system and a PC, you must install the "S7-REDCONNECT" software package on the PC. The software is part of the SIMATIC Net CD. As of version 8.1.1, communication over ISO-on-TCP is also supported. Please refer to the product information on the SIMATIC NET PC software to learn more about the CPs you can use at the PC end.

Communication combinations

The following table shows the possible combinations of fault-tolerant connections via Industrial Ethernet.

Local connection end point	Local network connection	Used network protocol	Remote network connection		Remote connection end point	
CPU 410SIS	CPU-PN interface	TCP	PN interface	TCP	CPU 410SIS	S7 fault tolerant connection via ISOonTCP
PC station with Simatic Net CD	PC station with Simatic Net CD CP1613/1623/1628, V8.1.1 or higher	TCP	PN interface	TCP	CPU 410SIS	S7 fault tolerant connection via ISOonTCP

Configuration

The availability of the system, including the communication, is set during configuration. Refer to the STEP 7 documentation to find out how to configure connections.

Only S7 communication is used for fault-tolerant S7 connections. To set this up, open the "New Connection" dialog box, then select "S7 Connection Fault-Tolerant" as the type.

The number of required redundant subconnections is determined by STEP 7 as a function of the redundancy nodes. Up to four redundant connections can be generated, if supported by the network.

In the "Properties - Connection" dialog box you can also modify specific properties of a fault-tolerant connection if necessary.

You have to extend the monitoring time of the connection when you use long synchronization cables.

Example: If you are operating 5 fault-tolerant S7 connections with a monitoring time of 500 ms and short synchronization cables up to 10 m and you want to change these to long synchronization cables with a length of 10 km, you must increase the monitoring time to 1000 ms.

To ensure CIR capability of the fault tolerant system, you must activate the "Save connections prior to loading" option in Step 7 NetPro.

Programming

High-availability communication can be used on the CPU 410SIS and runs using S7 communication.

This is possible only within an S7 project/multiproject.

You program the fault-tolerant communication with STEP 7 using communication SFBs. These communication blocks can be used to transmit data over subnets (Industrial Ethernet, PROFIBUS). The communication SFBs integrated in the operating system enable an

acknowledged data transmission. In addition to data transfer, you can also use other communication functions for controlling and monitoring the communication peer.

User programs written for S7 connections can also be used for fault-tolerant S7 connections without program modification. Cable and connection redundancy has no effect on the user program.

Note

For information on programming the communication, refer to the STEP 7 documentation (e.g., *Programming with STEP 7*).

The START and STOP communication functions act on exactly one CPU or on all CPUs of the AS 410H SIS (for more details refer to Reference Manual *System Software for S7-300/400, System and Standard Functions*).

Disruptions of a subconnection while communication jobs are active over fault-tolerant S7 connections can extend the runtime of these jobs.

Note

Downloading the connection configuration during operation

If you download a connection configuration during operation, established connections may be terminated.

16.7.1 Communication between fault-tolerant systems

Availability

The easiest way to increase the availability between linked systems is to use a redundant plant bus. This is set up with a duplex fiber-optic ring or a dual electrical bus system. The connected nodes may consist of simple standard components.

Availability can best be enhanced using a duplex fiber-optic ring. If a break of the two-fiber fiber-optic cable occurs, communication is maintained between the systems involved. The systems then communicate as if they were connected to a bus system (line). A ring topology basically contains two redundant components and automatically forms a 1-out-of-2 redundancy node. The fiber-optic network can also be set up in star topology as redundant bus.

If one electrical cable segment fails, communication between the participating systems is also upheld (1-out-of-2 redundancy).

The following examples illustrate the differences between a duplex fiber-optic ring and a dual electrical bus system.

Note

The number of connection resources required on the CPU depends on the network used.

When using a duplex fiber-optic ring (see figure below), two CPU resources are required on each CPU. In contrast, only one connection resource is required on each CP if a double electrical network (see figure after next) is used.

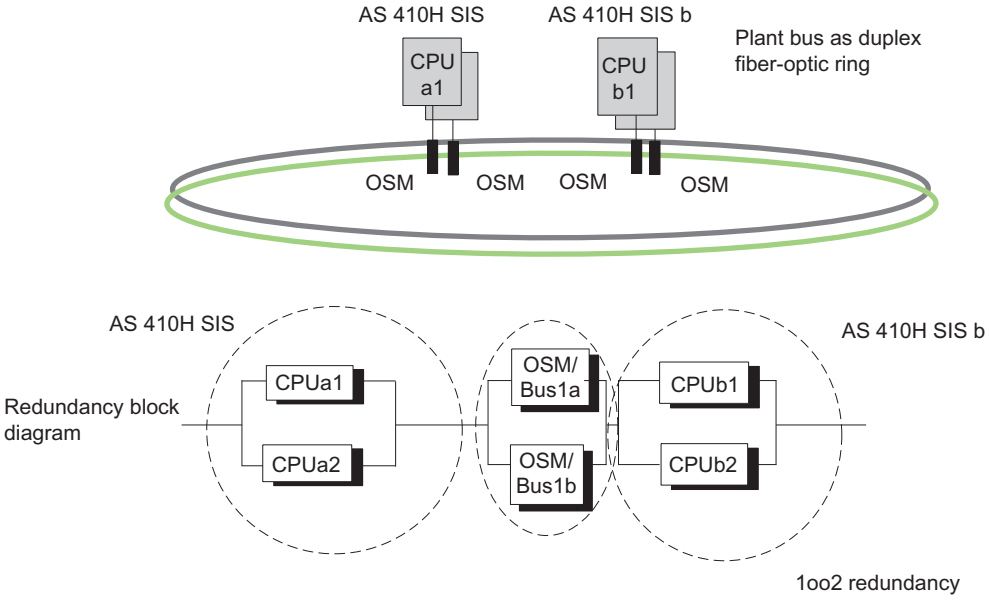
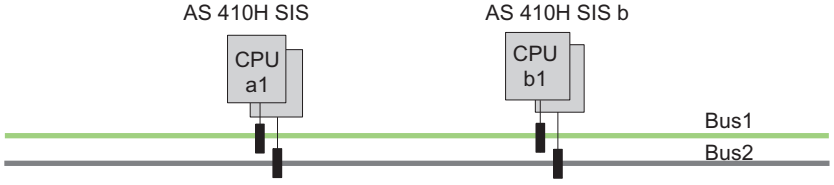


Figure 16-8 Example of redundancy with fault-tolerant system and redundant ring

Configuration view ≠ Physical view



Redundancy block diagram

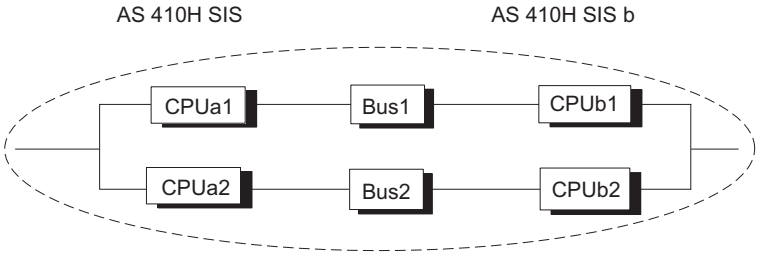


Figure 16-9 Example of redundancy with fault-tolerant system and redundant bus system

Configuration view = Physical view

Response to failure

With a duplex optic-fiber ring, only a double error within a fault-tolerant system, e.g., CPUa1 and CPUa2 in one system, leads to total failure of communication between the systems involved (see Figure 16-14).

Fault-tolerant S7 connections

Any disruption of subconnections while communication jobs are active over fault-tolerant S7 connections leads to extended delay times.

16.7.2 Communication between fault-tolerant systems and a fault-tolerant CPU

Availability

Availability can be enhanced by using a redundant plant bus and by using a fault-tolerant CPU in a standard system.

If the communication peer is a fault-tolerant CPU, redundant connections can also be configured, in contrast to systems with a standard CPU.

Note

High-availability connections occupy two connection resources on CPU b1 for the redundant connections. One connection resource is allocated to the CPU a1 and one to CPU a2.

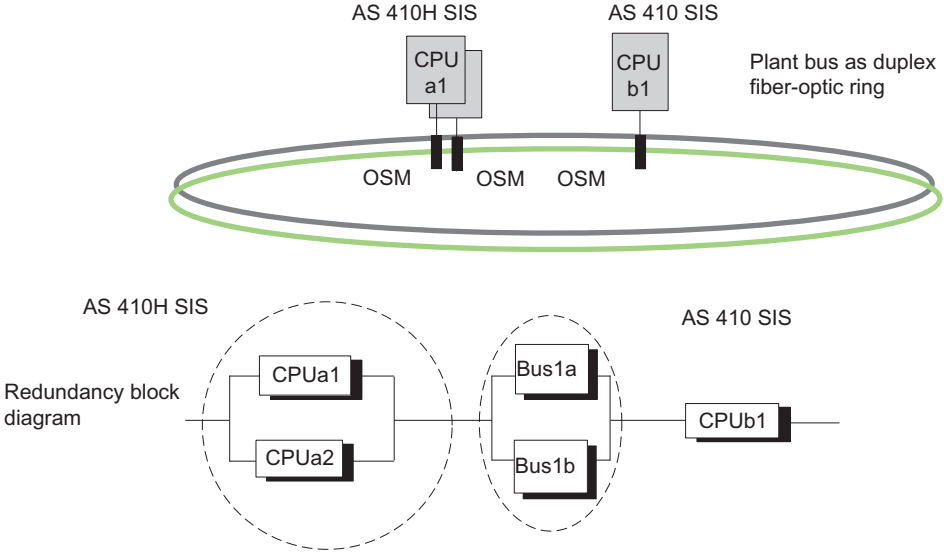


Figure 16-10 Example of redundancy with fault-tolerant system and fault-tolerant CPU

Response to failure

Double errors in the high-availability system, that is CPU a1 and CPU a2, or single errors in the standard system, CPU b1, result in total failure of the communication between the systems involved. This can be seen in the previous figure.

16.7.3 Communication between fault-tolerant systems and PCs

Availability

PCs are not fault-tolerant due to their hardware and software characteristics. The availability of a PC (OS) system and its data management is ensured by means of suitable software such as WinCC Redundancy.

Communication takes place via fault-tolerant S7 connections.

The "S7-REDCONNECT" software package is required for fault-tolerant communication on a PC. S7-REDCONNECT is used to connect a PC to a redundant bus system using one or two CPs. The second CP is merely used to redundantly connect the PC to the bus system and does not increase the availability of the PC. Always use the latest version of this software.

Only Industrial Ethernet is supported for connecting PC systems. The SIMATIC Net software V 8.1.2 is required for connection via ISOonTCP. This corresponds to the configuration TCP/RFC1006 at the PC end.

Note

The PROFINET IO MRP (Media Redundancy Protocol) for PROFINET IO ring topologies is not supported by SIMATIC NET PC modules. Plant buses as duplex fiber-optic rings cannot be operated with MRP.

Configuring connections

The PC must be engineered and configured as a SIMATIC PC station. Additional configuration of fault-tolerant communication is not necessary at the PC end. The connection configuration is uploaded from the STEP 7 project to the PC station.

You can find out how to use STEP 7 to integrate fault-tolerant S7 communication for a PC into your OS system in the WinCC documentation.

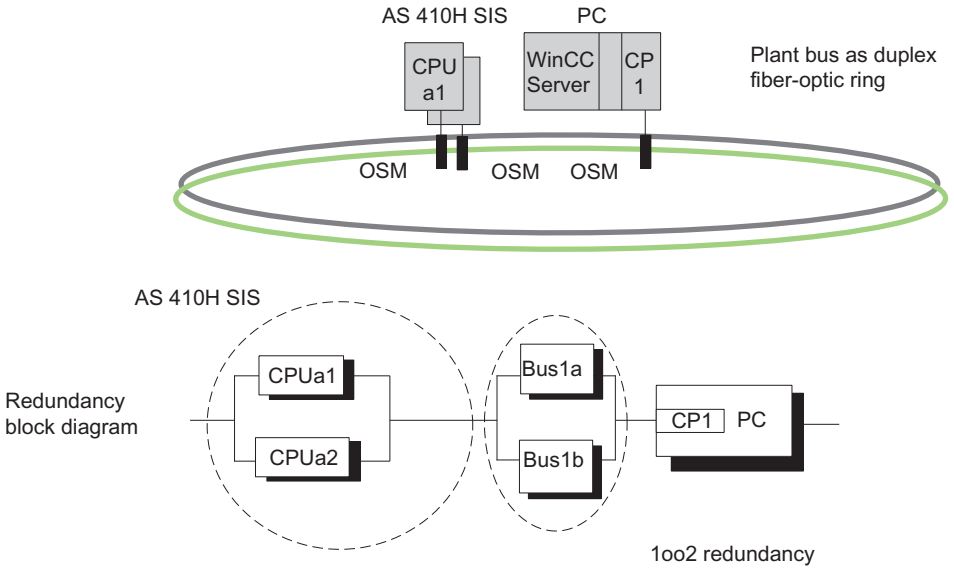


Figure 16-11 Example of redundancy with fault-tolerant system and redundant bus system

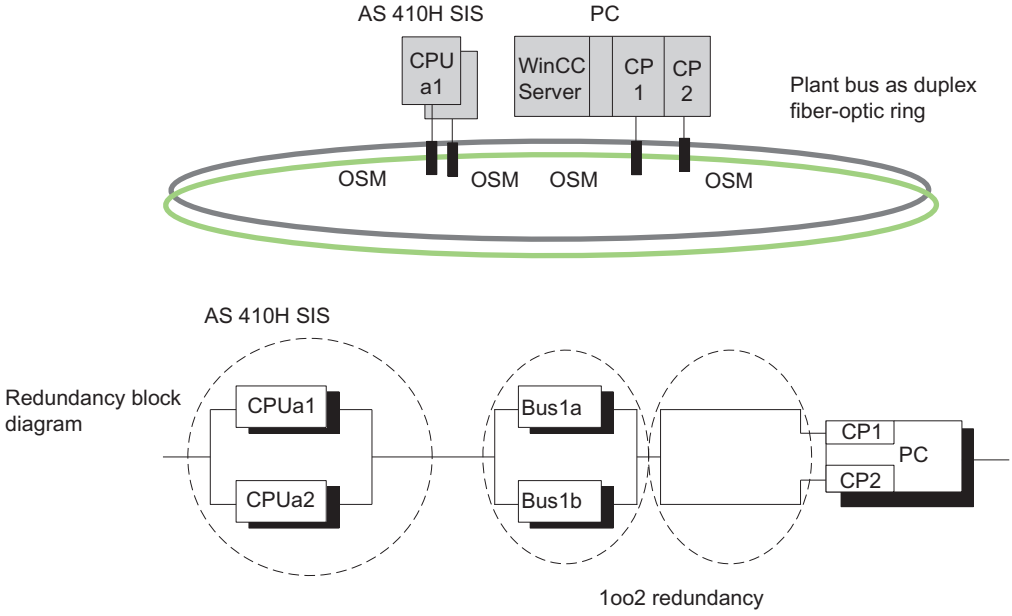


Figure 16-12 Example of redundancy with a fault-tolerant system, redundant bus system and redundant connection to the PC.

Response to failure

Double errors in the high-availability system, for example CPUa1 and CPUa2, or the failure of the PC station result in total failure of the communication between the systems involved, see previous figures.

PC/PG as Engineering System (ES)

If you want to use a PC as an engineering system, you must configure it under its name as a PC station in HW Config. The ES is assigned to a CPU and is capable of executing STEP 7 functions on that CPU.

If this CPU fails, communication between the ES and the fault-tolerant system is no longer possible.

16.8 Link-up and update sequence

There are two types of link-up and update operation:

- Within a "normal" link-up and update operation, the fault-tolerant system will change over from solo operation to redundant system state. The two CPUs then process the same program synchronously.
- When a link up and update operation takes place with master/standby changeover, the second CPU with modified components can assume control over the process. Either the hardware configuration or the operating system may have been modified.
  In order to return to redundant system state, a "normal" link-up and update operation must be performed subsequently.

How to start the link-up and update operation?

Initial situation: Solo operation, i.e., only one of the CPUs of a fault-tolerant system connected via fiber-optic cables is in RUN operating state.

You can initiate the link-up and update operation for achieving the redundant system state as follows:

- POWER ON the standby if prior to POWER OFF the CPU was not in STOP operating state.
- Operator input on the PG/ES.

You can only start a link-up and update operation with master/standby changeover by an operator input on the PG/ES.

Note

If a link-up and update operation is interrupted on the standby CPU (for example due to POWER OFF, STOP), this may cause data inconsistency and lead to a memory reset request on this CPU.

The link-up and update functions are possible again after a memory reset on the standby.

Flow chart of the link-up and update operation

The figure below outlines the general sequence of the link-up and update. In the initial situation, the master is in solo operation. In the figure, CPU 0 is assumed to be the master CPU.

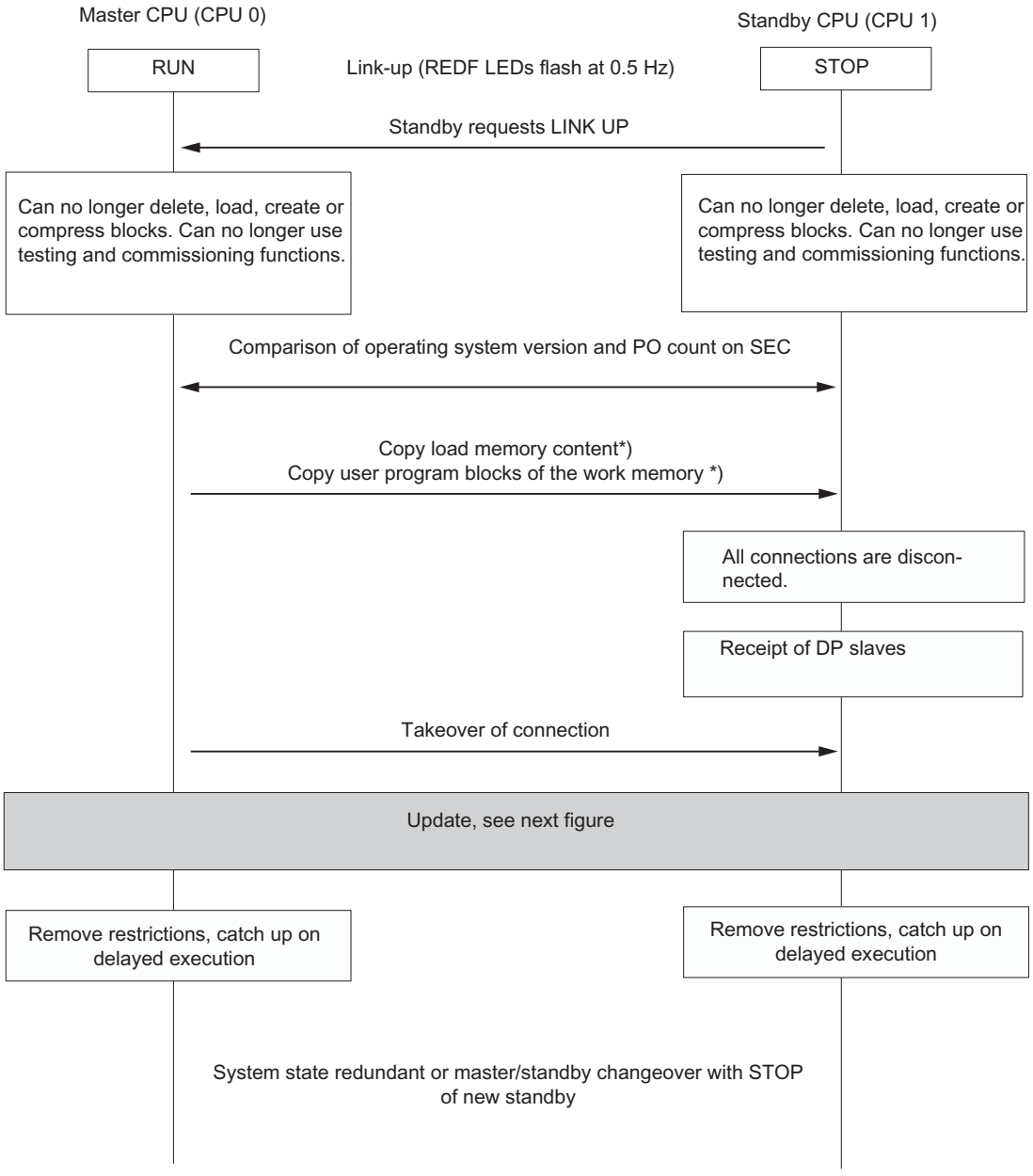


Figure 16-13 Sequence of link-up and update

*) If the "Switchover to CPU with modified configuration" option is set, the content of the load memory is not copied; what is copied from the user program blocks of the work memory (OBs, FCs, FBs, DBs, SDBs) of the master CPU is listed in Chapter Switch to CPU with modified configuration (Page 230)

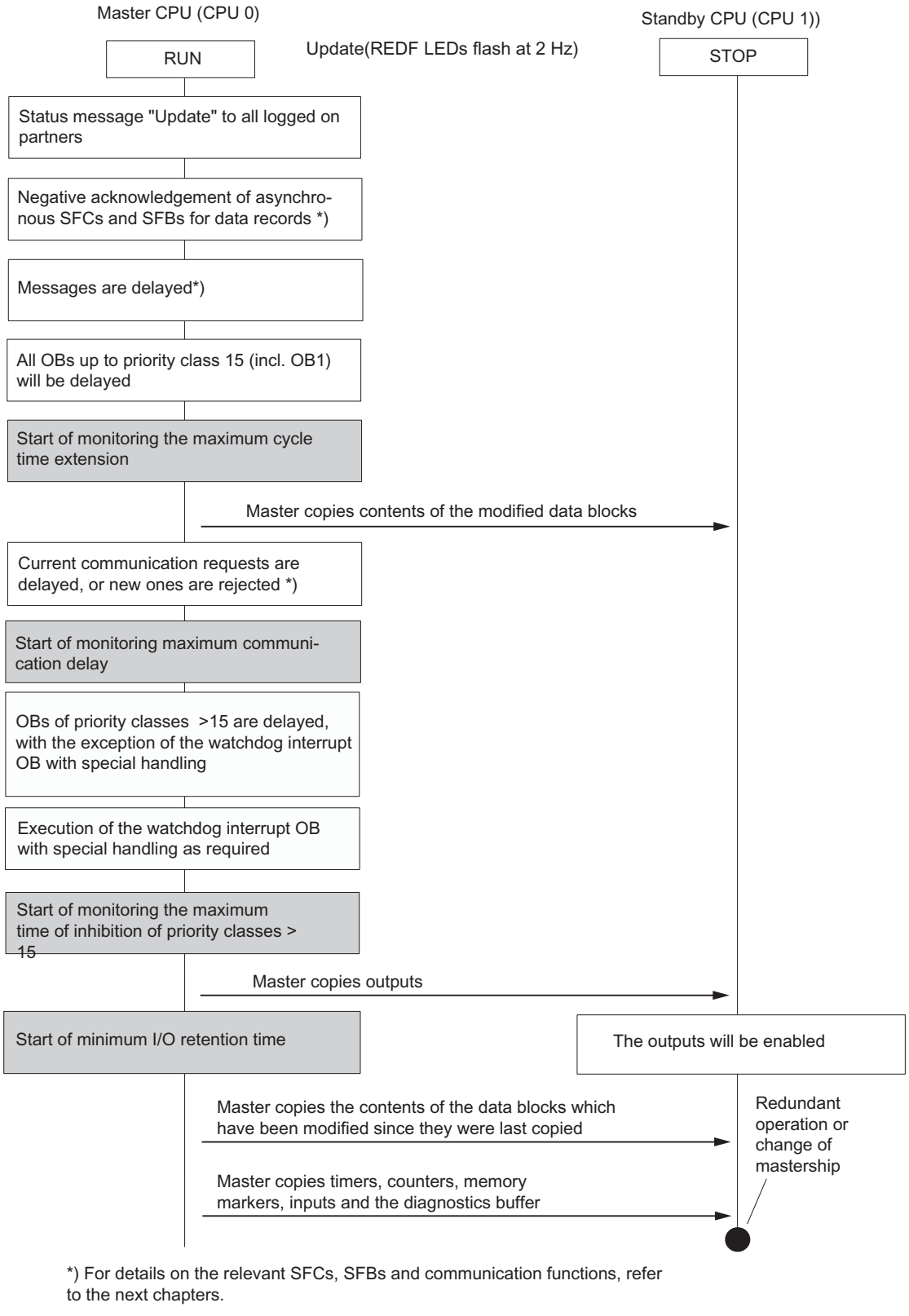


Figure 16-14 Update sequence

Minimum duration of input signals during update

Program execution is stopped for a certain time during the update (the sections below describe this in greater detail). To ensure that the CPU can reliably detect changes to input signals during the update, the following condition must be satisfied:

Minimum signal duration > 2 × time required for I/O update (DP and PNIO only)
+ call interval of the priority class
+ execution time for the program of the priority class
+ update time
+ execution time for programs of higher-priority classes

Example:

Minimum signal duration of an input signal that is evaluated in a priority class > 15 (e.g., OB 40).

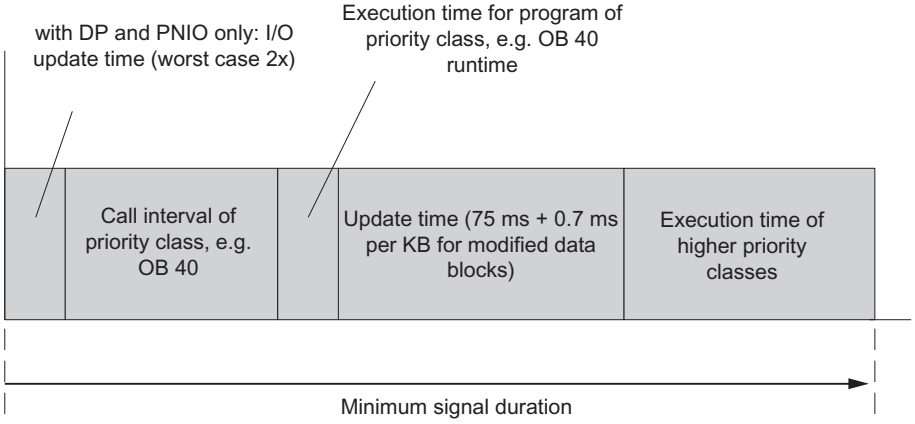


Figure 16-15 Example of minimum signal duration of an input signal during the update

16.8.1 Link-up sequence

For the link-up sequence, you need to decide whether to carry out a master/standby changeover, or whether the redundant system state is to be achieved after that.

Link-up with the objective of achieving the redundant system state

To exclude differences in the two subsystems, the master and the standby CPU run the following comparisons.

The following are compared:

1. Consistency of the memory configuration
2. Consistency of the operating system version
3. Consistency of the contents in load memory

If 1. or 2. are inconsistent, the standby CPU switches to STOP and outputs an error message.

If 3. is inconsistent, the user program in the load memory in RAM is copied from the master CPU to the standby CPU.

Link-up with master/standby changeover

In STEP 7 you can select one of the following options:

- "Switch to CPU with modified configuration"
- "Switchover to CPU with modified operating system"
- "Switchover to CPU with modified hardware version"
- "Switchover to CPU via only one intact redundant link"

Switch to CPU with modified configuration

You may have modified the following elements on the standby CPU:

- The hardware configuration

No blocks are transferred from the master to the standby during the link-up. The exact circumstances are described in Chapter Switch to CPU with modified configuration (Page 230).

For information on steps required in the scenarios mentioned above, refer to section Replacement of failed components during redundant operation (Page 165).

Note

Even though you have not modified the hardware configuration on the standby CPU, there is nevertheless a master/standby changeover and the previous master CPU switches to STOP.

16.8.2 Update sequence

What happens during updating?

The execution of communication functions and OBs is restricted section by section during updating. Likewise, all the dynamic data (content of the data blocks, timers, counters, and bit memories) are transferred to the standby CPU.

Update procedure:

1. Until the update is completed, all asynchronous SFCs and SFBs which access data records of I/O modules (SFCs 13, 51, 52, 53, 55 to 59, SFB 52 and 53) are acknowledged as "negative" with the return values W#16#80C3 (SFCs 13, 55 to 59, SFB 52 and 53) or W#16#8085 (SFC 51). When these values are returned, the jobs should be repeated by the user program.
2. Message functions are delayed until the update is completed (see list below).
3. The execution of OB 1 and of all OBs up to priority class 15 is delayed.
   In the case of cyclic interrupts, the generation of new OB requests is disabled, so no new cyclic interrupts are stored and as a result no new request errors occur.
   The system waits until the update is completed, and then generates and processes a maximum of one request per cyclic interrupt OB. The time stamp of delayed cyclic interrupts cannot be evaluated.
4. Transfer of all data block contents modified since link-up.

5. The following communication jobs are acknowledged negatively:
   - Reading/writing of data records using HMI functions
   - Reading diagnostic information using STEP 7
   - Disabling and enabling messages
   - Logon and logoff for messages
   - Acknowledgement of messages
6. Initial calls of communication functions are acknowledged negatively. These calls manipulate the work memory, see also *System Software for S7-300/400, System and Standard Functions*. All remaining communication functions are executed with delay, after the update is completed.
7. The system disables the generation of new OB requests for all OBs of priority class > 15, so new interrupts are not saved and as a result do not generate any request errors. Queued interrupts are not requested again and processed until the update is completed. The time stamp of delayed interrupts cannot be evaluated.
   The user program is no longer processed and there are no more I/O updates.
8. Generating the start event for the cyclic interrupt OB with special handling.

   Note

   The cyclic interrupt OB with special handling is particularly important in situations where you need to address certain modules or program parts within a specific time. This is a typical scenario in fail-safe systems. For details, refer to the *S7-400F and S7-400FH Automation Systems* and *S7-300 Automation Systems, Fail-safe Signal Modules* manuals.

   To prevent an extension of the special cyclic interrupt, the cyclic alarm OB with special handling must be assigned top priority.

9. Transfer of outputs and of all data block contents modified again. Transfer of timers, counters, bit memories, and inputs. Transfer of the diagnostic buffer.
   During this data synchronization, the system interrupts the clock pulse for cyclic interrupts, time-delay interrupts and S7 timers. This results in the loss of any synchronism between cyclic and time-of-day interrupts.
10. Cancel all restrictions. Delayed interrupts and communication functions are executed. All OBs are executed again.
    A constant bus cycle time compared with previous calls can no longer be guaranteed for delayed cyclic interrupt OBs.

    Note

    Process interrupts and diagnostic interrupts are stored by the I/O devices. Such interrupt requests issued by distributed I/O modules are executed when the block is re-enabled. Any such requests by central I/O modules can only be executed provided the same interrupt request did not occur repeatedly while the status was disabled.

If the PG/ES requested a master/standby changeover, the previous standby CPU assumes master mode and the previous master CPU goes into STOP when the update is completed. Both CPUs will otherwise go into RUN (redundant system mode) and execute the user program in synchronism.

When there is a master/standby changeover, in the first cycle after the update OB 1 is assigned a separate identifier (see *System Software for S7-300/400, System and Standard Functions* Reference Manual). For information on other aspects resulting from modifying the configuration, refer to section Switch to CPU with modified configuration (Page 230).

Delayed message functions

The listed SFCs, SFBs and operating system services trigger the output of messages to all logged-on partners. These functions are delayed after the start of the update:

- SFC 17 "ALARM_SQ", SFC 18 "ALARM_S", SFC 107 "ALARM_DQ", SFC 108 "ALARM_D"
- SFC 52 "WR_USMSG"
- SFB 31 "NOTIFY_8P", SFB 33 "ALARM", SFB 34 "ALARM_8", SFB 35 "ALARM_8P", SFB 36 "NOTIFY", SFB 37 "AR_SEND"
- Process control alarms
- System diagnostics messages

From this time on, any requests to enable and disable messages by SFC 9 "EN_MSG" and SFC 10 "DIS_MSG" are rejected with a negative return value.

Communication functions and resulting jobs

After it has received one of the jobs specified below, the CPU must in turn generate communication jobs and output them to other modules. These include, for example, jobs for reading or writing parameterization data records from/to distributed I/O modules. These jobs are rejected until the update is completed.

- Reading/writing of data records using HMI functions
- Reading data records using SSL information
- Disabling and enabling messages
- Logon and logoff for messages
- Acknowledgement of messages

Note

The last three of the functions listed are registered by a WinCC system, and automatically repeated when the update is completed.

16.8.3 Switch to CPU with modified configuration

Switch to CPU with modified configuration

You may have modified the hardware configuration on the standby CPU. The necessary steps are described in Section Replacement of failed components during redundant operation (Page 165).

Note

Even though you have not modified the hardware configuration on the standby CPU, there is nevertheless a master/standby changeover and the previous master CPU switches to STOP.

When you initiate the link-up and update operation from STEP 7 with the "Switch to CPU with modified configuration" option, the system reacts as follows with respect to handling of the memory contents.

Load memory

The content of the load memory is not copied by the master CPU to the reserve CPU.

Work memory

The following components are transferred from the work memory of the master CPU to the standby CPU:

- Content of all data blocks that have the same interface time stamp in both load memories and whose "write protected" and "unlinked" attributes are not set.
- Data blocks that were generated in the master CPU by SFC.
  The DBs generated by SFC in the standby CPU are deleted.
  If a data block with the same number is also contained in the load memory of the standby CPU, the link to an entry in the diagnostic buffer is removed.
- Process images, timers, counters, and bit memories

If data blocks containing instances of SFBs of S7 communication have been changed, these instances are reset to the state before the first call.

16.8.4 Disabling of link-up and update

Link-up and update entails a cycle time extension. This includes a period during which no I/O updates are performed; see Chapter Time monitoring (Page 90). You must pay special attention to this if you are using distributed I/O and a master/standby changeover occurs after the update (thus, when the configuration is modified during operation).

CAUTION

Caution: Personal injury and property damage

Always perform link-up and update operations when the process is not in a critical state.

You can set specific start times for link-up and update operations at SFC 90 "H_CTRL". For detailed information on this SFC, refer to Manual *System Software for S7-300/400, System and Standard Functions*.

Note

If the process tolerates cycle time extensions at any time, you do not need to call SFC 90 "H_CTRL".

The CPU does not perform a self-test during link-up and updating. If you use a fail-safe user program, you should avoid any excessive delay for the update operation. For more details, refer to Manual *S7-400F and S7-400FH Automation Systems*.

Example of a time-critical process

A slide block with a 50 mm cam moves on an axis at a constant velocity v = 10 km/h = 2.78 m/s = 2.78 mm/ms. A switch is located on the axis. So the switch is actuated by the cam for the duration of Δt = 18 ms.

For the CPU to detect the actuation of the switch, the inhibit time for priority classes > 15 (see below for definition) must be significantly below 18 ms.

With respect to maximum inhibit times for operations of priority class > 15, STEP 7 only supports settings of 0 ms or between 100 and 60000 ms, so you need to work around this by taking one of the following measures:

- Shift the start time of link-up and updating to a time at which the process state is non-critical . Use SFC 90 "H_CTRL" to set this time (see above).
- Use a considerably longer cam and/or substantially reduce the approach velocity of the slide block to the switch.

16.9 The user program

The rules of developing and programming the user program for the standard S7-400 system also apply to the S7-400H.

In terms of user program execution, the S7-400H behaves in the same manner as a standard system. The synchronization functions are integrated in the operating system and are executed automatically in the background. You do not need to consider these functions in your user program.

In redundant operation, the user programs are stored identically on both CPUs and are executed in event-synchronous mode.

However, we offer you several specific blocks for optimizing your user program, e.g., in order to improve its response to the extension of cycle times due to updates.

Specific blocks for S7–400H

In addition to the blocks that can be used both in S7-400 and in S7-400H, there are additional blocks for S7-400H. You can use these blocks to influence redundancy functions.

You can react to redundancy errors of the S7-400H using the following organization blocks:

- OB 70, I/O redundancy errors
- OB 72, CPU redundancy errors

SFC 90 "H_CTRL" can be used to influence fault-tolerant systems as follows:

- You can disable interfacing in the master CPU.
- You can disable updating in the master CPU.
- You can remove, resume or immediately start a test component of the cyclic self-test.
- You can execute a programmed master-standby changeover. The following changeovers are possible:
  - The current standby CPU becomes the master CPU.
  - The CPU in rack 0 becomes a master CPU.
  - The CPU in rack 1 becomes a master CPU.

Additional information

For detailed information on programming the blocks described above, refer to the STEP 7 Online Help.

16.10 Cycle and response times of the CPU 410SIS

16.10.1 Cycle time

This chapter describes the decisive factors in the cycle time, and how to calculate it.

Definition of cycle time

The cycle time represents the time that the operating system needs to execute a program, that is, one OB 1 cycle, including all program sections and system activities interrupting this cycle.

This time is monitored. The CPU 410SIS has a fixed cycle time monitoring of 6 seconds.

Time slice model

Cyclic program processing, and therefore also user program processing, is based on time slices. To demonstrate the processes, let us presume a global time slice length of exactly 1 ms.

Process image

So that the CPU provides a consistent process signal image for the duration of the cyclic program execution, the process signals are read or written before program execution. During program execution, the CPU does not access the signal modules directly when addressing the operand areas for inputs (I) and outputs (Q) It accesses the CPU's system memory area containing the image of the inputs and outputs.

Sequence of cyclic program processing

The table below shows the various phases in cyclic program execution.

Table 16-3 Cyclic program processing

Step	Sequence
1	The operating system initiates the scan cycle monitoring time.
2	The CPU copies the values from the process output images to the output modules.
3	The CPU reads the status of inputs of the input modules, and then updates the process image of the inputs.
4	The CPU processes the user program in time slices and executes the instructions specified in the program.
5	At the end of a cycle, the operating system executes pending tasks, e.g., loading and deleting of blocks.
6	Finally, on expiration of any given minimum cycle time, the CPU returns to the start of the cycle and restarts cycle monitoring.

Elements of the cycle time

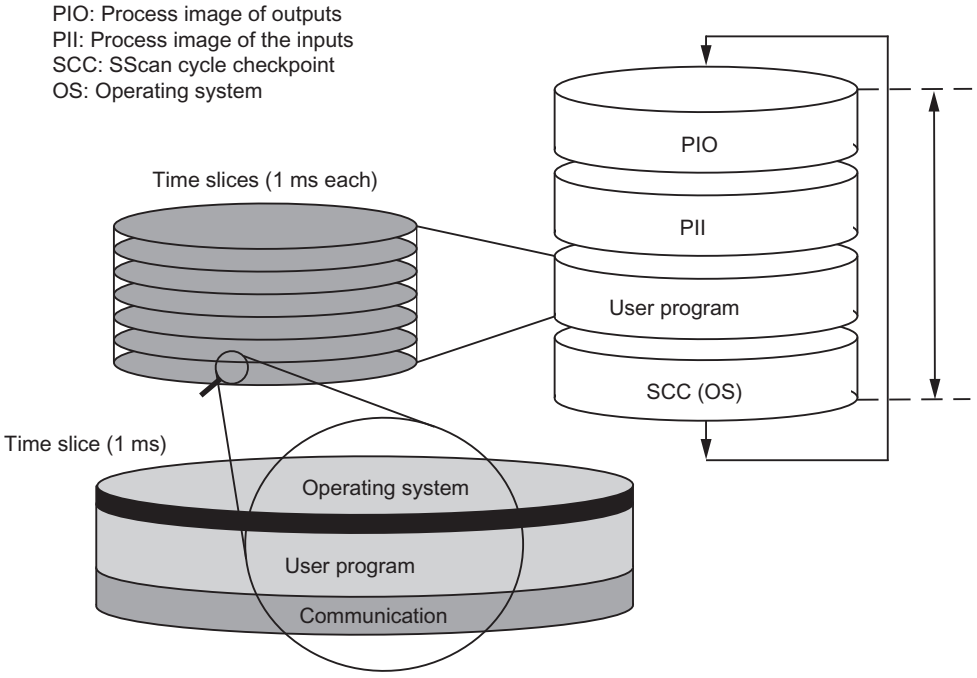


Figure 16-16 Elements and composition of the cycle time

16.10.2 Calculating the cycle time

Extending the cycle time

The cycle time of a user program is extended by the factors outlined below:

- Time-based interrupt processing
- Hardware interrupt processing (see also Chapter Interrupt response time (Page 245))
- Diagnostics and error handling
- Communication via the integrated PROFINET interface; contained in the communication load
- Special functions such as monitoring and modifying variables or the block status
- Transfer and deletion of blocks, compressing of the user program memory
- Runtime of signals using the synchronization cable

Influencing factors

The table below shows the factors influencing the cycle time.

Table 16-4 Factors influencing cycle time

Factors	Remark
Transfer time for the process image of outputs (PIQ) and the process image of inputs (PII)	See tables 16-3 onwards
User program execution time	This value is calculated based on the execution times of the various statements (see the *S7-400 statement list*).
Operating system execution time at the cycle control point	See Table 16-7
Extension of cycle time due to communication load	You configure the maximum permitted communication load on the cycle as a percentage in **STEP 7** (Manual *Programming with STEP 7*). See Chapter Cycle load due to communication (Page 237).
Load on cycle times due to interrupts	Interrupt requests can always stop user program execution. See Table 16-8

Process image update

The table below shows the time a CPU requires to update the process image (process image transfer time). The specified times only represent "ideal values", and may be extended accordingly by any interrupts or communication of the CPU.

Calculation of the transfer time for process image update:

K + portion in the central controller (from row A in the following table)
+ portion via integrated DP interface (from row D1)
+ portion of consistent data via integrated DP interface (from row E1)

= Transfer time for process image update

The tables below show the various portions of the transfer time for a process image update (process image transfer time). The specified times only represent "ideal values", and may be extended accordingly by any interrupts or communication of the CPU.

Table 16-5 Portions of the process image transfer time, CPU 410SIS

	Portions	CPU 410SIS stand-alone operation	CPU 410SIS redundant
K	Base load	2 µs	3 µs
A	In the central controller Read/write byte/word/double word	7.3 µs	15 µs
D1	In the DP area for the integrated DP interface Read byte/word/double word	0.4 µs	10 µs
E1	Consistent data in the process image for the integrated DP interface Read/write data	8 µs	30 µs

Extending the cycle time

For CPU 410SIS, you must also multiply the calculated cycle time by a CPU-specific factor. The table below lists these factors:

Table 16-6 Extending the cycle time

Startup	CPU 410SIS stand-alone operation	CPU 410SIS redundant
Factor	1.05	1.2

Long synchronization cables may increase cycle times. This extension can have the factor 2 - 5 with a cable length of 10 km.

Operating system execution time at the cycle control point

The table below shows the operating system execution time at the cycle checkpoint of the CPUs.

Table 16-7 Operating system execution time at the cycle control point

Sequence	CPU 410SIS stand-alone operation	CPU 410SIS redundant
Cycle control at the SCCP	25 - 330 µs ∅ 30 µs	120 - 600 µs ∅ 135 µs

Extended cycle time due to nested interrupts

Table 16-8 Extended cycle time due to nested interrupts

CPU	Hardware interrupt	Diagnostic interrupt	Time-of-day interrupt	Delay interrupt	Cyclic interrupt	Programming error	I/O access error	Asynchronous error
CPU 410SIS stand-alone operation	75 µs	40 µs	50 µs	40 µs	40 µs	20 µs	20 µs	55 µs
CPU 410SIS redundant	180 µs	70 µs	200 µs	120 µs	120 µs	90 µs	45 µs	130 µs

The program runtime at interrupt level must be added to this time extension.

If several interrupts are nested, their times must be added together.

16.10.3 Cycle load due to communication

The operating system of the CPU provides the configured percentage of the overall CPU processing capacity to the communication on a continuous basis (time slice technique). If this processing capacity is not required for communication, it is made available to the other processing.

In the hardware configuration you can specify a communication load value between 5% and 50%. The default value is 20%.

The parameter represents the share of the cycle load in the internal copy jobs created at the communication end. Communication at the interfaces is not affected.

This percentage is to be interpreted as a mean value, i.e., within one time slice, the communication portion may be significantly greater than 20%. On the other hand, communication load in the next time slice is very small or not present.

The formula below describes the influence of communication load on the cycle time:

$$\text{Actual cycle time} = \text{Cycle time} \times \frac{100}{100 - \text{"Configured communication load in \%"}}$$

Round the result up to the next highest integer !

Figure 16-17 Formula: Influence of communication load

Data consistency

The user program is interrupted to process communications. This interruption can be triggered after any command. These communication jobs may lead to a change in user data. As a result, data consistency cannot be ensured over several accesses.
How to ensure data consistency in operations comprising more than one command is described in Chapter "Consistent data".

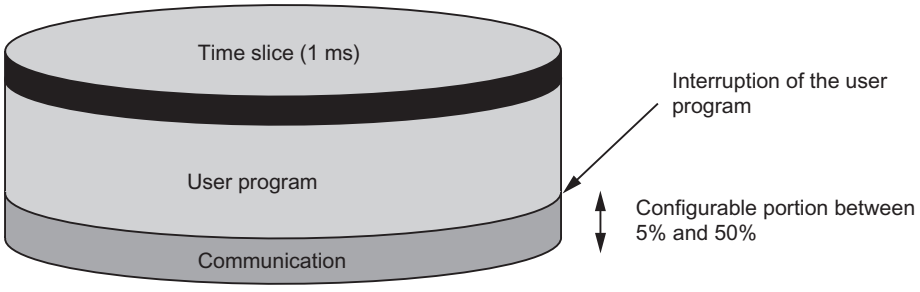


Figure 16-18 Distribution of a time slice

The operating system takes a certain portion of the remaining time slice for internal tasks. This portion is included in the factor defined in the tables starting at 16-3.

Example: 20% communication load

In the hardware configuration you have set a communication load of 20%.

The calculated cycle time is 10 ms.

This means that a setting of 20% communication load allocates an average of 200 µs to communication and 800 µs to the user program in each time slice. So the CPU requires 10 ms / 800 µs = 13 time slices to execute one cycle. This means the physical cycle time is equivalent to 13 times 1-ms time slice = 13 ms, if the CPU fully utilizes the configured communication load.

That is to say, 20% communication does not extend the cycle by a linear amount of 2 ms, but by 3 ms.

Example: 50% communication load

You configured a communication load of 50% in the hardware configuration.

The calculated cycle time is 10 ms.

This means that 500 µs remain in each time slice for the cycle. Therefore, the CPU requires 10 ms / 500 µs = 20 time slices to execute one cycle. This means the physical cycle time is 20 ms if the CPU fully utilizes the configured communication load.

So a setting of 50% communication load allocates 500 µs to communication and 500 µs to the user program in each time slice. Therefore, the CPU requires 10 ms / 500 µs = 20 time slices to execute one cycle. This means the physical cycle time is equivalent to 20 times 1-ms time slice = 20 ms, if the CPU fully utilizes the configured communication load.

This means that 50% communication does not extend the cycle by a linear amount of 5 ms, but by 10 ms (= doubling the calculated cycle time).

Dependency of the actual cycle time on communication load

The figure below describes the non-linear dependency of the actual cycle time on communication load. In our example we have chosen a cycle time of 10 ms.

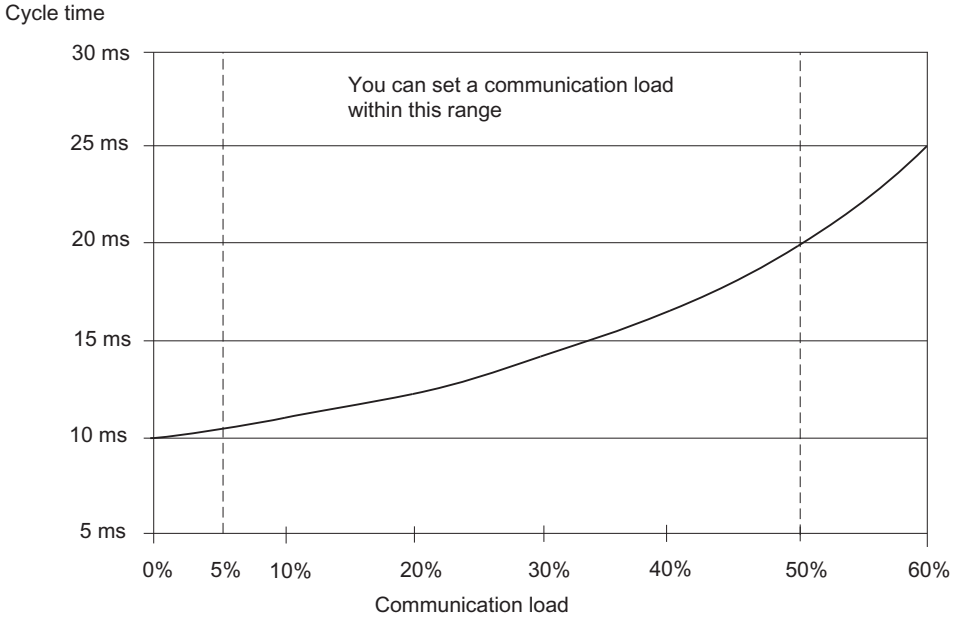


Figure 16-19 Dependency of the cycle time on communication load

Further effects on the actual cycle time

Seen statistically, the extension of cycle times due to communication load leads to more asynchronous events occurring within an OB 1 cycle, for example interrupts. This further extends the OB 1 cycle. How much it is extended depends on the number of events per OB 1 cycle and the time required for processing these events.

Remarks

- Change the value of the "communication load" parameter to check the effects on the cycle time during system runtime.
- Always take the communication load into account when you set the maximum cycle time, otherwise you risk timeouts.

16.10.4 Response time

Definition of response time

The response time is the time from detecting an input signal to changing the output signal associated with it.

Fluctuation range

The actual response time lies between the shortest and the longest response time. You must always assume the longest response time when configuring your system.

The shortest and longest response times are analyzed below so that you can gain an impression of the variation of the response time.

Factors

The response time depends on the cycle time and the following factors:

- Delay of the inputs and outputs
- Additional DP cycle times on the PROFIBUS DP network
- Execution in the user program

Delay of inputs/outputs

Make allowances for the following module-specific delay times:

- For digital inputs: the input delay time
- For interrupt-capable digital inputs: the input delay time + internal preparation time
- For digital outputs: negligible delay times

- For relay outputs: Typical delay times of 10 to 20 ms.
  The delay of the relay outputs is dependent on the temperature and voltage, among other things.
- For analog inputs: cycle time for analog input
- For analog outputs: response time at analog outputs

For information on delay times, refer to the technical specifications of the signal modules.

DP cycle times on the PROFIBUS DP network

If you configured your PROFIBUS DP network in **STEP 7**, **STEP 7** calculates the typical DP cycle time to be expected. You can then view the DP cycle time of your configuration on the PG in the bus parameters section.

The figure below provides an overview of the DP cycle time. In this example, we assume an average value for each DP slave of 4 bytes of data.

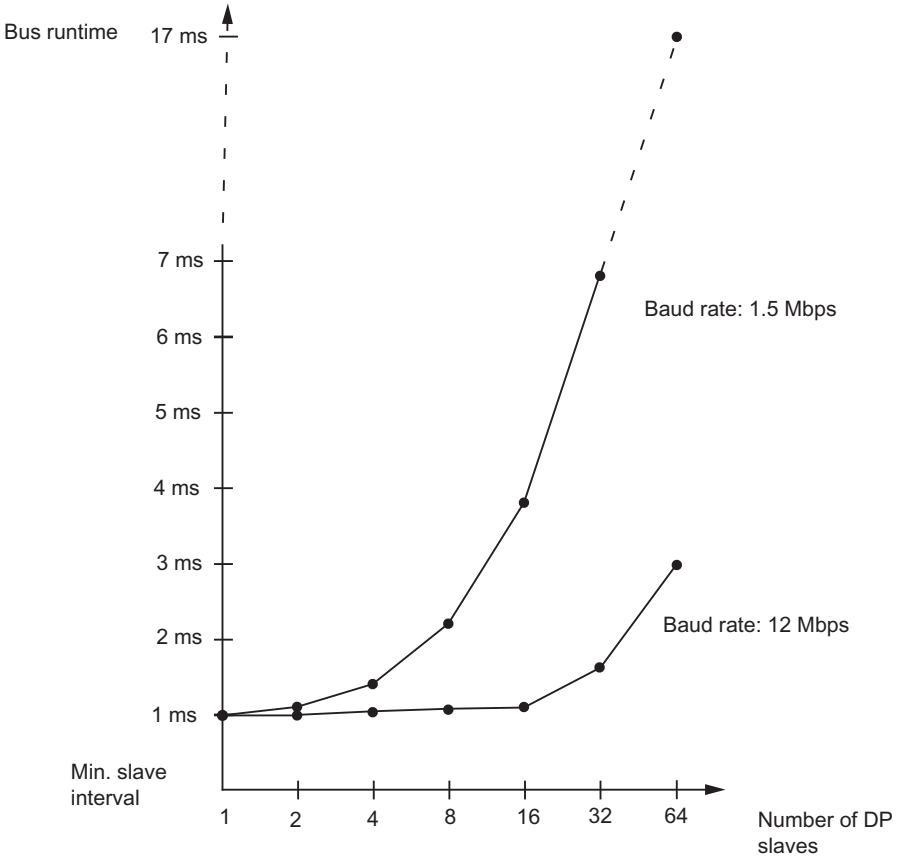


Figure 16-20 DP cycle times on the PROFIBUS DP network

Shortest response time

The figure below shows the conditions under which the shortest response time is achieved.

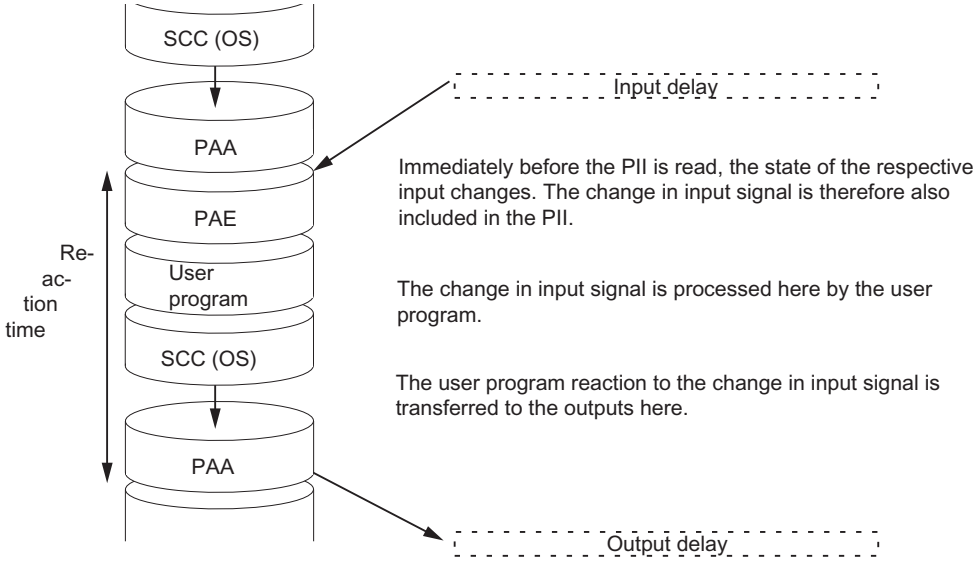


Figure 16-21 Shortest response time

Calculation

The (shortest) response time is calculated as follows:

- 1 x process image transfer time of the inputs +
- 1 x process image transfer time of the outputs +
- 1 x program processing time +
- 1 x operating system processing time at the SCCP +
- Delay of the inputs and outputs

The result is equivalent to the sum of the cycle time plus the I/O delay times.

Note

You must add the double runtime of the DP slave telegram (including processing in the DP master).

Longest response time

The figure below shows the conditions under which the longest response time is achieved.

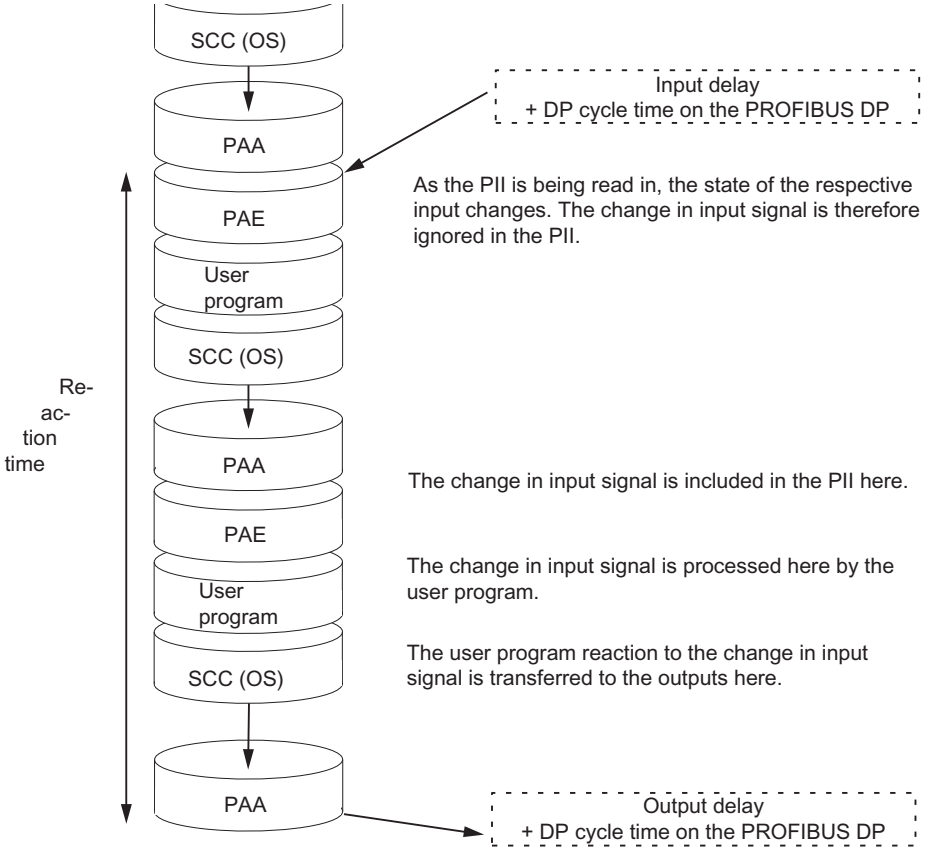


Figure 16-22 Longest response time

Calculation

The (longest) response time is calculated as follows:

- 2 x process image transfer time of the inputs +
- 2 x process image transfer time of the outputs +
- 2 x operating system processing time +
- 2 x program processing time +
- 2 x delay of the DP slave frame (including processing in the DP master) +
- Delay of the inputs and outputs

This is equivalent to the sum of twice the cycle time and the delay in the inputs and outputs plus twice the DP cycle time.

Processing direct I/O access

You can achieve faster response times by directly accessing the I/O in your user program, e.g., with the following instructions:

- L PIB
- T PQW

However, note that any I/O access requires a synchronization of the two units and thus extends the cycle time.

Reducing the response time

This reduces the maximum response time to

- Delay of the inputs and outputs
- Runtime of the user program (can be interrupted by higher-priority interrupt processing)
- Runtime of direct access
- 2x bus runtime of DP

Note

You can also achieve fast response times by using hardware interrupts; see Chapter Interrupt response time (Page 245).

16.10.5 Calculating cycle and response times

Cycle time

1. Determine the user program runtime with the help of the instruction list.
2. Calculate and add the process image transfer time. You will find guide values for this in the tables starting at 16-3.
3. Add the processing time at the scan cycle checkpoint. You will find guide values for this in Table 16-8.
4. Multiply the calculated value by the factor in Table 16-7.

The final result is the **cycle time**.

Extension of the cycle time due to communication and interrupts

1. Multiply the result by the following factor:
   100 / (100 – "configured communication load in %")
2. Using the instruction list, calculate the runtime of the program elements processing the interrupts. To do so, add the relevant value from Table 16-9.
   Multiply this value by the factor from step 4.
   Add this value to the theoretical cycle time as often as the interrupt is triggered or is expected to be triggered during the cycle time.

The result is an approximated **actual cycle time**. Note down the result.

Table 16-9 Example of calculating the response time

Shortest response time	Longest response time
3. Next, calculate the delays in the inputs and outputs and, if applicable, the cycle times on the PROFIBUS DP network.	3. Multiply the actual cycle time by factor 2.
	4. Next, calculate the delays in the inputs and outputs and the DP cycle times on the PROFIBUS DP network.
4. The result you obtain is the **shortest response time**.	5. The result you obtain is the **longest response time**.

16.10.6 Interrupt response time

Definition of interrupt response time

The interrupt response time is the time from the first occurrence of an interrupt signal to the call of the first instruction in the interrupt OB.

General rule: Higher priority interrupts are handled first. This means the interrupt response time is increased by the program execution time of the higher-priority interrupt OBs, and by previous interrupt OBs of the same priority which have not yet been processed (queue).

Note that any update of the standby CPU extends the interrupt response time.

Calculating the interrupt response time

Minimum interrupt response time of the CPU
+ minimum interrupt response time of the signal modules
+ cycle time on PROFIBUS DP

= Shortest interrupt response time

Minimum interrupt response time of the CPU
+ maximum interrupt response time of the signal modules
+ 2 * cycle time on PROFIBUS DP

= Longest interrupt response time

Hardware and diagnostic interrupt response times of the CPUs

Table 16-10 Hardware and interrupt response times; maximum interrupt response time without communication

CPU	Hardware interrupt response times		Diagnostic interrupt response times	
	min.	max.	min.	max.
CPU 410SIS stand-alone operation	60 µs	90 µs	60 µs	90 µs
CPU 410SIS redundant	140 µs	310 µs	120 µs	250 µs

Increasing the maximum interrupt response time with communication

The maximum interrupt response time is extended when the communication functions are active. The additional time is calculated using the following formula:

CPU 410SIS t_v = 100 µs + 1000 µs × n%, may be significantly longer

where n = cycle load due to communication

Signal modules

The hardware interrupt response time of signal modules is made up as follows:

- Digital input modules
  Hardware interrupt response time = internal interrupt processing time + input delay
  You will find these times in the data sheet for the respective digital input module.
- Analog input modules
  Hardware interrupt response time = internal interrupt processing time + conversion time
  The internal interrupt processing time for analog input modules can be neglected. The conversion times can be found in the data sheet for the individual analog input modules.

The diagnostic interrupt response time of the signal modules is the time from detection of a diagnostic event by the signal module to the triggering of the diagnostic interrupt by the signal module. This short time can be neglected.

Hardware interrupt processing

Hardware interrupt processing begins when the hardware interrupt OB 4x is called. Higher-priority interrupts stop hardware interrupt processing. Direct access to I/O modules is executed during the execution time of the operation. After the hardware interrupt has been processed, the system either resumes cyclic program processing, or calls and processes interrupt OBs of the same or lower priority.

16.10.7 Reproducibility of delay and watchdog interrupts

Definition of "reproducibility"

Time-delay interrupt:

The period that expires between the call of the first operation in the interrupt OB and the programmed time of interrupt.

Cyclic interrupt:

The fluctuation range of the interval between two successive calls, measured between the respective initial operations of the interrupt OB.

Reproducibility

The following table contains the reproducibility of time-delay and cyclic interrupts of the CPUs.

Table 16-11 Reproducibility of time-delay and cyclic interrupts of the CPUs

Module	Reproducibility	
	Time-delay interrupt	Cyclic interrupt
CPU 410SIS stand-alone operation	± 120 µs	± 160 µs
CPU 410SIS redundant	± 200 µs	± 180 µs

These times only apply if the interrupt can actually be executed at this time and if it is not delayed, for example, by higher-priority interrupts or queued interrupts of equal priority.

16.11 Runtimes of the FCs and FBs for redundant I/Os

Table 16-12 Runtimes of the blocks for redundant I/Os

Block	Runtime in stand-alone/single mode	Runtime in redundant mode
FC 450 RED_INIT Specifications are based on the startup	2 ms + 300 µs / configured module pairs The specification for a module pair is a mean value. The runtime may be < 300 µs for a few modules. For a large number of redundant modules the value may be > 300 µs.	-
FC 451 RED_DEPA	160 µs	360 µs

Block	Runtime in stand-alone/single mode	Runtime in redundant mode
FB 450 RED_IN Called from the corresponding sequence level.	750 µs + 60 µs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be additionally increased if discrepancies occur resulting in passivation and logging to the diagnostic buffer. The runtime may also be increased by a depassivation carried out at the individual sequence levels of FB RED_IN. Depending on the number of modules in the sequence level, the depassivation may increase the runtime of the FB RED_IN by 0.4 ... 8 ms. An 8 ms increase can be expected in redundant operation of modules totaling more than 370 pairs of modules at a sequence level.	1000 µs + 70 µs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be additionally increased if discrepancies occur resulting in passivation and logging to the diagnostic buffer. The runtime may also be increased by a depassivation carried out at the individual sequence levels of FB RED_IN. Depending on the number of modules in the sequence level, the depassivation may increase the runtime of the FB RED_IN by 0.4 ... 8 ms. An 8 ms increase can be expected in redundant operation of modules totaling more than 370 pairs of modules at a sequence level.
FB 451 RED_OUT Called from the corresponding sequence level.	650 µs + 2 µs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be < 2 µs for a few modules. For a large number of redundant modules the value may be > 2 µs.	860 µs + 2 µs / module pair of the current TPA The specification for a module pair is a mean value. The runtime may be < 2 µs for a few modules. For a large number of redundant modules the value may be > 2 µs.
FB 452 RED_DIAG	Called in OB 72: 160 µs Called in OB 82, 83, 85: 250 µs + 5 µs / configured module pairs Under extreme conditions the runtime of FB RED_DIAG is increased up to 1.5 ms. . This is the case when the working DB is 60 KB or larger and if there are interrupt trigger addresses that do not belong to the redundant I/O.	Called in OB 72: 360 µs Called in OB 82, 83, 85: 430 µs (basic load) + 6 µs / configured module pairs Under extreme conditions the runtime of FB RED_DIAG is increased up to 1.5 ms. . This is the case when the working DB is 60 KB or larger and if there are interrupt trigger addresses that do not belong to the redundant I/O.
FB 453 RED_STATUS	160 µs 4 µs/ configured module pairs * number of module pairs) The runtime depends on the random position of the module being searched for in the working DB. When a module address is not redundant, the entire working DB is searched. This results in the longest runtime of FB RED_STATUS. The number of module pairs is based either on all inputs (DI/AI) or all outputs (DO/AO).	350 µs + 5 µs / configured module pairs * number of module pairs) The runtime depends on the random position of the module being searched for in the working DB. When a module address is not redundant, the entire working DB is searched. This results in the longest runtime of FB RED_STATUS. The number of module pairs is based either on all inputs (DI/AI) or all outputs (DO/AO).

Note

These are guide values, not absolute values. The actual value may deviate from these specifications in some cases. This overview is intended as a guide and should help you estimate how use of the Redundant IO CGP V52 library may change the cycle time.

Characteristic values of redundant automation systems

A

This appendix provides a brief introduction to the characteristic values of redundant automation systems, and shows the practical effects of redundant configurations, based on a selection of configurations.

You will find an overview of the MTBF of various SIMATIC products in the SIMATIC FAQs in the following entry: Mean Time Between Failures (MTBF) list for SIMATIC Products (http://support.automation.siemens.com/WW/view/en/16818490)

A.1 Basic concepts

The quantitative assessment of redundant automation systems is usually based on their reliability and availability parameters. These are described in detail below.

Reliability

Reliability refers to the capability of technical equipment to fulfill its function during its operating period. This is usually no longer the case if any of its components fails.

So a commonly used measure for reliability is the **MTBF** (**M**ean **T**ime **B**etween **F**ailure). This can be analyzed statistically based on the parameters of running systems, or by calculating the failure rates of the components used.

Reliability of modules

The reliability of SIMATIC components is extremely high as a consequence of extensive quality assurance measures in design and production.

Reliability of automation systems

The use of redundant modules considerably prolongs the MTBF of a system. Combined with the high-quality self-tests and the error detection mechanisms integrated in CPU 410SIS, almost all errors are detected and located.

The MTBF of the AS 410H SIS is determined by the **MDT** (**M**ean **D**own **T**ime) of a subsystem. This time is derived in essence from the error detection time plus the time required to repair or replace defective modules.

In addition to other measures, a CPU provides a self-test function with an adjustable test cycle time. The default test cycle time is 90 minutes. This time has an influence on the error detection time. The repair time for a modular system such as the AS 410H SIS is usually 4 hours.

Mean Down Time (MDT)

The MDT of a system is determined by the times outlined below:

- Time required to detect an error
- Time required to find the cause of an error
- Time required for troubleshooting and to restart the system

The system MDT is calculated based on the MDT of the individual system components. The structure in which the components make up the system also forms part of the calculation.

Correlation between MDT and MTBF: MDT << MTBF

The MDT value is of the highest significance for the quality of system maintenance. The most important factors are:

- Qualified personnel
- Efficient logistics
- High-performance tools for diagnostics and error recognition
- A sound repair strategy

The figure below shows the dependency of the MDT on the times and factors mentioned above.

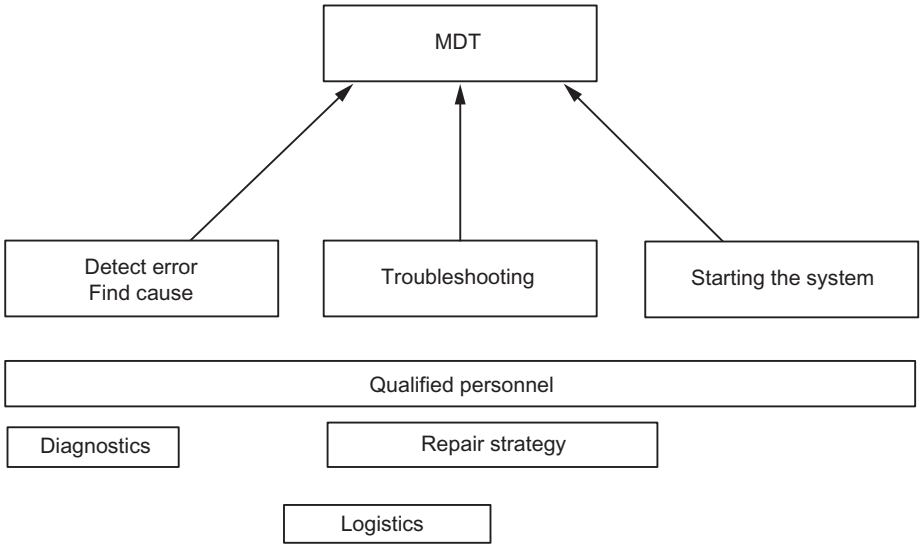


Figure A-1 MDT

The figure below shows the parameters included in the calculation of the MTBF of a system.

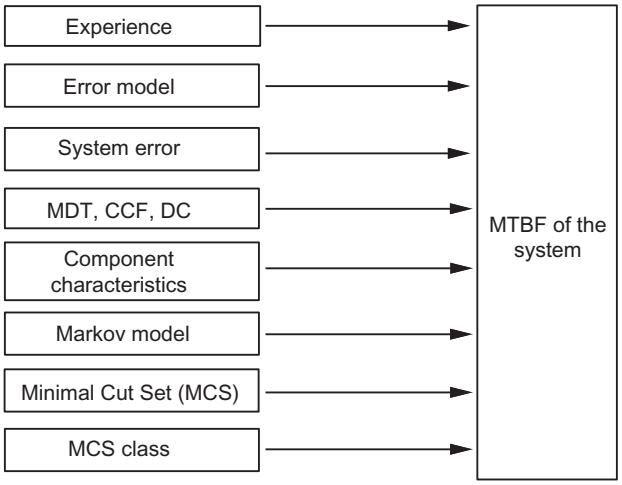


Figure A-2 MTBF

Requirements

This analysis assumes the following conditions:

- The failure rate of all components and all calculations is based on an average temperature of 40 °C.
- The system installation and configuration is free of errors.
- All replacement parts are available locally, in order to prevent extended repair times due to missing spare parts. This keeps the component MDT down to a minimum.
- The MDT of individual components is 4 h. The system's MDT is calculated based on the MDT of the individual components plus the system structure.
- The MTBF of the components meets the following standards:
  - SN 29500
    This standard is compliant with MIL–HDBK 217–F.
  - IEC 60050
  - IEC 61709
- The calculations are made using the diagnostic coverage of each component.
- A CCF factor between 0.2% and 2% is assumed, depending on the system configuration.

Common Cause Failure (CCF)

The Common Cause Failure (CCF) is an error which is caused by one or more events which also lead to an error state on two or more separate channels or components in a system. A CCF leads to a system failure.

The CCF may be caused by one of the following factors:

- Temperature
- Humidity

- Corrosion
- Vibration and shock
- Electromagnetic interference
- Electrostatic discharge
- RF interference
- Unexpected sequence of events
- Operating errors

The CCF factor defines the ratio between the probability of the occurrence of a CCF and the probability of the occurrence of any other error.

Typical CCF factors range from 2% to 0.2% in a system with identical components, and between 1% and 0.1% in a system containing different components.

Within the range stipulated in IEC 61508, a CCF factor between 0.02% and 5% is used to calculate the MTBF.

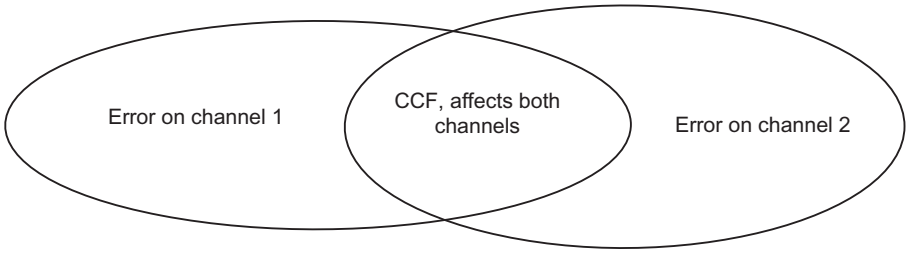


Figure A-3 Common Cause Failure (CCF)

Reliability of an AS 410H SIS

The use of redundant modules prolongs the system MTBF by a large factor. Due to the high-quality self-test and the testing and information functions integrated in the CPU 410SIS, almost all errors are detected and localized. The calculated diagnostic coverage is around 90%.

The reliability in stand-alone mode is described by the corresponding failure rate. The failure rate for all S7 components is calculated according to the SN29500 standard.

The reliability in redundant mode is described by the failure rate of the components involved. This is termed "MTBF" below. Those combinations of failed components which cause a system failure are described and calculated using Markov models. Calculations of the system MTBF take account of the diagnostic coverage and the common cause factor.

Availability

Availability is the probability that a system is operable at a given point of time. This can be enhanced by means of redundancy, for example by using redundant I/O modules or multiple encoders at the same sampling point. Redundant components are arranged such that system operability is not affected by the failure of a single component. Here, again, an important element of availability is a detailed diagnostics display.

The availability of a system is expressed as a percentage. It is defined by the mean time between failure (MTBF) and the mean time to repair MTTR (MDT). The availability of a two-channel (1-out-of-2) fault-tolerant system can be calculated using the following formula:

$$V = \frac{MTBF_{1v2}}{MTBF_{1v2} + MDT} 100\%$$

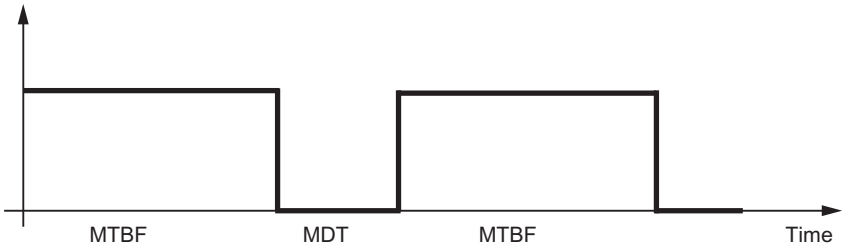


Figure A-4 Availability

A.2 Comparison of MTBF for selected configurations

The following sections compare systems with distributed I/O.

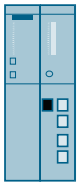
The following framework conditions are set for the calculation.

- MDT (Mean Down Time) 4 hours
- Ambient temperature 40 degrees
- Buffer voltage is safeguarded

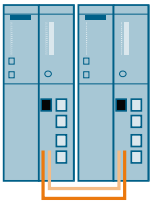
A.2.1 System configurations with redundant CPU 410

The following system with a CPU 410SIS in stand-alone mode serves as a basis for calculating a comparison factor to indicate the multiple of the system MTBF of the other systems with a central I/O compared to the base.

CPU 410SIS in stand-alone mode

CPU 410SIS in stand-alone mode	Factor
	1

Redundant CPUs in different racks

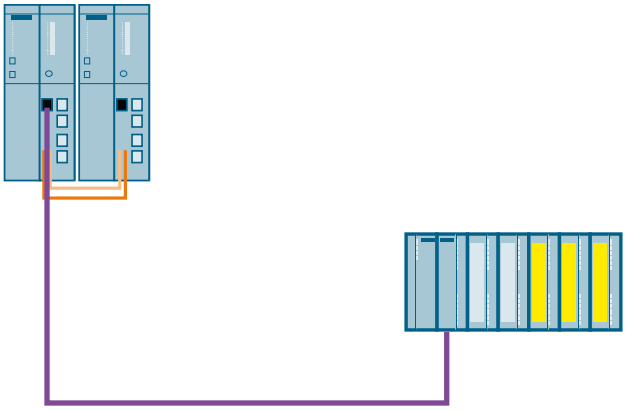
Redundant CPU 410SIS in shared rack, CCF = 2%	Factor
	approx. 20

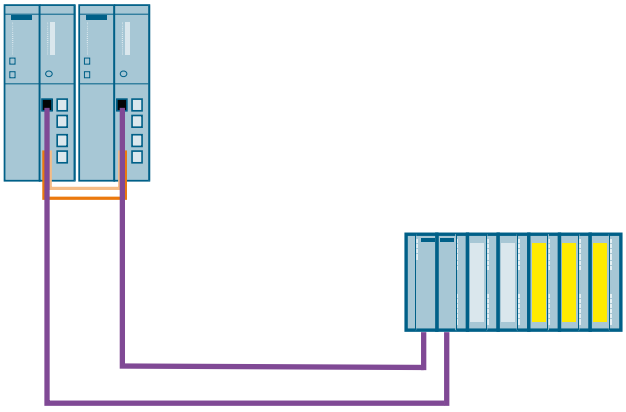
Redundant CPU 410SIS in two spatially separated racks, CCF = 1%	Factor
	approx. 38

A.2.2 System configurations with distributed I/Os

The following system with two CPUs 410SIS and one-sided I/O serves as the basis for calculating a comparison factor, which is the multiple of the availability of the other systems with distributed I/O compared to the base.

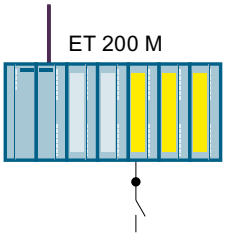
Redundant CPUs with single-channel one-sided or switched I/O

One-sided distributed I/O	Base line
	1

Switched distributed I/O, PROFIBUS DP, CCF = 2 %	Factor
	approx. 15

Redundant CPUs with redundant I/O

The comparison only took account of the I/O modules.

Single-channel one-sided I/O	MTBF factor
	1

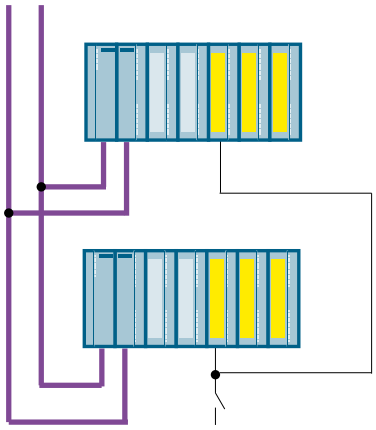
Redundant I/O	MTBF factor
	See following table

Table A-1 MTBF factors of the redundant I/O

Module	MLFB	MTBF factor CCF = 1%
Digital input modules, distributed		
DI 24xDC24V	6ES7 326–1BK02–0AB0	approx. 5
DI 8xNAMUR [EEx ib]	6ES7 326-1RF00-0AB0	approx. 5
DI16xDC24V, Alarm	6ES7 321–7BH01–0AB0	approx. 4
Analog input modules, distributed		
AI6x0/4...20mA HART	6ES7 336-7GE00-0AB0	approx. 5
AI8x12Bit	6ES7 331-7KF02-0AB0	approx. 5
Digital output modules, distributed		
DO 10xDC 24 V/2 A	6ES7 326-2BF10-0AB0	approx. 5
DO8xDC24V/2A	6ES7 322-1BF01-0AA0	approx. 3
DO32xDC24V/0.5A	6ES7 322–1BL00–0AA0	approx. 3

Summary

Several thousand redundant automation systems are in use in different configurations in manufacturing and process automation. To calculate the MTBF, we assumed an average configuration.

Based on experience in the field, an assumption of MTBF of 3000 years is 95% reliable.

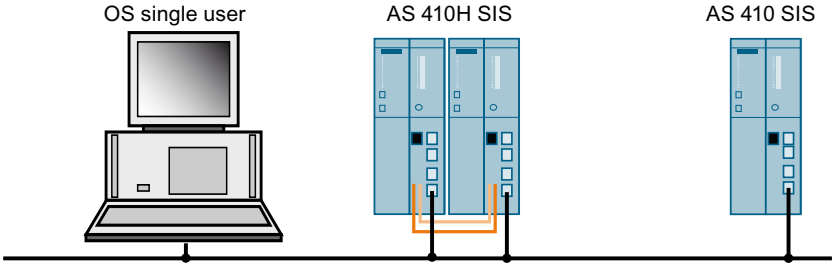
The calculated system MTBF value for a system configuration with redundant CPU 410SIS is approx. 230 years.

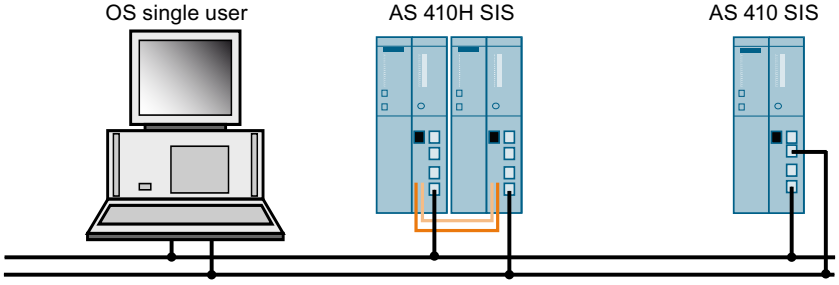
A.2.3 Comparison of system configurations with standard and fault-tolerant communication

The following section shows the comparison between standard and high-availability communication for a configuration with an AS 410H SIS, an AS 410 SIS in stand-alone mode, and a single-channel OS.

Only the PROFINET interfaces and cables were included in the comparison.

Systems with standard and fault-tolerant communication

Standard communication	Base line
	1

Fault-tolerant communication	Factor
	Approx. 80

Index

A

Analog output signals, 67
Applied value, 63
AS 410SIS
  Update block type in RUN, 111
Availability
  Definition, 252
  of systems, 47

B

Basic knowledge
  required, 9
Basic system, 16, 17
Behavior of the CPU, 139, 140, 145
  after download of the configuration in RUN, 145
  during re-configuration, 140
  Effects on the operating system functions, 145
Block type
  update for AS 410SIS, 111
Bus connectors, 33
  PROFIBUS DP interface, 33
BUS1F, 30
BUS5F, 30
BUS8F, 30
BUSF, 37

C

CC, 16
Central controller (CC), 16
Central processing unit, 17
Central system clock, 121
Checksum errors, 85
CiR, 123, 124, 125
CiR Element, 125
CiR elements, 126, 127
  I/O address areas, 127
  Types, 126
CiR module, 126, 127
CiR object, 126, 127
CiR synchronization time, 145
Cold restart, 73
Communication
  CPU services, 202
Communication functions, 229
Communication services
  Overview, 202
Communication via MPI and communication bus
  Cycle load, 235
Comparison error, 85
Components
  Basic system, 16, 17
  Duplicating, 47
Configuration, 15
Connection
  Fault-tolerant S7, 212
  S7, 211
Continued bumpless operation, 77
CPU
  Resetting to the factory settings, 112
CPU 410SIS
  Configuration and programming, 21
  DP master:diagnostics with LEDs, 37
  I/O, 20
  Operator controls and display elements, 23
  Parameter, 35
CPU redundancy errors, 232
Cycle control
  Execution time, 236
Cycle load
  Communication via MPI and communication bus, 235
Cycle time, 232
  Elements, 234
  Extending, 234
Cyclic self-test, 86

D

Defining CiR elements, 128, 129
  Exact procedure, 129
  Overview, 128
Deleting CiR elements, 129, 132
  Exact procedure, 132
  Overview, 128
Diagnostic addresses, 38
Diagnostic addresses for PROFIBUS, 38
Diagnostics buffer, 32
Digital output
  Fault-tolerant, 63, 67
Direct current measurement, 66
Direct I/O access, 243
Discrepancy
  Digital input modules, 60

Discrepancy time, 60, 63
DP interface, 33
DP master
  Diagnostics using LEDs, 37
DP master system
  Startup, 37

E

Encoders
  Double redundant, 62
Error LEDs, 30
  CPU 410, 31
Error messages, 27
Ethernet, 33
Execution time
  Cycle control, 236
  Operating system, 236
  Process image update, 235
  User program, 235
EXTF, 30

F

Factory settings, 112
Fail-safe, 45
Failure of a redundancy node, 48
Failure of components
  of distributed I/Os, 170
Fault-tolerant, 45
Fault-tolerant communication, 211
Fault-tolerant connections
  Configuration, 217
  Programming, 214, 217
FB 450 RED_IN, 54
FB 451 RED_OUT, 54
FB 452 RED_DIAG, 54
FB 453 RED_STATUS, 54
FC 450 RED_INIT, 54
FC 451 RED_DEPA, 54
Fiber-optic cable, 18
  Cable pull-in, 180
  Installation, 178
  Replacement, 169
  Selection, 181
  Storage, 179
Functional I/O redundancy, 54

G

Gateway, 205

H

Hardware
  Components, 16, 17
Hardware interrupt processing, 246
Hardware interrupt response time
  of signal modules, 246
  of the CPU, 245
Hardware requirements, 123
HOLD, 73
Hotline, 11

I

I/O, 20
  Switched, 46, 49
I/O redundancy errors, 232
IFM1F, 31
IFM2F, 31
Indirect current measurement, 65
Initial configuration, 125
Interface
  PROFINET, 25
INTF, 30
IP address
  Assigning, 33

L

LED
  BUSF, 37
LED displays, 23
LINK, 31
LINK1 OK, 32
LINK2 OK, 32
Link-up, 89, 90, 93, 223, 226, 231
  Flow chart, 224
  Sequence, 226
  Time response, 93
Link-up and update
  Disabling, 231
  Effects, 89
  Sequence, 223
  Starting, 223
Link-up with master/standby changeover, 227
Link-up, update, 71
Load memory, 230
Loss of redundancy, 77

M

MAINT, 32
Manual
  Purpose, 9
  Scope of validity, 9
Master CPU, 76
Master-standby assignment, 76
Maximum communication delay
  Calculation, 98
  Definition, 91
Maximum cycle time extension
  Calculation, 98
  Definition, 91
Maximum inhibit time for priority classes > 15
  Calculation, 95
  Definition, 91
MDT, 249
Memory reset, 72
  Sequence, 87
Message functions, 229
Minimum I/O retention time
  Calculation, 95
  Definition, 91
Monitoring functions, 27
Monitoring times, 91
  Accuracy, 94
  Configuration, 94
MSTR, 30
MTBF, 249, 253
Multiple-bit errors, 86

N

Network configuration, 201
Networking configuration, 201
Non-redundant encoders, 61, 64

O

OB 121, 84
Online help, 9
Operating mode
  Changing, 40
Operating objectives, 45
Operating states
  LINK-UP, 74
  STARTUP, 72
  System, 79
  UPDATE, 74
Operating system
  Execution time, 236
Organization blocks, 232

P

Parameter, 35
Parameter assignment tool, 35
Parameter block, 35
PG functions, 202
Plant changes with CiR, 132
  Overview, 132
Power supply, 16, 17
Precision
  Time stamping, 121
Process image update
  Execution time, 235
PROFIBUS address, 37
PROFIBUS DP interface, 25
PROFINET interface, 25
PROFINET interfaces
  Properties, 34
Protection level, 104
  Setting, 104

R

Rack, 17
RACK0, 30
RACK1, 30
RAM/PIQ comparison error, 85
Recommendations, 125
Reconfiguring, 139
  Requirements, 139
Re-configuring, 139, 141, 142
  a previously used channel, 141
  Behavior of the CPU, 139
  Removing a channel previously used, 142
  using a previously unused channel, 141
Re-configuring a previously used channel, 141
REDF, 31
Redundancy
  Active, 76
Redundancy nodes, 47, 211
Redundant analog output modules, 67
Redundant automation systems, 45
Redundant communication system, 211
Redundant encoders, 62
  Analog input modules, 67
Redundant I/O, 45
  Analog input modules, 63

Configuration, 56
Digital input modules, 60
Digital output modules, 63
in the switched DP slave, 53
Redundant system mode, 71
Reliability, 249
Removing a channel previously used, 142
Replacement during operation
of distributed I/Os, 170
Requirements, 124
Response time
Calculation of the, 241, 242
Elements, 239
Longest, 242
Reducing, 243
Shortest, 241
Response to time-outs, 92
Routing, 204
Rules for assembly, 19, 199
RUN, 29
RX/TX, 31

S

S7 connections
configured, 218
of CPU 410SIS, 203
S7 routing
Access to stations on other subnets, 204
Application example, 206
Gateway, 205
Requirements, 205
S7-400H
Blocks, 232
User program, 232
S7-REDCONNECT, 215, 216
Save service data, 115
Scope of validity
of the manual, 9
Self-test, 77, 84
SFC 109 PROTECT, 105
Signal modules for redundancy, 56
SIMATIC Manager, 202
Simple Network Management Protocol, 210
Single mode, 71
Single-bit errors, 86
Single-channel switched I/O, 46, 49
Failure, 51
Slot for synchronization modules, 24
SNMP, 210
Software requirements, 124
Stand-alone operation
Configuring, 40
Definition, 39
Points to note, 39
to a fault-tolerant system, 40
Standby CPU, 76
Startup, 73
Startup
DP master system, 37
Startup processing, 73
Startup time monitoring, 37
Startup types, 72
Status byte, 69
Status displays
CPU 410SIS, 29
Status word, 69
STOP, 29
Subconnection
Active, 213
Switch to CPU with modified configuration, 230
Synchronization, 77
Event-driven, 77
Synchronization module
Function, 175
Replacement, 169
Technical specifications, 178
Synchronization modules, 17
System design, 144
ET200iSP Stations, 144
ET200M Stations, 144
System planning, 143
DP or PA slaves, 143
System states, 79

T

Technical Support, 11
Time information
Synchronized, 121
Time monitoring, 90
Time response, 100
Time stamp, 121
Time stamping
Functionality, 121
Precision, 121
Requirements, 121
Resolution, 121
Using, 121
Time synchronization, 121
Time-of-day stamping (1 ms), 121
Time-out, 92
Tolerance window, 63

Tools, 21

U

Undo function, 137
Undoing changes, 137
Update, 89, 90, 93, 223, 231
    Block types in the multiproject with the AS 410
    SIS, 111
    Minimum input signal duration, 226
    Sequence, 227
    Time response, 93
User program, 232
User program execution time, 235
Using
    Time stamping, 121
Using a previously unused channel, 141
Using CiR elements in RUN, 136

W

Warm restart, 73, (Warm restart)
Work memory, 230