SIEMENS

SIMATIC NET

S7-300 - Industrial Ethernet / PROFINET CP 343-1 Advanced

Equipment Manual

Preface

Properties and services 1

Performance data 2

Requirements for use 3

LEDs 4

Installation and commissioning 5

Using the CP for PROFINET CBA 6

Configuration and operation 7

Diagnostics and upkeep 8

Technical specifications 9

Approvals A

References B

Manual Part B

06/2021

C79000–G8976–C202-07

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

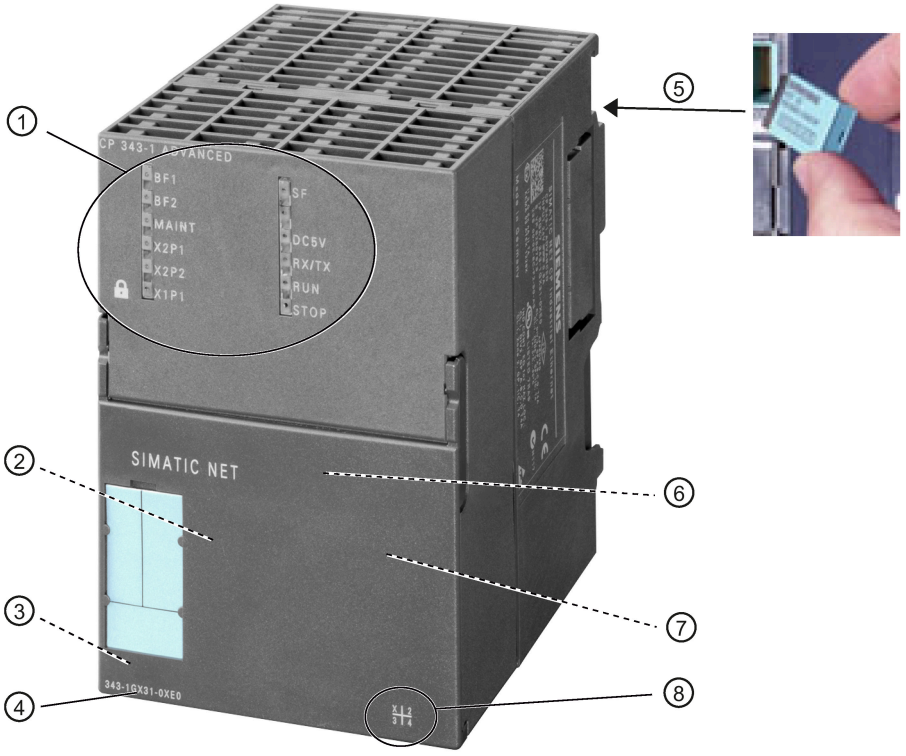
We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000–G8976–C202-07
Ⓟ 06/2021 Subject to change

Copyright © Siemens AG 2008 - 2021.
All rights reserved

Preface



Legend:

① LEDs

② Under the front panel:
PROFINET interface, 2 x 8-pin RJ-45 jack

Security function: Interface to the internal, protected subnet

③ Under the front panel:
- Socket for 24 V DC power supply
- Slider for setting the ground connector

④ Article number

⑤ CPLUG (at rear)

⑥ Under the front panel:
Printed text with MAC addresses of the interfaces and the firmware version

⑦ Under the front panel:
Gigabit interface, 1 x 8-pin RJ-45 jack

Security function: The padlock symbol identifies the interface to the external, non-secure subnet.

⑧ X = placeholder for hardware product version

Figure 1 CP 343-1 Advanced

Validity

This description contains information on the following product

- CP 343–1 Advanced
  Article number 6GK7343-1GX31-0XE0
  Hardware product version 1
  Firmware version V3.0
  Communications processor for SIMATIC S7–300 / C7–300 und SINUMERIK 840D power line
- CP 343–1 Advanced
  Article number 6AG1343-1GX31-4XE0
  Hardware product version 1
  Firmware version V3.0
  Communications processor for SIMATIC S7–300 / C7–300 und SINUMERIK 840D power line - conformal coating

New in this edition

Restrictions of the security functions, see security note on firmware below.

Replaced documentation

This manual replaces the manual edition 12/2018.

Notes on this document

Product names

- CP

  In this document, the term "CP" is also used instead of the full product name "CP 343-1 Advanced".

  The module names "CP 343-1 Advanced (GX30)" and "CP 343-1 Advanced (GX31)" identify the precise version of the module. Short name in brackets corresponds to the last four characters of the middle section of the order number of the CP:

  – CP 343-1 Advanced (GX30): Order number 6GK7 343–1GX30–0XE0

  – CP 343-1 Advanced (GX31): Order number 6GK7 343–1GX31–0XE0

- STEP 7

  The name STEP 7 is used for the configuration tool instead of the names STEP 7 V5.5 and STEP 7 Professional, if the respective function is supported by both configuration tools.

Cross-references

In this manual, there are often cross-references to other sections. To be able to return to the initial page after jumping to a cross-reference, some PDF readers support the command <Alt>+<left arrow>.

Search

To show all places where a term was found in a list, some PDF readers support the command <Ctrl>+<Shift>+<F>.

Compatibility with previous versions

Note

Make sure that you read the information relating to restrictions in the section Module replacement / upgrading (Page 96).

Structure of the documentation

The documentation for this device consists of the following parts

- Manual Part B: Manual "CP 343-1 Advanced" (this manual)
- Manual Part A: Configuration manual "S7-CPs for Industrial Ethernet Configuring and Commissioning"

  Relevant for configuration with STEP 7 V5.5

  Refer to /2/ (Page 108).(References).
- SIMATIC NET Industrial Ethernet Security - Basics and Application, configuration manual

  Relevant for configuration with STEP 7 V5.5

  Refer to /6/ (Page 108).
- Program blocks for SIMATIC NET S7 CPs - programming manual

  Relevant for configuration with STEP 7 V5.5

  Refer to /16/ (Page 110).

  Contains the detailed description of the program blocks for the following services:

  – Open communication services
  – Access coordination with FETCH/WRITE
  – Connection and system diagnostics
  – FTP services
  – Programmed connections and IP configuration
  – PROFINET
- Programming tips for S7Beans / Applets for IT-CPs, see /5/ (Page 108)

You can find a description of the configuration with STEP 7 Professional in the TIA Portal in the help (STEP 7 information system).

Current version of the manual and information on the Internet

You will find the current version of this document and further information (e.g. FAQs) on using the CP on the Internet at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15346)

CP documentation on DVD

You can find the documentation on the product and the configuration on the "SIMATIC NET Manual Collection" or "SIMATIC Communication Products" DVD. This DVD contains the product manuals valid at the time it is created.

Address label: Unique MAC address preset for the CP

The CP is supplied with total of 4 default MAC addresses with the following assignment:

- Gigabit interface
- PROFINET interface
- One MAC address for each of the 2 Ethernet ports of the PROFINET interface

  The MAC addresses of the Ethernet ports are required only for detection and evaluation of neighborhood and topology relations.

The two MAC addresses of the PROFINET interface and the gigabit interface are printed on the housing.

If you configure a MAC address (ISO transport connections), we recommend that you use the MAC addresses printed on the module for module configuration!

- This ensures that you assign a unique MAC address in the subnet!
- If you replace a module, the MAC address of the predecessor is adopted when you load the configuration data. Configured ISO transport connections remain operable.

You should also refer to the information in the section Replacing a module (Page 95).

License conditions

Note

Open source software

The product contains open source software. Read the license conditions for open source software carefully before using the product.

You will find license conditions in the following document on the supplied data medium:

- OSS_CP3431-Adv_86.pdf

Firmware

The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

Note

Critical restrictions on security for CP 343-1 Advanced (6GK7343-1GX31-0XE0 / 6AG1343-1GX31-4XE0)

Parts of the CP firmware come from third-party providers who have discontinued maintenance for the supplied software components. For this reason, these components are no longer monitored for newly detected critical vulnerabilities.

For CPs purchased from June 2021, this means:

- Siemens can no longer ensure that the firmware does not contain security-critical vulnerabilities.
- Siemens no longer publishes newly discovered security vulnerabilities as Security Advisories and no longer corrects vulnerabilities of this time.

This does not impair the functionality of the CP. It merely means that it is no longer guaranteed that the networks secured by the CP are protected without restrictions.

Siemens recommends the following measures:

- Implement a state-of-the-art security concept for the entire plant. You can find information on this at this address:
  Link: (https://www.siemens.com/industrialsecurity)
- Secure the Internet access realized via the CP additionally using security components such as a SCALANCE S. In this case, the plant would be adequately protected even if there was a security-critical vulnerability in the CP.

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit
Link: (http://www.siemens.com/industrialsecurity)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Link: (http://www.siemens.com/industrialsecurity)

Decommissioning

Shut down the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, restore the factory settings on the device.

Recycling and disposal



The product is low in pollutants, can be recycled and meets the requirements of the WEEE directive 2012/19/EU "Waste Electrical and Electronic Equipment".

Do not dispose of the product at public disposal sites. For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact.

Keep to the local regulations.

You will find information on returning the product on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/view/109479891)

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary on the Internet at the following address:

50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

Training, Service & Support

You will find information on Training, Service & Support in the multilanguage document "DC_support_99.pdf" on the "SIMATIC NET Manual Collection" DVD that ships with the products.

Table of contents

Preface ... **3**

1 Properties and services ... **13**

1.1 Application ... 13

1.2 Enhanced functions ... 14

1.3 Communication services ... 16

1.4 Other services ... 18

1.5 The CP as Web server ... 21

2 Performance data ... **23**

2.1 Transmission and reaction times ... 23

2.2 Number of possible connections via Ethernet ... 23

2.3 Characteristics of S7 communication ... 24

2.4 Characteristic data of the SEND/RECEIVE interface ... 25

2.5 Modes and characteristic data for PROFINET IO ... 26

2.6 Characteristic data for PROFINET CBA ... 28

2.7 Characteristics of e-mail mode ... 31

2.8 Characteristic data for FTP / FTPS mode ... 32

2.9 Characteristic data for HTTP / HTTPS ... 33

2.10 Characteristic data for the use of Java applets ... 33

2.11 Characteristic data of the C-PLUG ... 34

2.12 Characteristic data of the integrated switch ... 34

2.13 Memory organization ... 35

3 Requirements for use ... **37**

3.1 Operation in control device families ... 37

3.2 Configuration ... 40

3.3 Program blocks ... 41

4 LEDs ... **43**

5 Installation and commissioning ... **47**

5.1 Important notes on using the device ... 47

5.1.1 Notices on use in hazardous areas ... 47

5.1.2 Notes on use in hazardous areas according to ATEX / IECEx / UKEX ... 49

5.1.3 Notes on use in hazardous areas according to UL HazLoc / FM ... 49

5.2 Installing the CP, connecting power and ground ... 50

5.3 Connecting the CP to Ethernet ... 52
5.4 Commissioning the CP ... 53
5.5 CPLUG (configuration plug) ... 54
6 Using the CP for PROFINET CBA ... 59
6.1 CBA interface in the user program with FB88 ... 59
6.2 Preparing for configuration with STEP 7 ... 60
6.3 PROFINET CBA configuration with SIMATIC iMap ... 60
6.4 Using PROFINET CBA communication and standard communication at the same time ... 64
7 Configuration and operation ... 67
7.1 Security recommendations ... 67
7.2 Controlling the mode ... 70
7.3 Effects of protection levels ... 72
7.4 Configuration in STEP 7 ... 73
7.5 Network settings ... 73
7.5.1 IP address assignment and communications path ... 73
7.5.2 Fast Ethernet with the PROFINET and gigabit interface ... 74
7.5.3 Transmission speed of the gigabit interface ... 75
7.5.4 Using the CP as an IP router ... 76
7.6 IP configuration ... 76
7.6.1 Detection of double IP addressing in the network ... 76
7.6.2 Configured S7 connections cannot be operated if the IP address is assigned over DHCP ... 77
7.6.3 Address assignment with DHCP: Expiry of the lease ... 78
7.6.4 Address assignment via DHCP- gigabit interface ... 78
7.7 PROFINET IO ... 78
7.7.1 IP access protection using the IP access control list with a PROFINET IO device ... 78
7.7.2 How PROFINET IO devices start up in a large configuration ... 79
7.7.3 PROFINET IO when operating other services at the same time ... 79
7.7.4 Effects of multicast communication on RT communication ... 79
7.7.5 Media redundancy ... 80
7.7.6 IRT communication: Types of synchronization ... 80
7.8 Security ... 80
7.8.1 Attachment to Industrial Ethernet networks ... 80
7.8.2 Using VPN - effects on communication ... 81
7.8.3 Reloading firewall rules ... 81
7.8.4 Activating IP access protection ... 81
7.8.5 Importing certificates for SMTP with STARTTLS or FTPS ... 81
7.8.6 Security and STEP 7 special diagnostics activated - configuration activities blocked ... 82
7.9 Timeofday synchronization ... 82
7.10 SNMP agent ... 83
7.11 Programmed communication connections ... 85
7.11.1 Behavior with programmed communications connections ... 85
7.11.2 IP access protection with programmed communication connections ... 86
7.11.3 Programmed communications connections - assigning parameters to the ports ... 86

7.12 Influence of MPI on connections via Industrial Ethernet ... 86
7.13 Ping ... 87
7.14 Downtime if an S7 connection aborts ... 87
8 Diagnostics and upkeep ... 89
8.1 Online security diagnostics via port 8448 ... 89
8.2 Memory reset / reset to factory defaults ... 89
8.3 Loading new firmware ... 93
8.4 Replacing a module ... 95
8.4.1 Replacing older modules ... 95
8.4.2 Module replacement / upgrading ... 96
8.4.3 Replacing a module without a programming device ... 97
9 Technical specifications ... 99
A Approvals ... 101
B References ... 107
B.1 On configuring, commissioning and using the CP ... 107
B.2 For configuration and programming with STEP 7 / NCM S7 ... 108
B.3 On program blocks ... 110
B.4 On installing and commissioning the CP ... 111
B.5 For application and configuration of PROFINET IO ... 111
B.6 On setting up and operating an Industrial Ethernet network ... 112
B.7 On configuration of PROFINET CBA (components and systems) ... 112
Index ... 113

Properties and services

1

1.1 Application

Application

The CP 343-1 Advanced communications processor is intended for operation in a SIMATIC S7-300 or C7-300 automation system or SINUMERIK 840D power line. It allows the connection of the S7-300 to Industrial Ethernet and supports PROFINET.

Security Integrated

With a combination of different security measures such as firewall, NAT/NAPT routers and VPN (Virtual Private Network) over IPsec tunnels, the CP protects individual S7-300 stations or even entire automation cells from unauthorized access.

Note

Critical restrictions on security for CP 343-1 Advanced (6GK7343-1GX31-0XE0 / 6AG1343-1GX31-4XE0)

Parts of the CP firmware come from third-party providers who have discontinued maintenance for the supplied software components. For this reason, these components are no longer monitored for newly detected critical vulnerabilities.

For CPs purchased from June 2021, this means:

- Siemens can no longer ensure that the firmware does not contain security-critical vulnerabilities.
- Siemens no longer publishes newly discovered security vulnerabilities as Security Advisories and no longer corrects vulnerabilities of this time.

This does not impair the functionality of the CP. It merely means that it is no longer guaranteed that the networks secured by the CP are protected without restrictions.

Siemens recommends the following measures:

- Implement a state-of-the-art security concept for the entire plant. You can find information on this at this address:
  Link: (https://www.siemens.com/industrialsecurity)
- Secure the Internet access realized via the CP additionally using security components such as a SCALANCE S. In this case, the plant would be adequately protected even if there was a security-critical vulnerability in the CP.

The CP has the following interfaces:

- PROFINET interface (Ethernet interface)

  A 2-port switch with IRT capability and with autocrossing, autonegotiation and autosensing is integrated in the CP. The 2-port switch allows the integration of the CP in a bus or a ring with media redundancy.

  Each port can be disabled individually in the configuration.

  Note

  The following services or characteristics are only available on the PROFINET interface:
  - PROFINET
  - Programmed communications connections (program block IP_CONFIG).

- Gigabit interface

  The CP also has an Ethernet interface complying with the gigabit standard IEEE 802.3ab. This is independent of the PROFINET interface and supports autocrossing, autonegotiation and autosensing. The gigabit interface can, for example, be used to connect to a PG/PC or to a higherlevel company network.

  The port can be disabled in the configuration.

  The gigabit interface allows a secure connection to external networks via a firewall and VPN. The CP supports the protective functions:

  – Protection of the S7 station in which the CP is operated

  – Protection of the internal networks connected to the PROFINET interface.

1.2 Enhanced functions

Enhanced functions of the CP 343-1 Advanced (GX31) with firmware version V3.0 compared with the CP 343-1 Advanced (GX30) with firmware version V1.3.1

To use the new characteristics listed below, the STEP 7 configuration tool is required, see section Configuration (Page 40).

- Security functionality

  Functions: Firewall, NAT/NAPT router, VPN (Virtual Private Network) via IPsec tunnel, HTTPS, FTPS, NTP (secure), SNMPv3

- PROFINET IO

  – IRTtop (IRT option "High performance") as IO device

  – Configuring the CP as an IO device in the STEP 7 "I-device" dialog box (and as previously using a GSDML file)

  – The shared device function of the CP as an IO device in PROFINET IO can only be configured with STEP 7 V5.5.

- Use of PROFIenergy functionality

  This requires the following PROFIenergy program blocks for the CP 343-1 in the "SIMATIC_NET_CP" library with the STEP 7 version listed above:

  – PE_START_END_CP, PE_CMD_CP, PE_I_DEV_CP and the program block DS3_WRITE_CP to allow use of power modules of the ET 200S for PROFIenergy.

  – The supplementary program blocks FC0 to FC8 for the PROFIenergy response data can be found in the Standard Library.

  You will find the documentation of the program blocks in the online help and in the manual for the program blocks, see References, /16/ (Page 110).
- Expanded program block FTP_CMD for FTP services allows the establishment of secure SSL connections.
- New program block FB10 AG_CNTEX for connection diagnostics

Functional enhancements of the GX31 with firmware version V3.0 - regardless of the configuration tool used

- Full PROFINET IO diagnostics on the gigabit interface
- Advanced Web diagnostics (HTTP access) with the following additional options:
  – Update center with the following functions:

    Downloading firmware via Web

    Updating the IP access control list

    Downloading of language files for diagnostics buffer texts in STEP 7 format for new modules in the rack and for changing the language

  – Topology representation

  – Diagnostics of S7 connections

  – Status of the configured security functions

  – Module identification

  – Expansion of Web diagnostics for shared device
- SNMP: Support of the MRP Monitoring MIB
- Support of the C-PLUG 256 with free use of the 128 MB flash file system

Enhanced functions of earlier firmware versions and predecessor modules

You will find an overview of the earlier firmware versions and predecessor modules in the version history of the Industrial Ethernet CPs; see /3/ (Page 108).

You will find information about the characteristics of the individual firmware versions at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15346/dl)

1.3 Communication services

The CP supports the communication services listed below.

In each case, note the configuration tool required, see section Enhanced functions (Page 14) and Configuration (Page 40).

- **PROFINET IO**

  PROFINET IO can only be used via the ports of the PROFINET interface.

  PROFINET IO allows direct access to IO devices over Industrial Ethernet.

  The CP can be used as a PROFINET IO controller and a PROFINET IO device at the same time.

  – PROFINET IO controller

    IO controller mode with alarm block and acyclic data exchange by reading/writing a data record.

  – PROFINET IO device

    Integration of the SIMATIC S7-300 automation system via the CP as an intelligent PROFINET IO device (I-device).

  – Shared device with the CP as device

    Individual submodules of the CP as IO device can be assigned to up to two PROFINET IO controllers.

    Note the information on configuring PROFINET IO systems with shared IO devices in the "PROFINET System Description", see references, /19/ (Page 111).

  – IRT communication (Isochronous Real Time)

    In PROFINET IO, the CP 343-1 Advanced (GX31) supports IRT communication with the IRT option "high-performance" in the "PROFINET IO device" mode. The IRT option "high-performance" optimizes data traffic as the result of topology planning.

    The "high flexibility" IRT option isd only supported now if a module is replaced and the CP 343-1 Advanced (GX31) is configured in the STEP 7 project as a CP 343-1 Advanced (GX30).

    You will find detailed information on configuration in the general Part A of the manual, see /2/ (Page 108) and in the online help of STEP 7 V5.5.

    Note

    IRT communication or MRP

    If you are using IRT communication, no media redundancy is supported.

- **PROFINET CBA**

  Use of a SIMATIC S7300 for Component based Automation on the basis of the PROFINET standard of the PNO. This standard allows:

  – Component technology in automation

  – Communication between intelligent devices is configured graphically instead of requiring laborious programming.

  – Vendorindependent, plantwide engineering

Component based Automation allows access to the variables of the PROFINET components by all standard PC applications with an OPC client interface, for example visualization systems. Via OPC servers, the objects can be selected directly from a list for the relevant selected PROFINET component.

Note

PROFINET CBA versus security function

If you use PROFINET CBA, you cannot enable the CP for the "Security" functionality.

- **S7 communication and PG/OP communication with the following functions:**

  – PG functions (including routing)

  – Operator control and monitoring functions (HMI)

    Multiplexing TD/OP connections

  – Server for data exchange on S7 connections configured at one end only without communication blocks on the S7300 / C7300 station

  – Client and server for data exchange via communication blocks on S7 connections configured at both ends

  Blocks for S7 communication:

  – BSEND FB 12

  – BRCV FB 13

  – PUT FB 14

  – GET FB 15

  – USEND FB 8

  – URCV FB 9

  – C_CNTRL FC 62

  See also STEP 7 online help or the "System Software for S7-300/400 System and Standard Functions" manual.

- **Open communication services with the following functions:**
  - SEND/RECEIVE interface over ISO transport connections, ISOonTCP, TCP and UDP connections

    UDP frame buffering on the CP can be disabled during configuration. When necessary, this allows you to achieve a shorter reaction time between the arrival of a UDP frame and its evaluation on the CPU.
  - Multicast over UDP connection

    The multicast mode is made possible by selecting a suitable IP address when configuring connections.
  - FETCH/WRITE services (server; corresponding to S5 protocol) via ISO transport connections, ISO-on-TCP connections and TCP connections;

    The addressing mode can be configured for FETCH/WRITE access as S7 or S5 addressing mode.
  - LOCK/UNLOCK with FETCH/WRITE services
  - Connection diagnostics from the user program
- **IT functions**
  - Web server: Monitoring devices and process data with HTTP/HTTPS

    If you do not require this function, you can disable it in the STEP 7 configuration and disable port 80 (properties dialog of the CP > "Web" tab).
  - FTP and secure FTPS functions (File Transfer Protocol) for file management and access to data blocks in the CPU (client and server function).

    If you do not require this function, you can disable it in the STEP 7 configuration and disable port 21 (properties dialog of the CP > "FTP" tab).
  - Sending email via ESMTP with "SMTPAuth" for authentication on an email server
  - CP as file server with flash and RAM file system

1.4 Other services

- **Security functions**

  Depending on the configuration, the security functions of the CP provide protected communication beyond network boundaries and within a network.
  - Protection concept beyond network boundaries - separation of the internal from the external network

    On its gigabit interface, the CP provides the option of secure access from an external network connected here to the internal network (PROFINET interface).

    With a combination of different security measures such as firewall, NAT/NAPT routers and VPN (Virtual Private Network) over IPsec tunnels, the CP protects individual devices or even entire automation cells from unauthorized access.

The CP allows this protection flexibly, without repercussions, protocol-independent (as of Layer 2 according to IEEE 802.3).

The secure protocols HTTPS, FTPS, NTP (secure) and SNMPv3 can also be activated.

– Communication in the internal network (PROFINET interface)

  If security is enabled, you now have the option of using the secure protocols HTTPS, FTPS, NTP (secure) and SNMPv3 within the internal network.

  Note: The switch function of the PROFINET interface integrated in the CP forwards frames in the internal subnet regardless of the security setting of the CP.

You can enable the security function in the configuration with the required options.

Note

UDP multicast

UDP multicast via a VPN connection is not supported.

- **Media redundancy (MRP)**

  Within an Ethernet network with a ring topology, the CP supports the media redundancy protocol MRP. You can assign the role of redundancy manager or client to the CP.

  If you are using IRT communication, no media redundancy is supported.

- **Time-of-day synchronization over Industrial Ethernet**

  Time-of-day synchronization can be configured in the following modes:

  – SIMATIC mode

    The CP receives MMS timeofday messages and synchronizes its local time.

    You can choose whether or not the time of day is forwarded. You can also decide on the direction in which it is forwarded.

    Synchronization using the SIMATIC mode is only possible on the PROFINET interface.

  or

  – NTP mode (NTP: Network Time Protocol)

    The CP sends timeofday queries at regular intervals to an NTP server and synchronizes its local time of day.

    The time can also be forwarded automatically to the CPU modules in the S7 station allowing the time to be synchronized in the entire S7 station.

    If security is enabled, the CP supports the NTP (secure) protocol for secure time-of-day synchronization and transfer of the time of day.

- **Addressing using a factoryset MAC address**

  To assign the IP address to a new CP (direct from the factory), it can be accessed using the preset MAC address on the interface being used. The online address assignment is made in STEP 7.

- **SNMP agent**

  The CP supports data queries over SNMP in version V1 (Simple Network Management Protocol). It delivers the content of certain MIB objects according to the MIB II standard, LLDP MIB, Automation System MIB and MRP Monitoring MIB.

  If security is enabled, the CP supports SNMPv3 for transfer of encrypted network analytical information.

- **Module access protection**

  To protect the module from accidental or unauthorized access, protection can be configured at various levels.

- **IP access protection (IPACL)**

  IP access protection provides the following options:

  – Communication via the CP of the local S7 station can be restricted to partners with specific IP addresses.

  – Access, for example, from a subnet connected to the PROFINET interface to a further subnet can be restricted. The other subnet can, for example, be connected to the gigabit interface.

- **IP configuration**

  For the PROFINET interface and the gigabit interface, you can configure how and with which method the CP is assigned the IP address and the subnet mask, and whether a router is used.

  For the PROFINET interface, the IP configuration and the connection configuration can also be assigned to the CP by the user program (program block FB55 IP_CONFIG).

  Notes:

  – Configuration of S7 connections using IP_CONFIG is not possible.

  – Connection configuration using IP_CONFIG cannot be used in conjunction with the security functions.

- **Web diagnostics**

  With the aid of Web diagnostics, you can read out the diagnostics data from a station connected via the CP to a PG/PC with a Web browser.

  This makes it possible to read out information about security functions or special information on S7 connections from the diagnostics buffers of the intelligent modules in the rack.

  Using the integrated update center of the diagnostics pages, you can download new firmware versions and diagnostics buffer message texts.

  If you do not require the functions, you can disable it in the STEP 7 configuration and disable port 80.

- **Connection diagnostics with the AG_CNTEX program block**

  With the AG_CNTEX program block, you can diagnose connections.

  – When necessary, you can activate or deactivate connections or initiate reestablishment of a connection.

  – You can check the reachability of the connection partners using the ping function.

  – You can find out which connection types are set up for the SEND / RECEIVE interface.

1.5 The CP as Web server

The CP provides you with the functionality of a web server for access by means of a web browser.

Note

Please note the following special features when using IT functions:

The data exchange for productive communication (S7 connections + SEND/RECEIVE connections) always has a higher priority than data exchange with the Web browser. This can lead to delays in the HTTP process control in the Web browser.

Beans and applets

When shipped, the file system of the CP contains S7 beans and further information.

S7 applets are Java applets specially written for SIMATIC S7 and that are used to allow write or read access to the S7CPU. You can develop your own S7 applets with the supplied S7 beans and tailor them to your requirements. For information on this, refer to the manual /5/ (Page 108).

Web diagnostics

The CP also provides HTML pages for Web diagnostics. HTML pages are used to transfer and display information in a Web browser. These, for example, contain diagnostics information.

With the following address, you have access to Web diagnostics:
`http://<IP address of the CP>/diag`

Diagnostics buffer entries

When supplied, diagnostics buffer entries shown on diagnostics pages are always in English. This is not influenced by the language selected for display of the Web pages.

How to download other languages to the CP and further information about Web diagnostics can be found in the general Part A of this manual /2/ (Page 108).

Enabling the Web server function

To use the Web server functionality of the CP, enable the relevant option in STEP 7 in the module properties, "Web" parameter group.

The Web server function is enabled as default.

Web browser

To access the HTML pages on the CP and to use the S7 applets, you require a Web browser. The following Web browsers are suitable for communication with the CP (other browsers also possible):

- Internet Explorer (recommended version: as of 7.0)
- Chrome (recommended version: as of 12.0)
- Firefox (recommended version: as of 4.0)

These Web browsers support all the requirements for implementing the IT functions of the CP.

You will find these Web browsers, information and any necessary addons on the Internet.

Performance data

2

2.1 Transmission and reaction times

Measured values on the Internet

Note

Measured values of transmission and reaction times over Ethernet, PROFIBUS and PROFINET networks for a series of configurations can be found on the Internet at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/view/25209605)

Using VPN - effects on communication

Communication via a VPN tunnel reduces speed compared with communication outside a VPN tunnel.

In mixed operation with S7 communication and connections of the open communications services (SEND/RECEIVE interface), remember that the CP handles the open communications services with higher priority.

2.2 Number of possible connections via Ethernet

Table 2- 1 Maximum number of parallel connections

Characteristic	Explanation / values
Permitted number of simultaneous connections in total over Industrial Ethernet	48 maximum

Example of maximum load

You can, for example, operate:

- 16 configured S7 connections
- 16 OP multiplex connections
- 2 ISO-on-TCP connections
- 8 TCP connections
- 6 UDP connections

Also:

- Further TCP connections for Web diagnostics and FTP server mode
- PROFINET IO
  - As PROFINET IO device:

    1 PROFINET connection to a PROFINET IO controller

    or
  - As shared device:

    2 PROFINET connections to 2 PROFINET IO controllers

    or
  - As PROFINET IO controller:

    PROFINET connections to PROFINET IO devices

2.3 Characteristics of S7 communication

Number of connections

Table 2- 2 Number of connections for S7 communication

Characteristic	Explanation / values
Number of connections for S7 communication via Industrial Ethernet	• Connections: In each case, up to – 16 operator control and monitoring functions (HMI) – 16 S7 connections configured at one end – 16 S7 connections configured at both ends The number depends on the CPU type being used; the valid values can be found in / /2/ (Page 108) /. • Resources Maximum 16 resources For each executed S7 communications function, a job resource is required. If the CPU has 16 job resources, then only 1 PUT or GET job can be executed at the same time on each of the 16 S7 connections. The same applies to BSEND/BRECV and USEND/URECV jobs.
LAN interface - data field length generated by CP per protocol data unit • sending • receiving	 • 240 bytes / PDU • 240 bytes / PDU

Data lengths of the S7 services

Table 2- 3 Possible data lengths of the S7 services

S7 service	Maximum block length per frame
PUT / GET	160 bytes
USEND / URCV	160 bytes
BSEND / BRCV	32 KB (max. length of data block)

2.4 Characteristic data of the SEND/RECEIVE interface

The SEND/RECEIVE interface provides access to communication over TCP, ISOonTCP, ISO transport, email, and UDP connections.

The following characteristics are important:

Table 2- 4 Characteristic data of the SEND/RECEIVE interface

Characteristic	Explanation / values
Number of ISO transport connections, ISO-on-TCP connections + TCP connections + UDP connections + e-mail connections in total	16 maximum Notes: • All UDP connections are also possible in multicast mode. • Free UDP connections are supported by the CP. • E-mail connection: 1
Maximum data length for the blocks AG_SEND (as of V4.0) and AG_RECV (as of V4.0)	AG_SEND and AG_RECV allow the transfer of blocks of data with the following length: • 1 to 8192 bytes for ISO transport, ISO-on-TCP, TCP, e-mail • 1 to 2048 bytes for UDP
Restrictions for UDP	
• Transfer is not confirmed	The transfer of UDP frames is unconfirmed, in other words the loss of messages is not detected or displayed by the send block (AG_SEND).
• No receipt of UDP broadcast	To avoid communications overload of the CP due to high broadcast load, the CP does not allow receipt of UDP broadcasts.
• UDP frame buffering	Size of the frame buffer with buffering enabled: 2 Kbytes Note: Following a buffer overflow, newly arriving frames are discarded.

Execution times of the FCs AG_SEND / AG_RECV

The execution time required to process the FC blocks (AG_SEND, AG_RECV) required on the S7-300 / C7-300 CPU is decisive for the calculation of the CPU cycle times (OB1) for SEND/RECEIVE connections.

Table 2- 5 Execution times of the FCs AG_SEND / AG_RECV

Component	Explanation / values	
Execution time on the CPU 315-2 DP (6ES7 315-2EG10-0AB0)	Per AG_SEND block call: • <1 ms at <=240 bytes	Per AG_RECV block call: • <1 ms at <=240 bytes
Execution time on the CPU 317-2 PN/DP (6ES7 317-2EJ10-0AB0)	Per AG_SEND block call: • <0.8 ms at ≤240 bytes	Per AG_RECV block call: • <0.8 ms at ≤240 bytes

2.5 Modes and characteristic data for PROFINET IO

Possible mode combinations with PROFINET IO

In PROFINET IO, the CP can handle real-time communication (RT) and/or isochronous real-time communication (IRT). In this case, it can operate as a PROFINET IO device and/or as a PROFINET IO controller.

When configured as a CP 343-1 Advanced (GX31), the CP cannot operate in "IRT controller" mode.

The following individual and combined modes of the CP are possible:

- RT device
- RT controller
- IRT device (high performance)
- RT device + RT controller
- IRT device + RT controller
- RT device + IRT controller: Only when replacing module with a configuration as CP 343-1 Advanced (GX30)

Note

Note the IRT options supported by the module, see section Communication services (Page 16).

Configuration limits of the CP as a PROFINET IO controller

The CP supports the following maximum configuration as a PROFINET IO controller:

Table 2- 6 Configuration limits of the CP as a PROFINET IO controller

Characteristic	Explanation / values
Number of operable PROFINET IO devices *)	128 *), of which: • A maximum of 128 RT devices • If the CP is configured as a CP 343-1 Advanced (GX30), up to 128 IRT devices (high flexibility) can be configured. If data is kept on the CPU, the number of operable PROFINET IO devices may be < 32. This depends on the free configuration memory of the CPU type being used.
Size of the input area over all PROFINET IO devices **)	4096 bytes max.
Size of the output area over all PROFINET IO devices	4096 bytes max.
Size of the IO data area per submodule of a module in an IO device	• Inputs: 240 bytes • Outputs: 240 bytes
Size of the consistency area for a submodule	240 bytes
Permitted number of CP 343-1 Advanced modules that can be used as PROFINET IO controllers within an S7-300 station (rack including expansion racks)	1 Note: Regardless of the CP type (EX30, GX30, GX31 ...), only 1 CP may be a PROFINET IO controller.

*) The number of PROFINET IO devices that can be operated may be reduced if the devices used require extensive configuration data due to numerous submodules. In this case, the memory of the CP is not adequate and you will receive a message about lack of resources in the diagnostics buffer of the CP when downloading the configuration data.

**) The diagnostics addresses of the PROFINET IO devices cannot be used as an input on the IO controller. The data area of the inputs is reduced by the diagnostics addresses used.

Configuration limits of the CP as a PROFINET IO device

The CP supports the following maximum configuration as a PROFINET IO device:

Table 2- 7 Configuration limits of the CP as a PROFINET IO device

Characteristic	Explanation / values
Size of the input area of the PROFINET IO device	1024 bytes max.
Size of the output area of the PROFINET IO device	1024 bytes max.
Size of the IO data area per sub module on the PROFINET IO device	• Inputs: 240 bytes • Outputs: 240 bytes
Size of the consistency area for a submodule	240 bytes
Maximum number of submodules	32

Configuration limits of the CP as a PROFINET IO device and I-device

The CP supports the following configuration if it is configured as a PROFINET IO device and as an I-device:

Table 2- 8 Configuration limits of the CP as a PROFINET IO device and I-device

Characteristic	Explanation / values
Size of the transfer area	240 bytes
Number of transfer areas	32

Configuration limits of the CP as a shared device

The CP supports the following maximum configuration as a shared device:

Table 2- 9 Configuration limits of the CP as a shared device

Characteristic	Explanation / values
Number of possible controllers	2

Size of the user data

The size of the user data is calculated from the maximum frame size (gross 1060 bytes) minus the following values: 1 for the CP itself, 1 per Interface, 1 per port, 1 for each plugged-in module in HW Config or per slot used.

Table 2- 10 Example of calculating the user data of the CP 343-1 as an IO device

Bytes	Explanation
1060	Gross size of the frame
-1	for the CP itself
-1	for the Interface
-2	for 2 ports
-32	for the maximum number of pluggable modules
= 1024	Net size of the user data *

* By using fewer but larger modules, the volume of user data can be increased.

2.6 Characteristic data for PROFINET CBA

Note

PROFINET CBA versus security function

If you use PROFINET CBA, you cannot enable the CP for the "Security" functionality.

The CP supports PROFINET CBA interconnections between PROFINET CBA components.

The "typical" values specified below are values that cause the SIMATIC iMap configuration tool to generate a warning if they are exceeded; it is nevertheless possible that the configuration can be operated.

If one of the limit values specified for the interconnections is exceeded, they cannot be downloaded to the module. When the interconnections are downloaded, the SIMATIC iMap configuration tool generates an error message to this effect. If a limit value relating to the number or size of components is exceeded, the CPU will not change to RUN!

Table 2- 11 Characteristics of PROFINET CBA communication

Characteristic	Typical value	Limit value
PROFINET CBA		
Number of remote interconnection partners	32	64
Total of all attachments	600	1000
Data length of all incoming attachments	2048 bytes	8192 bytes
Data length of all incoming attachments	2048 bytes	8912 bytes
Data length for arrays and structures (acyclic interconnections), maximum	2048 bytes	8912 bytes *)
Data length for arrays and structures (cyclic interconnections), maximum	250 bytes	250 bytes
Data length for arrays and structures (local interconnections), maximum	-	2400 bytes
Remote interconnections with acyclic transmission		
Scanning frequency: Min. scanning interval, selectable values: 100, 200, 500 and 1000 ms	fast value: 20% medium value: 40% slow value: 40%	100 ms minimum
Number of incoming interconnections	50	128 maximum
Number of outgoing interconnections	50	128 maximum
Data length of all incoming interconnections	2048 bytes	8192 bytes
Data length of all outgoing interconnections	2048 bytes	8192 bytes
Remote interconnections with cyclic transmission		
Transfer interval: Min. transfer interval, selectable values: 8, 16, 32, 64, 128, 256 and 512 ms	fast value: 20% medium value: 40% slow value: 40%	8 ms minimum
Number of incoming interconnections	125	200
Number of outgoing interconnections	125	200
Data length of all incoming interconnections Note: The data length of all incoming interconnections limited to 484 bytes gross per transmission frequency and per partner station. Due to the differences in header information, the net data length depends on the data types being used. In the best case, a maximum of 2 byte arrays with a length of 238 bytes can be interconnected; in the worst case, a maximum of 120 properties of the type "Char" can be interconnected.	1000 bytes	2000 bytes
Data length of all outgoing interconnections	1000 bytes	2000 bytes
HMI variables over PROFINET (acyclic)		

Characteristic	Typical value	Limit value
Number of stations that can register for HMI variables (PN OPC/iMap) Stations are 2 * PN OPC and 1 * SIMATIC iMap	-	3
HMI variable update	-	500 ms minimum
Number of HMI variables	-	200 maximum
Data length of all HMI variables	1600 **)	8192 bytes
Deviceinternal interconnections		
Number of deviceinternal interconnections	50	256
Data length of all deviceinternal interconnections	400 bytes	2400 bytes
Interconnections with constants		
Number of interconnections with constants	100	200 maximum
Data length of all interconnections with constants	1024 bytes	4096 bytes
PROFIBUS proxy functionality		
supported	No	No
Access to S7extended variables		
Maximum number of S7 connections for access to variables with the PROFINET attribute "s7extended". Note: The PROFINET attribute "s7extended" is used only by OPC applications over the OPC server; variables with this attribute can only be used with OPC applications.	16 **)	32 maximum Note: You should also keep in mind the maximum number of connections according to section Module replacement / upgrading (Page 96)

*)The maximum size of an output property is 8191 bytes. 1 byte Lifestate must be added to this. This adds up to a total of 8192 bytes.

The same applies to an input property since this is interconnected with an output property of the same size. The maximum data length of 8192 bytes also applies to the sum of several input properties, for example in the case of a byte array (8191 bytes + 1 byte Lifestate).

**) The value is not checked by iMap.

Note

For information on the data length and data type in PROFINET CBA communication, refer to the online help on SIMATIC iMap, the "Creating PROFINET Components" manual (entry ID 22762278) and the "Configuring Plants with SIMATIC iMap" manual, see /22/ (Page 112).

Reaction times for PROFINET CBA

The achievable reaction times for PROFINET CBA communication depend on the following factors:

- Type of interconnection (cyclic or acyclic) and the transfer interval or scanning frequency
- Configuration limits on the component interface (interface DB of the PROFINET CBA function block (FB88))
- CPU cycle time

As a result, the reaction times for cyclic PROFINET CBA interconnections may exceed the configured value for the update time. You should therefore check the reaction time that can be achieved during commissioning.

Since reaction times < 50 ms cannot be guaranteed, you should not set a transfer interval of ≤ 32 ms for cyclic interconnections.

Reaction times of 50 ms can be achieved with CPU cycle times of < 5 ms and with the following configuration:

- < 200 bytes inputs and at the same time
- < 200 bytes outputs
- a maximum of 200 interconnections distributed on 32 partners

With higher CPU cycle times, the PROFINET CBA function block (FB88) should be called more often in the user program.

Note

The values of the utilization parameters of the selected components displayed by SIMATIC iMap with the "Edit / Check utilization" function in the network view relate to the data exchange as far as the CP. They do not apply to data access from the user program.

Execution times of the function block PN_InOut (FB88)

The execution time required to process FB PN_InOut (FB88) required on the S7-300 / C7-300 CPU is decisive for the calculation of the CPU cycle times (OB1) in CBA mode.

Table 2- 12 Execution times of the function block PN_InOut (FB88)

Duration	Length of the interface DB [bytes]			
	512	**1024**	**2948**	**4096**
minimum [µs]	122	123	123	123
maximum [µs]	2330	2330	2400	2400
typical [µs]	1100	1270	1400	1435

From the table, you can see that the OB1 cycle is extended by at least 122 µs and by maximum of 2400 µs.

2.7 Characteristics of e-mail mode

Characteristics

The Advanced CP operates as an email client. It supports SMTP / ESMTP, SMTP-Auth and STARTTLS.

To send emails, precisely one email connection must be set up per CP. The e-mail connection specifies the mail server of the e-mail provider via which all the mails sent by the Advanced CP are delivered.

To send e-mail in the user program of the S7-CPU, use the send call of the SEND/RECEIVE interface (FC AG_SEND).

The maximum data length is 8192 bytes.

Authentication

The CP supports the following authentication methods:

- PLAIN
- LOGIN
- CRAM-MD5
- DIGEST-MD5

For more detailed information, refer to the manual /2/ (Page 108).

If your service provider requires authentication, you need to import the certificate you received from your service provider into the CP to authenticate the CP with the server. For the procedure, refer to the section Importing certificates for SMTP with STARTTLS or FTPS (Page 81)

2.8 Characteristic data for FTP / FTPS mode

TCP connections for FTP/FTPS

FTP actions are transferred from the CP over TCP connections. Depending on the mode, the following characteristic data applies:

- FTP in client mode:

  You can configure a maximum of 10 FTP connections. Up to 2 CP-internal TCP connections are occupied per configured FTP connection. *

- FTP in server mode:

  You can operate a maximum of 2 FTP sessions at the same time. Up to 2 CP-internal TCP connections are occupied per FTP session (1 control connection and 1 data connection). *

* CP-internal TCP connections do not affect the configuration limits of the configured TCP connection resources.

If you use FTPS with authentication, you need to import the certificate you received from your service provider into the CP to authenticate the CP with the server. For the procedure, refer to the section Importing certificates for SMTP with STARTTLS or FTPS (Page 81).

Program block FTP_CMD (FB40) for FTP client mode

For communication via a TCP connection configured with the "Use FTP protocol" option, use the FTP program block FTP_CMD (FB40).

The block execution time in FTP depends on the reaction times of the partner and the length of the user data. A generally valid statement is therefore not possible.

Older program blocks for FTP client mode

The program blocks used in the predecessor modules for FTP transfer can continue to be used.

- FTP_CONNECT, FTP_STORE, FTP_RECTRIEVE, FTP_DELETE, FTP_QUIT

  Restriction: FTPS mode is not possible with these program blocks even when the security functions are enabled.

2.9 Characteristic data for HTTP / HTTPS

Characteristic data of TCP connections for HTTP / HTTPS

For HTTP access, up to 32 CP-internal TCP connections are available. When necessary, these TCP connections are used by one or more Web browsers to display data or files of the CP.

CP-internal TCP connections do not affect the configuration limits of the configured TCP connection resources.

2.10 Characteristic data for the use of Java applets

To transfer larger amounts of data efficiently from the S7BeansAPI using Java applets and the Java bean "S7Variable", you can make use of arrays.

Maximum array size

Depending on the transfer direction, arrays have the following maximum size with the CP 343-1 Advanced:

- When writing data to the CPU: 164 bytes
- When reading data from the CPU: 210 bytes

Note

Note that the maximum block size in bytes is specified here and that the maximum number of array elements is based on the size of the array basic data type (in bytes).

Example

The CP 3431 Advanced can transfer a maximum of 41 array elements of the type DWORD or REAL with a write job since each element of the type DWORD or REAL occupies four bytes.

2.11 Characteristic data of the C-PLUG

Usable C-PLUGs

The CP 343-1 Advanced (GX31) can be operated with the following C-PLUGs:

- C-PLUG 32

  Order number: 6GK1900-0AB00
- C-PLUG 256

  Order number: 6GK1900-0AB01

Write cycles

The flash area allows a limited number of write cycles.

- C-PLUG 32

  Number of write cycles: approx. 100000
- C-PLUG 256

  Number of write cycles: approx. 200000

Recommendation: Avoid writing data cyclically.

For information on the usable memory space, refer to section Technical specifications (Page 99).

2.12 Characteristic data of the integrated switch

Learning addresses / deleting addresses (aging time)

The switch integrated in the CP (PROFINET interface) reads the source addresses included in the data packets. The switch therefore learns the addresses of the end devices connected via a port.

If the switch receives a data packet, it directs this packet only to the port via which the appropriate end node can be obtained.

The switch monitors the age of the learned addresses. Addresses that exceed the "aging time" are deleted and only learned again when required. The aging time is 5 minutes.

Ports can be deactivated individually

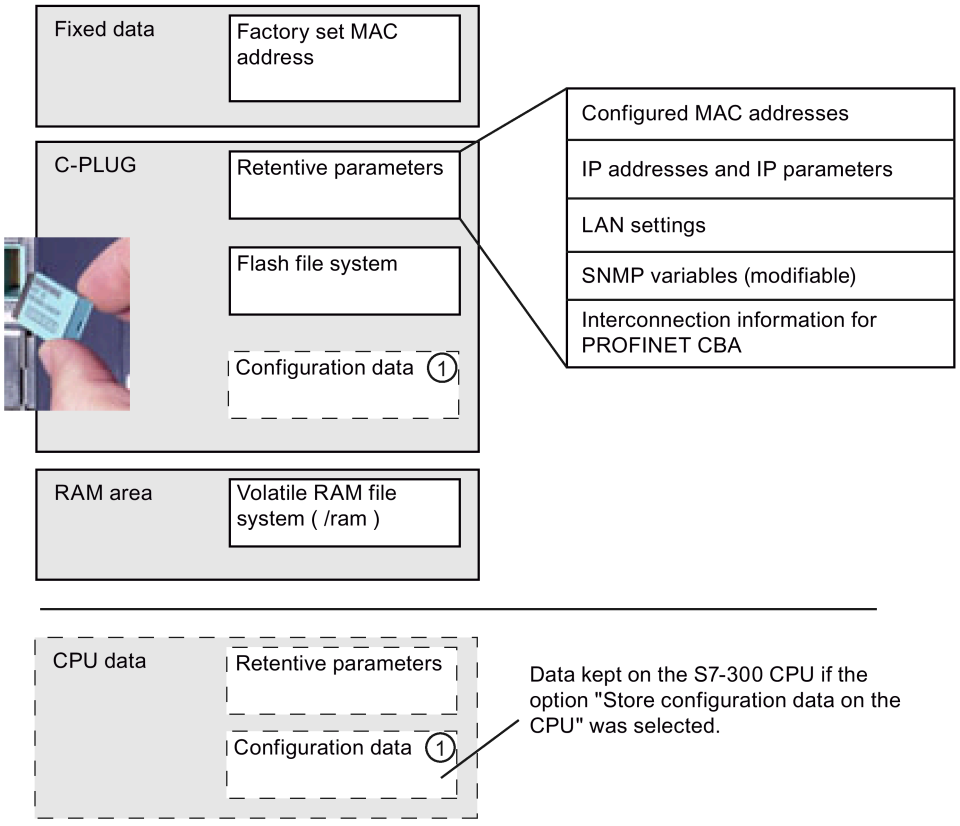
The ports of the switch integrated in the CP and of the gigabit interface can be deactivated individually in STEP 7 in the "Port parameters" parameter group. This can, for example, be used for service purposes.

The port is turned off completely when it is disabled. The corresponding LED on the device is then turned off.

2.13 Memory organization

Memory distribution

The data areas of the CP 3431 Advanced are organized as follows:



Legend:

1) The configuration data can be stored on the CPU or on the CP. This option can be selected in the "Options" > "Replace Module without PG" parameter group.

Figure 2-1 Memory of the CP 3431 Advanced

Recommendation for data storage

If you use the CP in a complex plant configuration - for example as a PROFINET IO controller with up to 128 IO devices - the volume of the configuration data will increase accordingly. In such cases, the time for the transfer of the configuration data from the CPU to the CP may take several minutes.

In such cases, you should weigh up the pros and cons of storing the data on the CP.

Note

Adapting the CPU configuration

If you have large volumes of configuration data and store the configuration data on the CPU you may need to increase the time for the "Transfer of parameters to modules" in the CPU configuration (parameter area "Startup"). This applies, in particular, if there are several CPs in the rack that have their configuration data stored on the CPU.

Meaning of the memory areas

On the CP 343-1 Advanced, the file system is divided into the 2 following areas:

- **Flash area in the CPLUG** (nonvolatile memory):

  The flash area allows data to be stored and retained if there is a power down.

  Since the number of times it is possible to write to this area is restricted, you should avoid repetitive write operations to this area, when such operations are necessary, write to RAM.

  Note

  The flash area of the file system allows a limited number of write cycles, see section Technical specifications (Page 99). You should therefore avoid writing data cyclically.

  If you write temporary data often, you should switch to the RAM file system located in the /ram subfolder. The files of the RAM file system (/ram) are lost if there is power down.

- **RAM area** (/ram volatile memory):

  In contrast to the flash area, the RAM can be written to and read from any number of times. The data in the RAM is retained as long as the CP is supplied with power.

  The RAM is intended to store data that changes during operation and needs to be recorded (data recording services). The RAM is also suitable for temporary storage.

  The RAM area is located in the file system below the "/ram" folder. All files and folders below this folder are lost when there is a power down.

Note the following configuration limits:

Table 2- 13 Configuration limits of the CP 343-1 Advanced

Characteristic	Explanation / values
File names	The length of the file names is limited. Up to 64 characters for the file name, up to 256 characters for the path are permitted. Case sensitivity of the file name can be set in STEP 7.
Memory area for the file system	• Flash area (nonvolatile memory): Refer to "C-PLUG" in section Technical specifications (Page 99). • RAM area (volatile memory): 32 MB
Maximum file size	• RAM: 8 MB • C-PLUG 32: 8 MB • C-PLUG 256: 126 MB

Requirements for use

3

3.1 Operation in control device families

The CP can be operated in the following device families:

- S7-300 stations with the following CPU types:
  - Standard
  - Compact
  - Modular
- C7 compact units in C7 packaging system
- SINUMERIK

The following tables show the device environment in which the CP can be operated with the range of functions described here.

Note

The tables list the CPUs and devices released at the time this manual went to print. CPUs of the S7-300 or C7 control systems released later and not listed in the tables can also handle the range of functions described here.

Table 3- 1 Use of the CP with S7-300

CPU	Order number
CPU 312	6ES7312-1AD10-0AB0 6ES7312-1AE13-0AB0 6ES7312-1AE14-0AB0
CPU 312C	6ES7312-5BD00-0AB0 6ES7312-5BD01-0AB0 6ES7312-5BE03-0AB0
CPU 312 IFM	6ES7312-5AC02-0AB0 6ES7312-5AC82-0AB0
CPU 313	6ES7313-1AD03-0AB0
CPU 313C	6ES7313-5BE00-0AB0 6ES7313-5BE01-0AB0 6ES7313-5BF03-0AB0
CPU 313C-2 DP	6ES7313-6CE00-0AB0 6ES7313-6CE01-0AB0 6ES7313-6CF03-0AB0
CPU 313C-2 PtP	6ES7313-6BE00-0AB0 6ES7313-6BE01-0AB0 6ES7313-6BF03-0AB0

CPU	Order number
CPU 314	6ES7314-1AE00-0AB0 6ES7314-1AE04-0AB0 6ES7314-1AE84-0AB0 6ES7314-1AF10-0AB0 6ES7314-1AF11-0AB0 6ES7314-1AG13-0AB0 6ES7314-1AG14-0AB0 6AG1314-1AG14-2AY0 6AG1314-1AG14-7AB0
CPU 314 IFM	6ES7314-5AE03-0AB0 6ES7314-5AE10-0AB0 6ES7314-5AE82-0AB0 6ES7314-5AE83-0AB0
CPU 314C-2 DP	6ES7314-6CF00-0AB0 6ES7314-6CF01-0AB0 6ES7314-6CF02-0AB0 6ES7314-6CG03-0AB0
CPU 314C-2 PtP	6ES7314-6BF00-0AB0 6ES7314-6BF01-0AB0 6ES7314-6BF02-0AB0 6ES7314-6BG03-0AB0
CPU 315	6ES7315-1AF03-0AB0
CPU 315-2 DP	6ES7315-2AF03-0AB0 6ES7315-2AF83-0AB0 6ES7315-2AG10-0AB0 6ES7315-2AH14-0AB0 6AG1315-2AH14-2AY0 6AG1315-2AH14-7AB0
CPU 315-2 PN/DP	6ES7315-2EG10-0AB0 6ES7315-2EH13-0AB0 6ES7315-2EH14-0AB0 6AG1315-2EH14-2AY0 6AG1315-2EH14-7AB0
CPU 315F-2 DP	6ES7315-6FF00-0AB0 6ES7315-6FF01-0AB0 6ES7315-6FF04-0AB0 6ES7315-6FF04-2AB0 6AG1315-6FF04-2AB0 6AG1315-6FF04-2AY0
CPU 315F-2 PN/DP	6ES7315-2FH10-0AB0 6ES7315-2FH13-0AB0 6ES7315-2FJ14-0AB0 6AG1315-2FJ14-2AB0 6AG1315-2FJ14-2AY0
CPU 315T-2 DP	6ES7315-6TG10-0AB0 6ES7315-6TH13-0AB0
CPU 315T-3 PN/DP	6ES7315-7TJ10-0AB0
CPU 316-2 DP	6ES7316-2AG00-0AB0
CPU 317-2 DP	6ES7317-2AJ10-0AB0
CPU 317-2 PN/DP	6ES7317-2EJ10-0AB0 6ES7317-2EK13-0AB0 6ES7317-2EK14-0AB0 6AG1317-2EK14-2AY0 6AG1317-2EK14-7AB0

CPU	Order number
CPU 317F-2 DP	6ES7317-6FF00-0AB0 6ES7317-6FF03-0AB0 6ES7317-6FF04-0AB0 6AG1317-6FF04-2AB0
CPU 317F-2 PN/DP	6ES7317-2FJ10-0AB0 6ES7317-2FK13-0AB0 6ES7317-2FK14-0AB0 6AG1317-2FK14-2AB0 6AG1317-2FK14-2AY0
CPU 317T-2 DP	6ES7317-6TJ10-0AB0 6ES7317-6TK13-0AB0
CPU 317T-3 PN/DP	6ES7317-7TK10-0AB0
CPU 317TF-3 PN/DP	6ES7317-7UL10-0AB0
CPU 318-2 DP	6ES7318-2AJ00-0AB0
CPU 319-3 PN/DP	6ES7318-3EL00-0AB0 6ES7318-3EL01-0AB0
CPU 319F-3 PN/DP	6ES7318-3FL00-0AB0 6ES7318-3FL01-0AB0

Table 3- 2 Use of the CP with C7 control systems

C7	Order number
C7-613	6ES7613-1CA01-0AE03 6ES7613-1CA02-0AE3
CPU 614	6ES7614-1AH03-0AB3
C7-633 DP	6ES7633-2BF02-0AE03
C7-635 Key	6ES7635-2EC01-0AE3 6ES7635-2EC02-0AE3
C7-635 Touch	6ES7635-2EB01-0AE3 6ES7635-2EB02-0AE3
C7-636 Key	6ES7636-2EC00-0AE3
C7-636 Touch	6ES7636-2EB00-0AE3

Table 3- 3 Using the CP with SINUMERIK 840D power line

Equipment group with CPU type	Order number
NCU561.4 with PLC 314-2 DP	6FC5 356-0BB14-0AA0
NCU571.4 with PLC 314C-2 DP	6FC5 357-0BB14-0AA0
NCU572.4 with PLC 314C-2 DP	6FC5 357-0BB24-0AA0
NCU573.4 with PLC 314C-2 DP	6FC5 357-0BB34-0AA0
NCU561.5 with PLC 317-2 DP	6FC5 356-0BB15-0AA0
NCU571.5 with PLC 317-2 DP	6FC5 357-0BB15-0AA0 6FC5 357-0BB25-0AA0
NCU573.5 with PLC 317-2 DP	6FC5 357-0BB35-0AA0

3.2 Configuration

Software versions

STEP 7 as of the following version is required:

Table 3- 4 Configuration tools for the CP 3431 Advanced

STEP 7 versions	Function
• STEP 7 V5.5 SP 3 • Security Configuration Tool (SCT) V4.0	Requirement for configuration of the CP with the functions of firmware version 3.0
STEP 7 Professional V12.0 SP 1	The functionality of the module CP 343 1 Advanced (6GK7 343-1GX31-0XE0) can be configured. The following is not supported: • PROFINET CBA

Locating support packages

You can install support packages from your local file system if they are already stored there. You will find the support packages on the Internet pages of Siemens Industry Online Support.

- STEP 7 V5.5

  Link: (http://support.automation.siemens.com/WW/view/en/23183356)

- STEP 7 Professional

  Link: (https://support.industry.siemens.com/cs/ww/en/ps/14667/dl)

- Firmware of the CP

  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15346/dl)

Installing support packages (HSPs)

- STEP 7 V5.5

  Install HSPs in STEP 7 / HW Config with the "Options" > "Install Hardware Updates" menu command.

  You will find further information in the STEP 7 online help (under "HSP" or "Hardware update"). After installing an HSP, close and restart STEP 7.

- STEP 7 Professional

  Install support packages in STEP 7 using the menu command "Options" > "Support packages".

  The information system of STEP 7 will provide you with information (keyword "Support Packages" or "Installing Support Packages"). After installing a support package, close and restart STEP 7.

Configuration for use of PROFINET CBA

To be able to work in the PROFINET CBA environment, you require the SIMATIC iMap engineering tool. SIMATIC iMap requires a connection via Industrial Ethernet (TCP/IP protocol).

Table 3- 5 Required SIMATIC iMap version

SIMATIC iMap version	Functions of the CP
V3.0 + Service Pack 3	The PROFINET CBA functionality of the device with hardware product version 1 and firmware version V3.0 can be used.

Table 3- 6 Required SIMATIC iMap STEP 7 addon version

STEP 7 addon version	Functions of the CP
V3.0 + Service Pack 7	The full functionality as described in this document can be used.

To operate PROFINET CBA, you require the current service packs of SIMATIC iMap containing the current version of the program block PN_InOut (FB88).

- SIMATIC iMap V3.0 - Download Service Pack 3
- SIMATIC iMap STEP 7 addon V3.0 - Download Service Pack 7

You can download the service packs at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/14366/dl)

Downloading configuration data

It is possible to download the configuration data to the CP via MPI or LAN/Industrial Ethernet. Downloading is possible over the PROFINET or the gigabit interface of the CP.

GSDML file for configuration in third-party systems

You will find the GSDML file for the CP described here on the Internet under the following entry ID (entry type "Download"):

Link: (https://support.industry.siemens.com/cs/ww/en/ps/14288)

3.3 Program blocks

Program blocks

For some communications services, there are preprogrammed program blocks (FCs / FBs) available as the interface in your STEP 7 user program.

Please note the documentation of the program blocks in the online help of STEP 7 or in the manual /16/ (Page 110).

Note

Current block versions

We recommend that you always use the latest block versions for all module types.

You will find information on the current block versions and the current blocks for download on the Internet under:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15342/dl)

With older module types, this recommendation assumes that you are using the latest firmware for the particular module type.

LEDs

4

The display on the front panel consists of the following LEDs that indicate the operating mode and communication status.

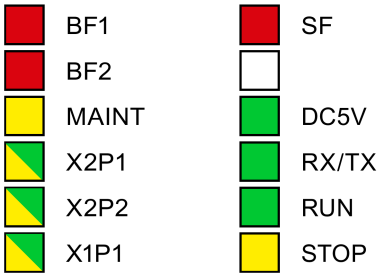


Figure 4-1 LEDs of the CP 3431 Advanced

The LEDs have the following meaning:

- SF: Group error
- BF1: Gigabit interface bus fault
- BF2: PROFINET interface bus fault
- MAINT: Maintenance necessary (diagnostics buffer)
- DC5V: 5 VDC power supply via the backplane bus (green = OK)
- RX/TX: Acyclic data traffic, for example SEND/RECEIVE
  (not relevant for PROFINET IO data)
- RUN: RUN mode
- STOP: STOP mode
- X2P1: Link status / activity of Ethernet port 1 (PROFINET interface)
- X2P2: Link status / activity of Ethernet port 2 (PROFINET interface)
- X1P1: Link status / activity of the gigabit interface

Legend for the following LED tables

The LED symbols in the following tables have the following significance:

LED symbol				-
Meaning	ON	OFF	Flashing	Any status

LEDs for displaying the mode

The different combinations of the LEDs on the front panel indicate the status:

Table 4- 1 LEDs : SF, BF1, BF2, RUN, STOP

SF(red)	BF1 / BF2 (red) *)	RUN (green)	STOP (yellow)	CP operating mode
●	-	○	●	• Starting up after power "ON" or • Stopped (STOP) with errors – For example no valid C-PLUG detected In this state, the CPU or intelligent modules in the rack remain accessible using PG functions.
○	○	☼	●	Starting up (STOP → RUN)
○	○	●	○	Running (RUN)
○	○	●	☼	Stopping (RUN → STOP)
○	○	○	●	Stopped (STOP) In STOP mode, configuring and performing diagnostics on the CP remain possible.
-	●	-	-	Duplicate IP address detected
-	☼	●	-	The CP is configured as a PROFINET IO device; there is no data exchange with the PROFINET IO controller. (BF2 only)
●	☼	●	-	The CP (configured as an I/O controller) has recognized at least 1 IO device as being disrupted. (BF2 only)

SF(red)	BF1 / BF2 (red) *)	RUN (green)	STOP (yellow)	CP operating mode
				• The ports X2P1/X2P2 were configured with a fixed setting for the transmission speed and direction dependency. In the real system, different network properties were detected. Remedy Change the properties of the PROFINET ports in STEP 7 ("Options" tab): – Set the ports to "Automatic settings". or – Enable the "End of topology discovery" option if you want the ports to continue having fixed settings. or • RUN with external error; diagnostics alarm from one or more IO devices is pending. IO device diagnostics will provide detailed information. or • Event display in conjunction with the MRP function. The CP diagnostics buffer provides detailed information.
				Loading using the Firmware Loader is active. **)
				Firmware activation after loading using the Firmware Loader is active. **)
				Firmware was successfully downloaded. **)
				Firmware download aborted. **)
				Module fault / system error

*)) The behavior applies to BF1 and BF2 if there is no restriction listed in the "CP mode" column.

**) Does not apply to loading via the update center in Web diagnostics.

The "MAINT" LED

Note

When the "MAINT" LED lights up, important error messages and/or diagnostics interrupts have occurred. The CP continues in RUN mode.

Check the entries in the diagnostics buffer of the device.

LEDs for displaying the CP communication status

In addition to the LEDs that signal the CP state, the following LEDs provide information about the status of the CP interface to Industrial Ethernet.

Table 4- 2 LEDs : RX/TX, X2P1, X2P2, X1P1

LED	Display	Meaning
RX/TX (green)		The CP is sending/receiving over Industrial Ethernet. Note: PROFINET IO services are not signaled here.
X2P1, X2P2, X1P1 (green / yellow)		Port has no connection to Industrial Ethernet.
		Existing connection via port to Industrial Ethernet (LINK status).
		LED flashes yellow (constant light green): Port sending / receiving over Industrial Ethernet or PROFINET IO. Note: All received / sent frames are signaled for each specific port including those simply forwarded by the switch.
		There is permanent data transfer at the port via Industrial Ethernet (e.g. PROFINET IO on the PROFINET interface).

Module identification (PROFINET or gigabit interface)

Note

Module identification - make the port LEDs flash briefly

With the help of Web diagnostics or the online functions of STEP 7, you can search for and identify the module in the rack. The options for this are as follows:

- In Web diagnostics

  You click the "Flash" button in the update center.
- In STEP 7

  You click the "Flash" button in the "Browse network" dialog

If you click the "Identify" or "Flash" buttons, all the port LEDs of the particular interface flash briefly.

Installation and commissioning 5

5.1 Important notes on using the device

Safety notices on the use of the device

Note the following safety notices when setting up and operating the device and during all associated work such as installation, connecting up or replacing the device.

⚠ WARNING

Safety requirements for installation

The devices are "open equipment" according to the standard IEC 61010-2-201or UL 508 / CSA C22.2 No. 142. To fulfill requirements for safe operation with regard to mechanical stability, flame retardation, stability, and protection against contact, the following alternative types of installation are specified:

- Installation in a suitable cabinet.
- Installation in a suitable enclosure.
- Installation in a suitably equipped, enclosed control room.

5.1.1 Notices on use in hazardous areas

⚠ WARNING

Cleaning the housing

- **In hazardous areas**
  Only clean the outer parts of the housing with a damp, but not wet, cloth.
- **In non-hazardous areas**
  Only clean the outer parts of the housing with a dry cloth.

Do not use any liquids or solvents.

⚠ WARNING

The device may only be operated in an environment with pollution degree 1 or 2 (see IEC 60664-1).

⚠ WARNING

EXPLOSION HAZARD

The device must not be opened.

⚠ WARNING

EXPLOSION HAZARD

SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.

⚠ WARNING

Power supply

The device is designed for operation with a directly connectable safety extra low voltage (SELV) from a limited power source (LPS).

The power supply therefore needs to meet at least one of the following conditions:

- Only safety extra low voltage (SELV) with limited power source (LPS) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

NOTICE

LAN attachment

A LAN or LAN segment with the attachments belonging to it should be within a single low-voltage supply system and within a single building.

Ensure that the LAN is in an of type A environment according to IEEE 802.3 or in a type 0 environment according to IEC TR 62101.

Never establish a direct electrical connection to TNV networks (telephone network) or WANs (Wide Area Network).

⚠ WARNING

EXPLOSION HAZARD

DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.

⚠ WARNING

When used in hazardous environments corresponding to Class I, Division 2 or Class I, Zone 2, the device must be installed in a cabinet or a suitable enclosure.

5.1.2 Notes on use in hazardous areas according to ATEX / IECEx / UKEX

⚠ WARNING

Requirements for the cabinet

To comply with EC Directive 2014/34 EU (ATEX) or the conditions of IECEx, this enclosure or cabinet must meet the requirements of at least IP54 in compliance with EN 60529.

⚠ WARNING

Cable

If the cable or conduit entry point exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 50 °C, only use cables with admitted maximum operating temperature of at least 80 °C.

⚠ WARNING

Take measures to prevent transient voltage surges of more than 40% of the rated voltage. This is the case if you only operate devices with SELV (safety extra-low voltage).

5.1.3 Notes on use in hazardous areas according to UL HazLoc / FM

⚠ WARNING

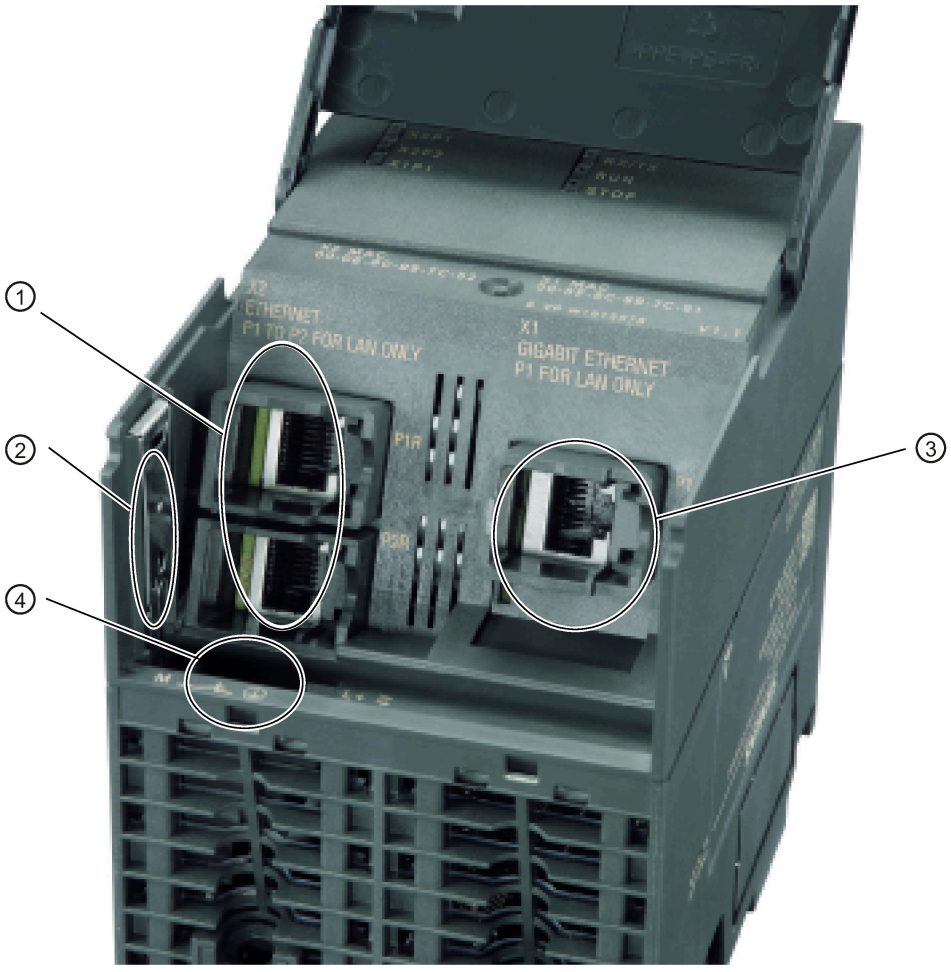
EXPLOSION HAZARD

DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or non-hazardous locations only.

This equipment is suitable for use in Class I, Zone 2, Group IIC or non-hazardous locations only.

5.2 Installing the CP, connecting power and ground



Legend:

① PROFINET interface:
2 x 8-pin RJ-45 jack (ring ports "P1R" and "P2R")

② Slider for setting the chassis ground connection

③ Gigabit interface: 1 x 8-pin RJ-45 jack (P1)
Security function: The padlock symbol identifies the interface to the external, non-secure subnet.

④ Connecting the power supply

Figure 5-1 Connectors of the CP 343-1 Advanced

Installing the CP

Note

During installation, make sure that the upper and lower ventilation slits of the module are not obstructed and good ventilation is possible.

Install the CP as follows:

1. Install the CP on the S7 standard rail.

   Slots 4 to 11 are permitted for the CP in racks 0 to 3 (connected by IM 360/361).

2. Establish the connection via the enclosed bus connector to the backplane bus.

   Proceed as described in the sections dealing with setup and wiring, explained in detail in /18/ (Page 111).

   Note

   The CP cannot be used in an extension rack that is connected via the IM 365! Reason: The required communication bus is not connected to the extension rack via the IM 365.

3. Connect the CP to the power supply.

   Follow the steps as described in detail in /18/ (Page 111) when wiring between the power supply and the CPU.

   Note

   The CPU, CP and IM (if one exists) must be connected to the same power supply.

   Only wire up the S7300 / C7300 with the power switched off!

The connection to Industrial Ethernet is described in the next section.

Ground/chassis ground concept

Note

Note the instructions regarding the grounding and chassis ground concept in the SIMATIC S7 installation guides; see "SIMATIC S7 Programmable Controller S7300 - CPU 31xC and 31x Installation and Hardware", see /18/ (Page 111).

Behind the hinged panel on the left of the device, you will see a slider with which you can connect or disconnect the chassis ground of the 24V power supply with reference ground.

- Slider pushed in: Chassis ground and reference ground are connected (caution: you can feel the slider lock into position).
- Slider pulled out: There is no connection between chassis ground and reference ground.

When shipped: Slider pushed in

Use a screwdriver to set the slider.

5.3 Connecting the CP to Ethernet

Connecting interface X2 to Industrial Ethernet

1. Connect the CP to Industrial Ethernet via one of the RJ45 jacks.
2. Where necessary, connect another component to the remaining free RJ45 jack.

Note

Autocrossing mechanism - effects on the connectors

For small local area networks or for attaching several Ethernet devices, a 2port switch has been integrated on the PROFINET interface of the CP 3431 Advanced.

With the autocrossing mechanism integrated in the switch, it is possible to use a standard cable to connect the PG/PC. A crossover cable is not necessary.

Please note the following points:

- Manual configuration

  If a port is set to manual configuration and autonegotiation is disabled, the autocrossing mechanism is also disabled for this port. Which cable you need to use depends on the partner device (network component or end device).

  In the factory, the ports are set for automatic configuration.

  For more information, refer to section Network settings (Page 73)
- Connecting switches

  If you connect further switches, make sure that no ring is formed in the network.

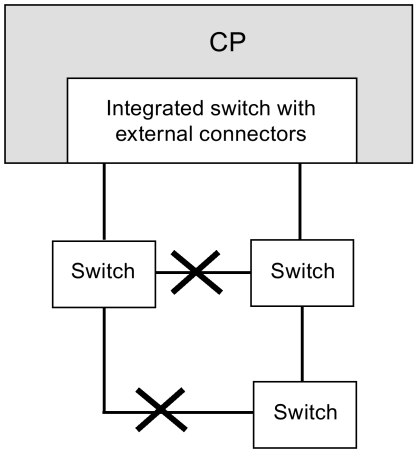


Figure 5-2 Connecting switches

Note

MRP configuration

With an MRP configuration, keep to the setup guidelines for MRP.

You will find examples of network attachments in the general Part A of this manual, see /2/ (Page 108).

Connecting interface X1 to Industrial Ethernet

Note

Operation with security function on the external network

Make sure that the interfaces function correctly if you use the Security function of the CP.

If you use the security function of the CP, only connect the gigabit interface port X1 P1 to the network after the configuration with the security function enabled has been loaded.

You will find examples of network attachments in the general Part A of this manual, see /2/ (Page 108).

Separating the PROFINET and the gigabit interface

It is advisable to connect the PROFINET interface and gigabit interface physically to separate networks. If the two interfaces are not separated, problems can occur when establishing an S7 connection using the ISO protocol under the following conditions:

- Connections to the same partner address were configured via different interfaces.
- When an S7 connection configured at one end needs to be established.

5.4 Commissioning the CP

Configuration

To set up the CP for communication services, read information about the requirements in section Configuration (Page 40) of this manual.

The remaining steps in commissioning involve downloading the configuration data.

Downloading configuration data

You can connect the PG as follows when downloading the configuration:

- Via MPI
- Via Industrial Ethernet

  For further details, refer to the general Part A of this manual:

  – Addressing the first time (IP address assignment / node initialization)

  – To download the defined configuration

  The PG / PC requires a LAN connection, for example via CP 1613, and the corresponding software (e.g. the S7-1613 package or SOFTNET IE). The TCP/IP protocol must be installed. The protocol used must then be applied to the S7ONLINE access point or the ISO protocol.

Loading CBA components

Optional when used with PROFINET CBA: Loading PROFINET CBA components.

If the S7 station in which the CP is operated is used as a PROFINET CBA component, download the interconnections using SIMATIC iMap. For more detailed information, refer to section Using the CP for PROFINET CBA (Page 59).

Diagnostics

Use the diagnostics functions during commissioning and to analyze problems.

The following options are available:

- The LED displays on the CP
- Hardware diagnostics and troubleshooting with STEP 7
- Communication diagnostics with STEP 7 diagnostics
- Static information using HW Config
- Web diagnostics
- If applicable, evaluation of the alarm block FB 54 in the user program
- Queries via SNMP

Startup

Note

Note the following about the start-up procedure:

By starting IT services, particularly when initializing the flash file system, there may be delays during startup. It may then be necessary to set the CPU parameter "Monitoring time for transferring parameters to modules" to a higher value, for example 30 s instead of 10 s.

This avoids the CP changing to the STOP state stopped with error.

You will find the parameter in the properties dialog of the CPU on the "Startup" tab.

5.5 CPLUG (configuration plug)

Exchangeable C-PLUG

The CP has a receptacle for a configuration plug (C-PLUG) that is supplied as standard with the device. Data can be stored on this exchangeable medium and this is retained if there is a power down. You will find the memory capacity in the section Technical specifications (Page 99).

Area of application

The C-PLUG is an exchangeable medium for storage of the configuration data of the basic device (CP). This means that the configuration data remains available if the basic device is replaced. It is possible to replace the module without a PG.

The retentive parameters include the entire configuration data:

- IP address and IP parameters
- Newly set MAC address
- LAN settings
- SNMP variables (modifiable)
- Interconnection information for PROFINET CBA

Note

The CP functions are available only when a C-PLUG is inserted.

If the C-PLUG is missing, the CP starts up but only diagnostics functions are available.

Recommendations for data storage

It is generally recommended that you store the configuration data on the CPU.

If the configuration data is extensive, for example due to using the maximum PROFINET IO configurations, storage of the configuration data on the CP (on the C-PLUG) is recommended in the following situations:

- The configuration memory on the CPU is inadequate.
- The delays due to the extent of the configuration data when starting up the module are unacceptable.

How it works

Power is supplied by the basic device. The C-PLUG retains all data permanently when the power is turned off.

Flash components are used in the C-PLUG in which the number of write operations is limited.

This must be taken into account when using blocks in the user program that write data to the C-PLUG (for example FB55 IP_CONFIG with changing IP parameters). Refer to the information in section Characteristic data of the C-PLUG (Page 34).

Inserting and removing the C-PLUG

Note

Insert and remove the C-PLUG only when power is off

The C-PLUG must be inserted or removed only when the power is off!

The slot for the C-PLUG is on the rear panel of the device.

The C-PLUG is inserted in the receptacle.

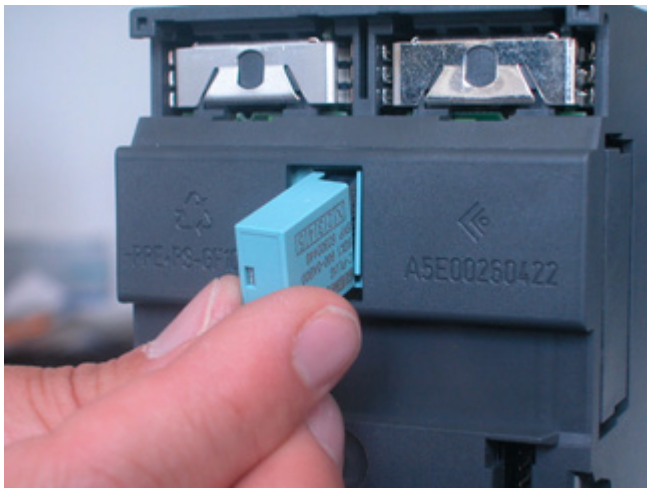


Figure 5-3 Inserting a C-PLUG

It is only necessary to remove the C-PLUG if a fault occurs on the basic device (see figure).

Remove the C-PLUG from the slot using a screwdriver.

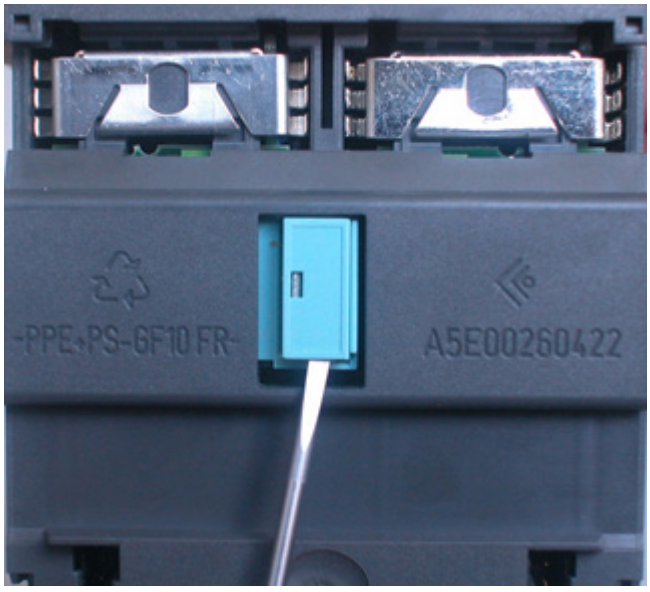


Figure 5-4 Removing the C-PLUG

Function

If the CPLUG has not yet been written to (as shipped) when the device starts up, all the configuration data of the CP is saved automatically on it. Changes to the configuration during operation are also saved on the C-PLUG without any operator intervention being necessary.

If the C-PLUG is inserted, the basic device automatically uses the configuration data of the C-PLUG. This is, however, only possible when the data was written by a compatible device type.

This allows fast and simple replacement of the basic device. If a device is replaced, the C-PLUG is taken from the failed device and inserted in the replacement. As soon as it starts up, the replacement automatically has the same device configuration as the failed device.

C-PLUG formatting

Use only C-PLUGs that are formatted for the CP 343-1 Advanced. C-PLUGs that have already been used and formatted in other device types must first be formatted for the CP 343-1 Advanced device type.

Use STEP 7 to do this. For more detailed information, refer to the online help in the topic “General Diagnostics Functions - C-PLUG Diagnostics Object".

After formatting, all data areas are deleted on the C-PLUG. The configuration data is adopted only after reloading or after turning on the power supply again.

Diagnostics

Inserting a C-PLUG containing the configuration of an incompatible device type, accidentally removing the C-PLUG or general malfunctions of a C-PLUG are signaled by the diagnostic mechanisms of the host device (SFLED red).

Using the CP for PROFINET CBA

6

Requirements and conditions

- Configuration for PROFINET CBA is only possible with STEP 7 V5.5.

  For details, see section Configuration (Page 40)

- Operation under PROFINET CBA is supported only via the PROFINET interface.

  The following information on configuration therefore relates only to the configuration of the PROFINET interface.

Note

Simultaneous operation of PROFINET CBA and a PROFINET IO device is not possible and is interlocked in the configuration in STEP 7.

Note

PROFINET CBA versus security function

If you use PROFINET CBA, you cannot enable the CP for the "Security" functionality.

Procedure

1. To be able to use the CP with PROFINET CBA, you create your user program with STEP 7 and configure the S7300 station.
2. You then configure the interconnections between the PROFINET CBA components with SIMATIC iMap.

6.1 CBA interface in the user program with FB88

PN_InOut (FB88) and interface DB

The interface to the user program is the interface DB for PROFINET CBA. The task of function block PN_InOut (FB88) is to transfer data from the interface DB to the CP and from the CP to the interface DB.

Please note the documentation of the function blocks in the online help of STEP 7 or in the manual /16/ (Page 110).

6.2 Preparing for configuration with STEP 7

Requirements

During configuration, remember the following requirements for subsequent use with PROFINET CBA:

- Configure the modules for the S7300 station in STEP 7

  You can assign the option "Use this module for PROFINET CBA communication" to one (and one only) CP 3431 Advanced in an S7300 station (in the "PROFINET" parameter group)

- Configuration of the PROFINET interface

  If you use the S7300 station as a standard component, you will need to make the following settings when you later configure the PROFINET interface:

  Disable the "Set MAC address / use ISO protocol" option.

  Note

  ISO transport connections and S7 connections using the ISO protocol cannot be operated when using the S7300 station as a PROFINET CBA standard component!

For more detailed information on adopting the configuration data in the SIMATIC iMap engineering tool, refer to the documentation on SIMATIC iMap, see /22/ (Page 112).

6.3 PROFINET CBA configuration with SIMATIC iMap

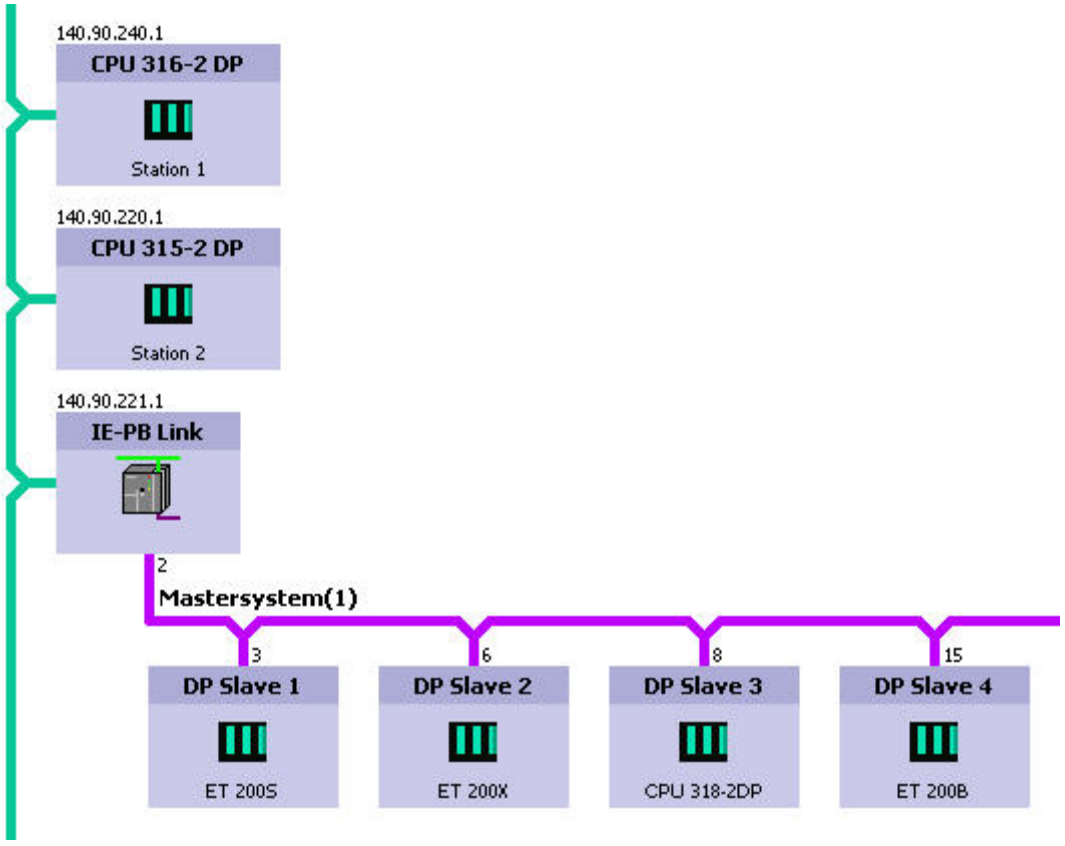
Function in the PROFINET CBA environment

The CP is a PROFINET CBAcompliant device. An S7300 station equipped with this CP can be interconnected in SIMATIC iMap as a PROFINET CBA component.

The configuration of the interconnections between the PROFINET CBA components is created in the plant view of SIMATIC iMap.

Network view in SIMATIC iMap

The following graphic shows the network view of SIMATIC iMAP and illustrates how a CP in an S7300 station establishes a connection between DP slaves on PROFIBUS DP and the S7300 station on Industrial Ethernet via an IE/PB Link.



Legend:

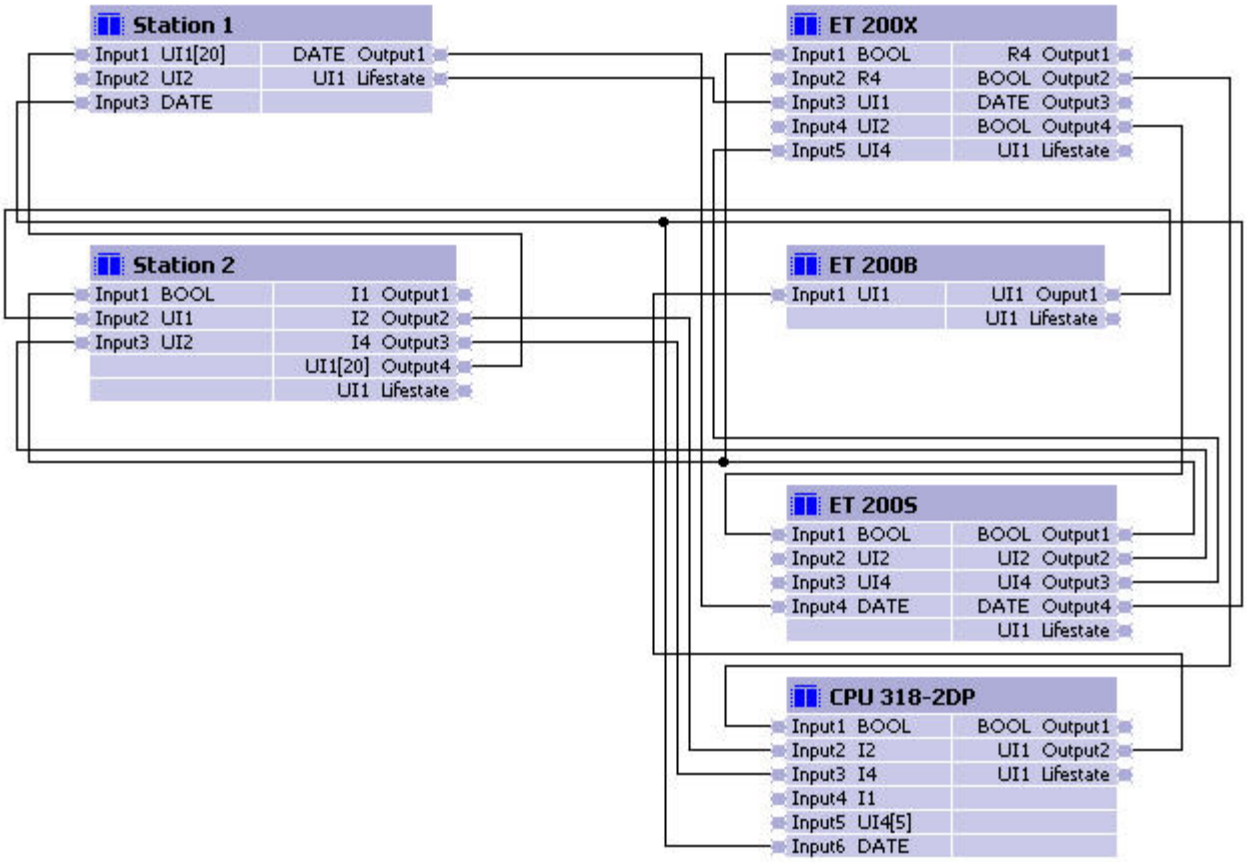
S7-300 stations with CP 343-1 Advanced

Figure 6-1 Network view in SIMATIC iMap

Plant view in SIMATIC iMap

In the plant view, the interconnection of input and outputs via the CP 3431 Advanced becomes visible.

Here, you can only see the PROFINET CBA components with their interconnections to the process inputs and process outputs.



Legend:

S7-300 stations with CP 343-1 Advanced

Figure 6-2 Plant view in SIMATIC iMap

Assigning addresses and properties in SIMATIC iMAP

You assign addresses and properties depending on the component type of the S7300 station as follows:

- S7300 station as singleton component

  Addresses and properties can only be changed in STEP 7.

- S7300 station as standard component

  Addresses and properties can only be changed in SIMATIC iMap.

Note

Remember that with the CP 343-1 Advanced, the initial addressing must be made using STEP 7. You will find the description of this in the general Part A of this manual.

Downloading configuration data

When using PROFINET CBA, downloading configuration data depends on the component type of the S7300 station, as follows:

- **Case A: S7300 station as singleton component**
  - Downloading with STEP 7

    Download the user program and configuration data to the S7300 station with STEP 7.
  - Download the interconnection information of the process inputs and process outputs to the PROFINET CBA components over the Ethernet connector with SIMATIC iMap.
- **Case B: S7300 station as standard component**
  - Downloading with SIMATIC iMap

    Download the user program and configuration data to the S7300 station with SIMATIC iMap.
  - Download the interconnection information of the process inputs and process outputs to the PROFINET CBA components over the Ethernet connector with SIMATIC iMap.

NOTICE
If problems occur while downloading interconnections from SIMATIC iMap, for example power down on the target station, it is not always possible to download the interconnections again when the power returns. If this error occurs, SIMATIC iMap reports the station as being unreachable. Remedy: Change the CP 343-1 Advanced from STOP to RUN using the PG command to bring the target station back to an operable statuss and to allow renewed downloading of the interconnections from SIMATIC iMAP.

Device diagnostics in SIMATIC iMap

In the online view of SIMATIC iMap, you can use diagnostics functions and, for example, read out device and functional information.

Note

For more detailed information on adopting the configuration from STEP 7 and use with PROFINET CBA and the SIMATIC iMap engineering tool, refer to the documentation on SIMATIC iMap /22/ (Page 112).

6.4 Using PROFINET CBA communication and standard communication at the same time

Note

The information in this section applies only if a singleton component was created from the S7300 station. With a standard component, the connection information configured in STEP 7 is lost.

Overview

Parallel operation of PROFINET CBA communication and standard communication using the services S7 communication and S5compatible communication is possible with the CP.

This mode is important for your application when, for example, you want to implement communication between existing "conventional" SIMATIC devices and PROFINET CBA devices in an existing system.

The special feature is that the configuration of the communication for PROFINET CBA devices is only possible in SIMATIC iMap. Communication with conventional devices, on the other hand, requires that the connections are configured in STEP 7.

Recommended procedure

Here, we would like to give you a few tips and recommendations.

For communication between a PROFINET CBA device and a conventional device, use S7, ISO transport, TCP or ISOonTCP connections.

Configure the S7 and TCP connections in STEP 7 as follows:

- For S7 communication
  - PROFINET CBA device: Single-ended passive (partner unspecified)

    No configuration is necessary if the device involved in S7 communication is operated simply as a server.
  - Conventional device: Single-ended active
- For S5compatible communication (TCP / ISOonTCP connections)
  - PROFINET CBA device: Unspecified passive
  - Conventional device: Unspecified active

This achieves the following:

- You can specify the connection partner for the conventional devices at any time with STEP 7;
- You can use the PROFINET CBA devices in SIMATIC iMAP, in other words interconnect them, without needing to change the connection configuration again afterwards in STEP 7. On the configured connections, the devices are always ready to send and receive (the connection is established by the active partner).

For the PROFINET CBA device, this means the following procedure:

Note

The steps involved depend on whether it is a standard or singleton component!

The following procedure applies only to singleton components.

1. First configure unspecified connections in STEP 7 (only with TCP, see above).
2. Create suitable user programs in STEP 7 to handle communication with the conventional devices.
3. Then generate the PROFINET CBA component in STEP 7 and enter this in the SIMATIC iMap library.
4. Interconnect the PROFINET CBA component in SIMATIC iMap.
5. Download the user program and configuration data to the S7300 station with STEP 7.
6. Download the interconnection information of the process inputs and process outputs to the PROFINET CBA components over the Ethernet connector with SIMATIC iMap.

Configuration and operation

7

Note

Closing the front panel

During operation, keep the hinged front panel closed. The upper and lower ventilation slits of the module must not be covered. Good ventilation must be possible.

7.1 Security recommendations

Keep to the following security recommendations to prevent unauthorized access to the system.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Check regularly for news on the Siemens Internet pages.
  - You can find information on Industrial Security here:
    Link: (http://www.siemens.com/industrialsecurity)
  - You can find information on security in industrial communication here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.

  Information regarding product news and new firmware versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15353/dl)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the PC directly to the Internet. If a connection from the CP to the Internet is required, arrange for suitable protection before the CP, for example a SCALANCE S with firewall.

Security functions of the product

Use the options for security settings in the configuration of the product. These includes among others:

- Enable the security functions of the CP and set up the firewall.
- Use the secure protocol variants HTTPS, FTPS, NTP (secure) and SNMPv3.
- Protection levels

  Configure access to the CPU under "Protection".
- Leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CP disabled.
- Logging function

  Enable the function in the security configuration and check the logged events regularly for unauthorized access.
- Protection of the passwords of program blocks

  Protect the passwords that are stored for the blocks in data blocks from being viewed. The procedure is described below.

Know-how protection of blocks (STEP 7 V5)

You can prevent the contents of data blocks (e.g. passwords) from being read out by protecting the block with the "KNOW_HOW_PROTECT" option. Follow the steps outlined below in STEP 7:

1. Select the DB in the block folder.
2. Open the block in the editor.
3. Close the block in the editor.
4. Generate a source from the block in the editor.
5. Select the source of the DB in the sources folder.
6. Open the source.
7. Insert an empty line in the header of the source and write "KNOW_HOW_PROTECT" in this line.
8. Compile the source.

   Result: The block is protected. You can recognize this by the padlock symbol of the DB in the block folder.

If you want to later change parameters in a DB, for example a password, remember the following: The contents of a DB with know-how protection are no longer visible and can only be changed via the source or by direct assignment of parameters.

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.

  See also the preceding section for information on this.
- Do not use one password for different users and systems.

Certificates and keys

- Use a certification authority including key revocation and management to sign certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- It is recommended that you use password-protected certificates in the PKCS #12 format
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- It is recommended that you use certificates with a key length of at least 2048 bits.
- Change certificates and keys immediately if there is a suspicion of compromise.

Protocols

List of available protocols

The following is a list of all available protocols and their ports through which the device can be accessed.

Service/ Protocol	Protocol/ port number	Default port status	Configurable		Authentication	Encryption
			Service	Port		
S7 protocol	TCP/102	Open	--	--	No	No
HTTP	TCP/80	Open	✓	--	No	No
HTTPS	TCP/443	Closed	✓	--	Yes	Yes
FTP	TCP/20	Closed	✓	✓	Yes	No
FTPS	TCP/21					Yes
SNMP	UDP/161	Open	✓	--	Yes (with SNMPv3)	Yes (with SNMPv3)
TCP Modbus	TCP/502	Closed	✓	--	No	No
IPsec	UDP/500	Closed	✓	--	Yes	Yes
PROFINET CM	UDP/34964	Open	--	--	No	No
PROFINET-RPC 2x **PROFINET-PN-EPM**	UDP/552xx	Open	--	--	No	No
PROFINET-CBA RPC	TCP/135	Closed	--	--	No	No

Explanation for table:

- **Service/Protocol**

  Protocols that the device supports.
- **Protocol/port number**

  Port number assigned to the protocol.
- **Default port status**
  - Open

    The port is open at the start of the configuration.
  - Closed

    The port is closed at the start of the configuration.
- **Configurable port**
  - ✓

    The port can be configured.
  - --

    The port cannot be configured
- **Authentication**

  Specifies whether the communication partner is authenticated.
- **Encryption**

  Specifies whether the transfer is encrypted.

Ports of communication partners and routers

Make sure that you enable the required client ports in the corresponding firewall on the communications partners and in intermediary routers.

These can be:

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SNMP / 161 (UDP)
- SMTP / SMTP (STARTTLS) / 25 (TCP) - Open in CP on block call (outgoing only)
- FTPS / 20, 21 (TCP)
- Syslog / 514 (UDP)

7.2 Controlling the mode

You have the option of changing the mode of the CP between RUN and STOP using the STEP 7 configuration software (PLC > Accessible Nodes).

Change from STOP to RUN

The CP loads configured and/or downloaded data into the work memory and then changes to RUN mode.

Change from RUN to STOP

The CP changes to STOP - transitional phase with LED display "Stopping (RUN → STOP").

- Established connections (ISO transport, ISOonTCP, TCP, UDP connections) are terminated.
- Downloading interconnections for PROFINET CBA communication is not possible.
- The following the functions are disabled:
  - PROFINET CBA
  - PROFINET IO
  - Time-of-day synchronization
- The following functions remain enabled:
  - Downloading the configuration data and diagnostics of the CP

    Suitable system connections for configuration, diagnostics and PG channel routing still exist.
  - Web diagnostics
  - FTP/FTPS access to the file system
  - HTTP / HTTPS access
  - Routing function

Module access protection

The configurable module access protection has the following effects on the functions described here:

- Module access protection: Not locked

  The functions cannot be executed.
- Module access protection: Status-dependent

  With this setting, it is only possible to control the mode when the CPU is in STOP mode.

7.3 Effects of protection levels

Module access protection on the CP

If you enable the protection level "Status dependent" in the CP configuration (“Options” tab), the following actions are only possible when either the CPU or the CP is in the STOP state:

- Changing the operating status of the CP (RUN → STOP)
- Resetting / memory reset

  Note the additional restriction if a protection level of the CPU is enabled.
- Formatting the C-PLUG

  Note the additional restriction if a protection level of the CPU is enabled.
- Loading firmware using the NCM Firmware Loader.

Further restrictions on access to the CP result from configuring a protection level for the CPU.

Protection levels of the CPU

If you configure a protection level ≥ 2 in the configuration of the CPU ("Options” tab), this has the following effects on the operation of the CP:

- **Initialization of the CP / assigning an IP address using a different method**

  Using the Primary Setup Tool (PST) / SINEC PNI, you can only assign an IP address to the CP once.
- **No PST / SINEC PNI with IP configuration using DHCP or in the user program**

  If you have configured the setting of the IP addresses of the CP from a DHCP server or using the user program (IP_CONFIG), you cannot assign an IP address to the CP with the PST / SINEC PNI.
- **Formatting the C-PLUG**

  It is not possible to format the C-PLUG of the CP.

  Remove the protection level of the CPU to take this action.
- **Resetting / memory reset**

  It is not possible to reset or to reset the memory of the CP.

  Remove the protection level of the CPU to take this action.
- **Downloading configuration data to the CP (EX11, GX11)**

  The following restriction applies only to the CP "EX11" and "GX11":

  A change between data storage on the CPU and data storage on the CP is not possible.

  Remove the protection level of the CPU to take this action.

7.4 Configuration in STEP 7

Configuration in STEP 7

You configure the CP alternatively with the following configuration tools:

- STEP 7 V5

  For configuring the security functions, you also require the Security Configuration Tool (SCT).

- STEP 7 Professional

You will find the required versions in the section Configuration (Page 40).

The following information on configuration applies to both configuration tools.

7.5 Network settings

7.5.1 IP address assignment and communications path

Networking the gigabit interface and PROFINET interface

If the communications partner can be reached via the PROFINET interface and a router, you should not network the gigabit interface with the subnet of the communications partner at the same time. Depending on the communications service or physical network configuration there may otherwise be conflicts.

Example: Gigabit interface networked but not connected

The gigabit interface is, for example, networked with a subnet A, however not physically connected to subnet A.

The PROFINET interface is networked with a subnet B and communications partner X in subnet A can be reached via a router.

There is now communication with communications partner A. During operation, based on the configuration the CP selects the gigabit interface as the direct possible communications path to communications partner X. Because it is not connected the gigabit interface is actually not available and communication cannot be established.

Separating the PROFINET and the gigabit interface

It is advisable to separate the PROFINET interface and gigabit interface physically. If the two interfaces are not separated, problems can occur when establishing an S7 connection using the ISO protocol under the following conditions:

- If connections to the same partner address were configured via different interfaces.
- if an S7 connection configured at one end needs to be established.

7.5.2 Fast Ethernet with the PROFINET and gigabit interface

The common transmission characteristics of the two interfaces are described below. For information on the transmission speed 1 Gbps of the gigabit interface, see Influence of MPI on connections via Industrial Ethernet (Page 86)

The configuration of the network settings "Transmission medium / duplex" is made for both interfaces in STEP 7 in the port properties of the relevant interface.

Row "X1P1": Port properties of the gigabit interface

Row "X2P1": Properties of port 1 of the PROFINET interface

Row "X2P2": Properties of port 2 of the PROFINET interface

Automatic setting or individual network settings

As default, the CP is configured for automatic detection (autosensing / autonegotiation / autocrossing).

Note

In normal situations, the basic setting ensures troublefree communication. You should only change this in exceptional situations.

If you create a manual configuration for the CP, the automatic negotiation of the network settings (autonegotiation) is no longer effective. If, on the other hand, the communication partner works with autonegotiation, no communication will be established.

Only use manual configuration when the communication partner works with the same manually set configuration.

Autocrossing mechanism

The automatic setting also includes an "autocrossing" mechanism. With autocrossing, you can connect network components and end devices using either crossover or straight-through cables.

STEP 7 special diagnostics and Web diagnostics display the network setting

Diagnostics of the port settings for the CP described here is possible using the entries in the diagnostic buffer, with Web diagnostics, with SNMP, special diagnostics and the LED displays.

You will find information on the currently used network settings in STEP 7 as follows:

- In special diagnostics under the diagnostics object "Industrial Ethernet" in the "Network Connection" group box
- in STEP 7 with the menu command "PLC > Module Information"
- In Web diagnostics

Further notes:

- Autocrossover

  If you disable the "Automatic setting" option, autocrossing is disabled; which cable you then use depends on the integration of the CP (network component or end device).

- 10/100 Mbps network components without "autonegotiation"

  If you use 10/100 Mbps network components that do not support "Autonegotiation", it is possible that you will have to set the mode manually in the CP configuration. As default, the CP is configured for automatic detection.

- Forcing a specific network setting instead of "Autonegotiation"

  If your application requires a fixed network setting instead of "Autonegotiation", both partner devices must have the same setting.

- No reaction to autonegotiation query with manual configuration

  Remember that if you configure the CP manually, it will not react to an autonegotiation query! As a result, a connected partner will not be able to make the required network setting and communication will not be established.

  Example:
  If the CP is set to "100 Mbps full duplex", a CP connected as partner will set itself to "100 Mbps half duplex". Reason: Due to the fixed setting, no autonegotiation response is possible; the connected partner recognizes the 100 Mbps with autosensing but nevertheless remains in half duplex.

- Recommendation: Change "individual network settings" only over MPI

  If you modify the LAN settings using the port parameters, these changes will be adopted by the CP and activated when the configuration data is downloaded to the CP. In some situations, the device may then no longer be obtainable over Ethernet.

  We therefore recommend that you download configuration data to the S7 station over an MPI connection if you change this setting.

  If you download the configuration data over the LAN interface then, depending on the selected setting, it is possible that the current download will not be completed due to the changes to the configuration taking immediate effect and an inconsistent configuration is reported.

  Example:
  The download is started initially with the setting TP/ITP at 10 Mbps half duplex. If the "Individual network setting" is now changed to 100 Mbps full duplex, the download cannot be completed.

7.5.3 Transmission speed of the gigabit interface

If you want to use transmission speed 1 Gbps, leave the interface set to "Automatic settings".

The connection partner must also be configured with the "Automatic settings" (autonegotiation). If the connection partner does not support gigabit Ethernet, the data will be transferred at the next lower speed (100 or 10 Mbps).

7.5.4 Using the CP as an IP router

The CP as an IP router

The CP can be used to forward IP messages from a local network to a higher-level network and vice versa. The CP controls access permission according to the configuration.

An extensive network with further IP subnets can be connected to one of the Ethernet interfaces. To allow this, an external router can be configured on this interface that handles the forwarding for nodes that are not reachable directly. Enter the IP address of this router for the relevant interface in "Default router" in STEP 7.

NOTICE

Router address with DHCP

If an IP address is entered for the relevant interface in "Default router" in STEP 7 and the CP on this interface obtains its IP address from a DHCP server, the reaction is as follows:

- A default router proposed by the DHCP server is not accepted.
- Instead, the IP address set in the "Default router" box is used as the effective router.

If you want the router proposed by the DHCP server to be used, the option "Do not use router" must be set in the "Properties - Ethernet interface" dialog.

You can make the necessary setting in STEP 7 at the following location: Properties dialog "IP configuration" of the interface in question > option "Obtain IP address from a DHCP server"

Note

The use of the CP as a universal router between two extensive networks with other subnets is not supported.

7.6 IP configuration

7.6.1 Detection of double IP addressing in the network

Detecting duplicate addressing

To save you timeconsuming troubleshooting in the network, the CP detects duplicate assignment of an IP address in the network.

If the CP recognizes a duplicate address, an entry is written to the diagnostics buffer. How the CP then reacts depends on the interface and the mode:

- **PROFINET interface**
  - **CP during startup:**

    The CP remains in STOP mode.

    The bus fault LED BF2 lights up.

    When you eliminate the cause by removing the device with the same IP address or by changing its address, you can change the CP to RUN with the control mode function.
  - **CP in RUN mode:**

    The CP remains in RUN mode.

    The bus fault LED BF2 lights up.

    To acknowledge the bus fault LED in RUN mode, set the CP to STOP and then restart it.

    Alternative: After the device with the duplicate IP address has been removed from the network, the bus fault LED goes off automatically.
- **Gigabit interface**
  - **CP during startup:**

    The CP changes to RUN.

    The bus fault LED BF1 lights up.

    The CP cannot be reached via the gigabit interface.
  - **CP in RUN mode:**

    The CP remains in RUN mode.

    The bus fault LED BF1 lights up.

    To acknowledge the bus fault LED in RUN mode, set the CP to STOP and then restart it.

    Alternative: After the device with the duplicate IP address has been removed from the network, the bus fault LED goes off automatically.

7.6.2 Configured S7 connections cannot be operated if the IP address is assigned over DHCP

Note

If you obtain the IP address using DHCP, any S7 connections you may have configured will not work. Reason: The configured IP address is replaced by the address obtained via DHCP during operation.

Note

Obtaining the IP address via DHCP is possible either on the PROFINET interface or on the gigabit interface.

7.6.3 Address assignment with DHCP: Expiry of the lease

Expiry of the lease

If you have configured “Obtain IP address from a DHCP server", when the CP starts up, it is assigned a valid IP address by the DHCP server for a restricted time (period of the lease).

Note

When the lease expires the reaction of the CP is as follows:

- DHCP on the PROFINET interface:

  The CP changes to STOP and loses the previously assigned IP address if the DHCP server does not extend it before expiry of the lease. All communication connections are terminated.
- DHCP on the gigabit interface:

  The CP remains in RUN mode.

7.6.4 Address assignment via DHCP- gigabit interface

Static DHCP

When assigning addresses using DHCP on the gigabit interface, the module should be assigned a fixed IP address in the DHCP server (static DHCP).

A modified IP address is adopted only following a STOP → START change.

Note the restrictions when a protection level is configured for the CPU. See section Effects of protection levels (Page 72) for information on this.

Changing the default router in the DHCP configuration

If you change the data of the default router in the configuration of the DHCP server, the CP needs to be restarted (cycle power).

7.7 PROFINET IO

7.7.1 IP access protection using the IP access control list with a PROFINET IO device

Note the following behavior if IP access protection is activated:

If the CP is configured as a PROFINET IO device, you will need to enter the IP address of the PROFINET IO controller in the IP access control list.

7.7.2 How PROFINET IO devices start up in a large configuration

When operating the module with a large configuration (up to 48 communications connections and up to 128 PROFINET IO devices), it may take several minutes when the station starts up before all PROFINET IO devices have received configuration data from the PROFINET IO controller. The IE/PB Link PN IO operating as a PROFINET IO device is particularly affected by this.

To ensure that the CPU does not interrupt the distribution of project engineering data in this situation, the monitoring times may need to be increased on the CPU ("Startup" parameter group).

7.7.3 PROFINET IO when operating other services at the same time

Sporadically used services

Note the following if you are using functions alongside PROFINET IO that affect the configuration or the operating status, for example IP_CONFIG (FB55), Primary Setup Tool / SINEC PNI, STEP 7 special diagnostics:

Note

The functions listed above can influence the flow in PROFINET IO so that an interruption of cyclic IO data exchange of the PROFINET IO devices lasting several seconds may occur.

7.7.4 Effects of multicast communication on RT communication

Note

If PROFINET IO RT communication is operated at the same time as broadcast (BC) or multicast (MC) in an industrial Ethernet subnet, RT frames can be delayed by long BC frames or MC frames.

Among other things, these frames can be generated by the communications FCs AG_SEND or AG_RECV.

With certain constellations, this can lead to a PROFINET RT communication abort. The factors that influence this are the switch configurations ("switch depth"), the update time and the MC/BC frame lengths.

You will find further information about the influencing factors as well as possible solutions in:

Link: (https://support.industry.siemens.com/cs/ww/en/view/29104898)

7.7.5 Media redundancy

You can use the CP in a ring topology with media redundancy. The CP itself can be redundancy manager or redundancy client.

For more detailed information on configuration, refer to the online help of the "Media redundancy" tab and in Part A of the manual /2/ (Page 108).

Note

If you are using IRT communication, no media redundancy is supported.

7.7.6 IRT communication: Types of synchronization

IRT communication (Isochronous Real Time)

Within an IRT domain, you can use the CP for IRT communication.

The CP supports IRT communication with the IRT option "high-performance". The IRT option "high-performance" optimizes data traffic as the result of topology planning.

Note: The IRT option "high flexibility" is now only supported for the CP 343-1 Advanced (GX30) when the CP 343-1 Advanced (GX31) is configured as a CP 343-1 Advanced (GX30) in STEP 7.

You specify the required synchronization parameters in the "Synchronization" parameter group of the PROFINET interface.

Note

Requirements for configuration

Configuration for IRT communication is only possible with STEP 7 V5.5.x.

7.8 Security

Note on SOFTNET Security Client V4.0

For VPN connections between the CP and SOFTNET Security Client, SOFTNET Security Client V4.0 Hotfix 1 is required.

7.8.1 Attachment to Industrial Ethernet networks

Since the CP forwards frames from and to private and public IP addresses via its two interfaces, you should not connect the CP to a public network.

7.8.2 Using VPN - effects on communication

Communication via VPN tunnel

Communication via a VPN tunnel reduces speed compared with communication outside a VPN tunnel.

In mixed operation with S7 communication and connections of the open communications services (SEND/RECEIVE interface), remember that the CP handles the open communications services with higher priority.

7.8.3 Reloading firewall rules

Behavior with an active tunnel connection

Reloading firewall rules using the "Reload firewall rules online" (in STEP 7 / HW Config in "CP properties", "Security" tab) can lead to communication on an active tunnel connection being aborted.

7.8.4 Activating IP access protection

Dynamically expanding the IP access protection list with the firewall deactivated

If security is activated while the firewall is deactivated, there is no IP access protection. In other words IP access in this device status is not restricted to the IP addresses entered in the IP access protection list.

Nevertheless, even in this device status, it is possible to expand the list for IP access protection dynamically if you have suitable user rights. As result of this action, the added entries are displayed in STEP 7 special diagnostics. Access protection is, however, only effective when the firewall is activated.

Solution:

Activate the firewall in the configuration. With this, the blocking of access for IP addresses not entered in the list becomes effective.

7.8.5 Importing certificates for SMTP with STARTTLS or FTPS

Certificate for authentication

To import a certificate you need to enable the security functions of the CP in STEP 7.

You import the certificate using the certificate manager in STEP 7. Follow the steps outlined below:

1. Open the certificate manager.
   - STEP 7 V5 / SCT: "Options" > "Certificate manager...".
   - STEP 7 Professional: “Global security settings > Certificate manager”
2. Import the certificate that you stored previously in the file system of the PG / engineering station.
   - STEP 7 V5 / SCT: “Import”
   - STEP 7 Professional: In the certificate table, open the shortcut menu "Import" (right mouse button).

7.8.6 Security and STEP 7 special diagnostics activated - configuration activities blocked

Modules with activated security configuration

Note the following behavior on modules with an activated security configuration:

Initial situation:

In HW Config, you open the "Module Information" dialog with the <Ctrl + d> keyboard shortcut. From here, you can start STEP 7 special diagnostics.

Effect:

In this STEP 7 status, the properties of the CP cannot be configured.

Solution:

Close STEP 7 special diagnostics to obtain access to the properties dialog of the CP.

7.9 Timeofday synchronization

General rules

The CP supports the two modes explained below for timeofday synchronization:

- SIMATIC mode
- NTP mode (NTP: Network Time Protocol)

  No automatic changeover to daylight saving time is defined in NTP. As a result, you may need to implement this changeover using a program application.

Security enabled

In the extended NTP configuration, you can create and manage several NTP servers. All NTP servers can be of the type NTP (secure).

Note

Ensuring a valid time of day

If you have enabled security, a valid time of day is extremely important. If you do not obtain the time-of-day from the station (CPU), we therefore recommend that you use an NTP server of the type NTP (secure).

Configuration

For more detailed information on configuration, refer to the online help of the "Time-of-day synchronization" parameter group and in Part A of the manual /2/ (Page 108).

7.10 SNMP agent

SNMP (Simple Network Management Protocol)

SNMP is a protocol for managing networks. To transmit data, SNMP uses the connectionless UDP protocol.

The information on the properties of SNMPcompliant devices is entered in MIB files (MIB = Management Information Base).

The CP supports data queries using SNMP in version 1. It delivers the content of certain MIB objects according to the MIB II standard, LLDP MIB, Automation System MIB and MRP Monitoring MIB.

The CP continues to support data queries via SNMPv3 (security enabled).

MIB file and SNMP profile file

You will find the MIB file and the SNMP profile file of the module in the STEP 7 installation in the folders "S7DATA" > "snmp" under the name of the module.

Further information

For more detailed information on working with MIB files, refer to the documentation of the SNMP client you are using (example of an SNMP client: SNMP OPC server from SIMATIC NET).

You will find more information on MIB in the manual /4/ (Page 108) and on the following page:
Link: (https://support.industry.siemens.com/cs/ww/en/view/15177711)

Supported MIBs

The CP supports the following groups of MIB objects of the standard MIB II according to RFC1213:

- System
- Interfaces
- Address Translation (AT)
- IP
- ICMP
- TCP
- UDP
- SNMP

The other groups of the MIB II standard are not supported:

- EGP
- Transmission

The CP also supports the LLDPMIB according to IEEE 802.1AB, the PROFINET expansions of the LLDPMIB (see also IEC 61158106), the Automation System MIB and the MRP Monitoring MIB.

Exceptions / restrictions:

- Write access is permitted only for the following MIB objects of the system group:
  - sysContact
  - sysLocation
  - sysName

    If DHCP is activated, a set sysName is sent as the host name using DHCP option 12 to the DHCP server to register with a DNS server.

  For all other MIB objects / MIB object groups, only read access is possible for security reasons.
- Traps are not supported by the CP.

"Interfaces" MIB group

This group returns status information about the CP interfaces. The MIB objects of the ifTable provide the status information of the interfaces. The "ifIndex" object identifier is assigned to the CP interfaces as follows:

Table 7- 1 ifIIndex

ifIndex if gigabit interface is		**Type of interface**
networked	not networked	
1	-	Gigabit interface

ifIndex if gigabit interface is		Type of interface
2-3	1-2	Port 1-2 (PROFINET interface)
4	3	Internal CP interface

Access permissions using community name

The CP uses the following community names to control the access rights in the SNMP agent:

Table 7- 2 Access rights in the SNMP agent

Type of access	Community name *)
Read access	public
Read and write access	private

*) Note the use of lowercase letters!

MIB files for your SNMP tools

If you use an SNMP tool, you will find the MIB files relevant to the CP in the STEP 7 installation in the following folder:
`<Drive>\<Installation folder>\Siemens\Step7\S7DATA\snmp\mib`

For the Automation System MIB, for example, these are the following files:

- automationPS.mib
- automationSmi.mib
- automationSystem.mib
- automationTC.mib

7.11 Programmed communication connections

7.11.1 Behavior with programmed communications connections

Downloading the configuration using IP_CONFIG (FB55)

IP_CONFIG (FB55) allows programcontrolled transfer of the configuration data.

Note

If the CP is in PG STOP mode and the configuration is downloaded using IP_CONFIG (FB55), the CP then changes automatically to RUN.

7.11.2 IP access protection with programmed communication connections

In principle, it is possible to set up communications connections using program block IP_CONFIG (FB55) by programming and at the same time by configuring IP access protection.

When configuring specified connections (active endpoints) in STEP 7, the IP addresses of the partners are entered automatically in the IPACL (IP Access Control List).

Communications connections programmed with IP_CONFIG (FB55) are also entered in the ACL.

Please note the following point:

Note

The IP addresses of partners with unspecified connections (passive end points) are not entered in the IPACL. Communication with unspecified nodes is only possible when IP access protection is enabled if the IP addresses were entered previously in the ACL during configuration.

The configuration of IP access protection and the aspects when the security function is enabled are described in the general part of this manual /2/ (Page 108).

7.11.3 Programmed communications connections - assigning parameters to the ports

The CP supports the following settings when assigning parameters to the ports in the parameter block for TCP connections and UDP connections:

- SUB_LOC_PORT parameter

  The port can be specified as an option when the connection is established actively.

- SUB_REM_PORT parameter

  The port can be specified as an option when the connection is established passively.

7.12 Influence of MPI on connections via Industrial Ethernet

Adding/removing MPI nodes

If a station on the MPI bus is added or removed, for example because a service PG has been connected or disconnected, it is possible that active communication connections on the communications bus are aborted. This has the following effects on the communication connections on Industrial Ethernet:

All S7 connections are temporarily aborted.

- Exceptions: This does not apply when using CPUs with a separate communication bus, for example:

  CPU 318-2, CPU 317-2 PN/DP, CPU 319-3 PN/DP, CPU 315-2 PN/DP, CPU 315F-2 PN/DP, CPU 317-2 DP, CPU 317T-2 DP, CPU 317F-2 DP, CPU 317F-2 PN/DP, CPU 318-2 DP

  FETCH/WRITE connections are temporarily aborted.

On the FC interface in the user program, the condition codes made up of the DONE, ERROR and STATUS parameters must be evaluated in FC11 / FC12.

7.13 Ping

Permitted length of ICMP packets

Pings with a packet size of more than 1000 bytes are evaluated as an attack and filtered by the CP. This response is intentional and improves the robustness of the CP in an industrial environment.

7.14 Downtime if an S7 connection aborts

Note

Downtime if an S7 connection aborts

If an S7 connection is aborted, for example failure of the connection partner, it can take up to 40 s before the connection abort is recognized in the block. Block processing is aborted and the block resource is available again. This applies to BSEND (FB12), BRCV (FB13), USEND (FB8), URCV (FB9).

With PUT/GET, block processing cannot be aborted.

Diagnostics and upkeep

8

8.1 Online security diagnostics via port 8448

Security diagnostics via port 8448

Requirements:

- With an activated firewall, access must be enabled.

If you want to perform security diagnostics in STEP 7 Professional, follow the steps below:

1. Select the CP in STEP 7.
2. Open the "Online & Diagnostics" shortcut menu.
3. In the "Security" parameter group, click the "Connect online" button.

In this way, you perform the security diagnostics via port 8448.

8.2 Memory reset / reset to factory defaults

Note

Data on the CP is deleted - CPU data is retained

The functions for resetting and resetting to factory defaults described here do not change the configuration data on the CPU! Only the data kept on the CP (CPLUG and RAM) is deleted.

If you subsequently upload the configuration data from the CPU to a PG you will always object the configuration data that was previously on the CP (with parameters, connections, IP address).

Available functions

The CP has a twolevel function available for deleting:

- **Memory reset**

  Following the memory reset, the CP retains the preset MAC addresses and the retentive parameters. The CP is therefore immediately ready for downloads via the LAN with the IP address.

  Note

  CP no longer reachable via VPN

  With a memory reset, the VPN configuration is deleted and the CP can no longer be reached via VPN.

  The configuration of the IP-ACL (IP Access Control List) and the firewall configuration are retained after the memory reset.

The undeleted retentive parameters include:

- IP address, subnet mask and, if applicable, router address
- LAN settings
- PROFINET CBA interconnections

- **Resetting to factory settings**

  After resetting to factory settings, the CP only contains the default MAC addresses (as shipped).

How to use the functions

You can start the memory reset functions in STEP 7. The CP must be in STOP. When you reset memory using special diagnostics, the CP is automatically changed to STOP.

- Memory reset
  - In STEP 7 V5.5 with the menu command "PLC" > "Clear/Reset"
  - In STEP 7 special diagnostics with the "Operating Mode" > "Clear/Reset Module" menu command
  - In STEP 7 Professional V11 with STEP 7 special diagnostics
- Resetting to factory settings
  - In STEP 7 V5.5 with the menu command "PLC" > "Edit Ethernet Node..." > Select CP > "OK" > "Reset to Factory Defaults"
  - In STEP 7 special diagnostics with the "Operating Mode" > "Reset to Factory Settings" menu command
  - In STEP 7 Professional V11 with "Online > Online & Diagnostics > Functions > Reset to Factory Settings"

Memory reset: Effects

The CPU in the S7 station does not recognize that the CP memory was reset. The CP therefore changes to the "stopped with error" state (see section LEDs (Page 43)).

Following the memory reset, the CP retains the configured MAC addresses, the IP address and the retentive parameters. For information on the retentive parameters, refer to Memory organization (Page 35). The configuration data must then be reloaded.

The CP is therefore immediately ready for downloads using the IP address.

If the configuration data is stored on the CPU, you can start a download by cycling power.

This has the following overall effect:

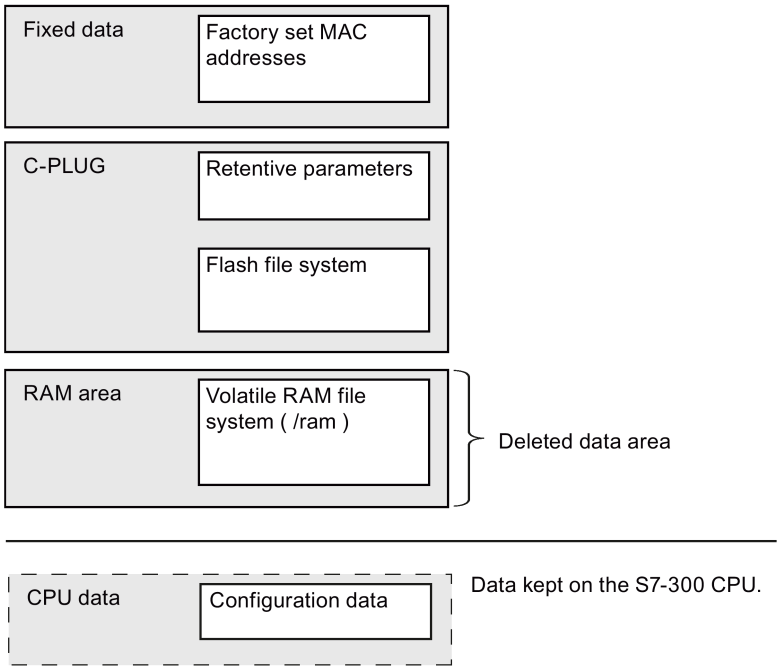


Figure 8-1 Memory following a memory reset

Resetting to factory settings: Effect

The following data is not deleted:

- After resetting to factory defaults, the CP always retains the factory set MAC addresses (as supplied).
- The data in the file system of the CPLUG (flash area) is retained.

The following data is deleted:

- The data in the volatile RAM area is deleted.
- The retentive parameters on the C-PLUG are deleted.

This has the following overall effect:

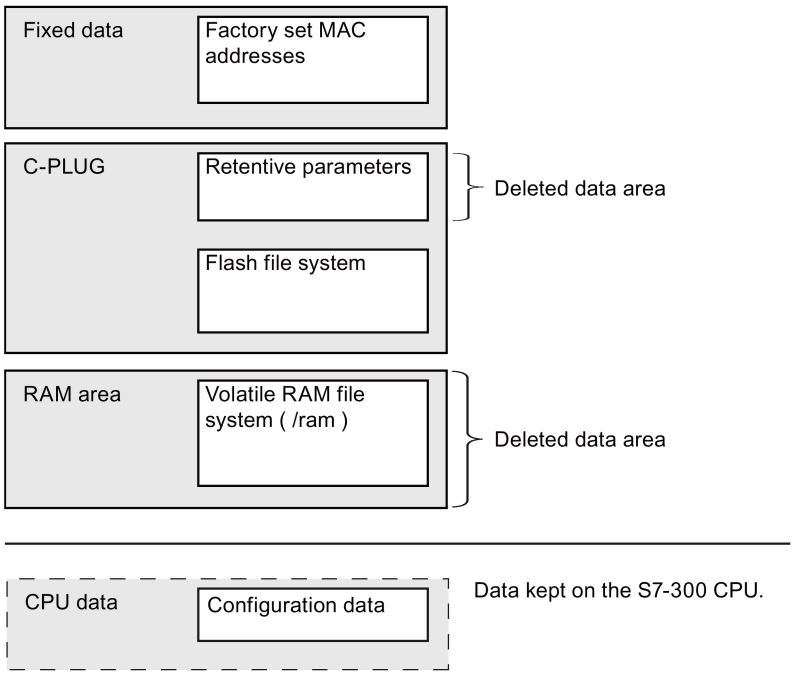


Figure 8-2 Memory after Reset to Factory Settings

Note

Interconnection information for PROFINET CBA is deleted

Interconnection information for PROFINET CBA is included in the retentive parameters on the C-PLUG. This interconnection information is therefore deleted in this procedure.

8.3 Loading new firmware

Options for a firmware update

The following alternative methods can be used to download new firmware to a SIMATIC NET CP:

- Using the update center

  You can reach the update center using Web diagnostics.

  The CP supports the storage of several firmware versions. Using the firmware load function in the update center, you can activate the required firmware version.

  Requirement:

  The "Firmware download via Web" option is selected in the configuration and the user rights have been set.

- Using the firmware loader supplied with STEP 7

  Requirement:

  – To download firmware, you require an Industrial Ethernet CP module in the PG/PC (for example, CP 1613) or a normal Ethernet module with the "Softnet" software package.

  – The S7ONLINE interface must be set to the "ISO - Industrial Ethernet" protocol. It is not possible to download using TCP/IP (and therefore not to other networks).

  Always run the download using the active MAC address of the CP!

  Note the descriptions of firmware downloads in the manual Part A /2/ (Page 108).

Note

Security function enabled

If the security function is enabled on modules, it is not possible to load firmware using the Firmware Loader.

Instead, we recommend that you load the firmware when necessary using the update center in Web diagnostics.

To load the firmware on the module using the Firmware Loader, the module must be in the "security disabled" status. Where necessary, one of the following steps is therefore necessary:

- Reset the module to the factory settings.

  or

- Download the configuration data to the module without security enabled.

Preparing to download new firmware

The following applies to both download methods:

Connect the CP module to the PG/PC via a LAN cable.

You can download the firmware via one of the two interfaces of the CP.

Downloading using the update center

1. Use your browser to navigate to Web diagnostics of the CP on the "Update Center / Firmware" page.
2. Open and download the required firmware download file using the "Browse" / "Download" button.

   The firmware file is downloaded.

   On completion of the download:
3. Activate the loaded firmware with the "Activate" button.
4. After successfully activating the downloaded firmware turn the CP off and on again.

   After the CP restarts, an appropriate entry is made in the diagnostics buffer of the CP.

Downloading new firmware via the update center does not affect the LED display.

If downloading new firmware via the update center is interrupted, the procedure can be repeated as often as necessary without restarting the CP.

Downloading with the firmware loader supplied with STEP 7

1. Set the S7ONLINE interface to the "ISO - Industrial Ethernet" protocol.

   It is not possible to download using TCP/IP and therefore not to other networks.
2. Select the firmware to be loaded using the "Browse" button.
3. In STEP 7, select the interface via which you want to download the firmware and set the active MAC address of the connected CP interface.
4. Check the displayed configuration and click the "Download" button.
5. After successfully downloading the firmware, switch the entire rack with the CP off and on again.

   After the CP restarts, an appropriate entry is made in the diagnostics buffer of the CP.

You will find the corresponding LED displays in the section LEDs (Page 43).

If the download is aborted, RUN and STOP flash alternately.

Aborted downloads when using the Firmware Loader

Disturbances or collisions on the network can lead to frames being lost. In such cases, this can lead to an interruption of the firmware download. The firmware loader then signals a timeout or negative response from the module being loaded. An entry is written to the diagnostics buffer.

The CP restarts with the firmware that existed before the aborted download.

Repeat the download using the active MAC address after the CP has started up again.

If you cannot start the download again following an aborted attempt, turn off the entire rack and turn it on again. You can then restart the firmware download.

8.4 Replacing a module

Note

Recommendation to reset address data if the use of the CP is changed

The following data is stored permanently on the CP:

- A configured MAC address
- IP parameters when using DHCP

If the CP has already been operated in your plant and you want to use it at a different location in the plant, it starts up with the permanently configured parameters.

If the CP has been used previously in your plant or has been repaired, delete all stored data by resetting to the factory settings.

8.4.1 Replacing older modules

Distinction

When replacing existing modules with the module described here, the following variants must be distinguished:

- **Replacing a module**

  Describes the situation when an existing module can be replaced with a new module simply by pulling/plugging without changing the configuration.

- **Upgrading**

  (module replacement with compatible functions)

  Describes the situation when the module described here can be used instead of an older module as long as adaptations are made to the configuration. Here, the previously used CP needs to be replaced in the configuration by the new CP.

Unless otherwise specified, the range of functions of the older module continues to be supported.

You can also upgrade modules listed in "Module replacement". This is necessary when new characteristics that were not available in the previously used module are required.

8.4.2 Module replacement / upgrading

Replacing a module

The CP 343-1 Advanced described here (6GK7 343-1GX31-0XE0) can be used as a replacement for the following predecessor products:

- CP 343-1 IT (6GK7 343-1GX11-0XE0) *)
- CP 343-1 IT (6GK7 343-1GX20-0XE0)
- CP 343-1 Advanced (6GK7 343-1GX21-0XE0) **)
- CP 343-1 Advanced (6GK7 343-1GX30-0XE0)
- CP 343-1 (6GK7 343-1EX21-0XE0) **)

*) Note that there is no longer an AUI interface as was available in these device types. To link to an AUI network, use the media converter SCALANCE X101-1 AUI (6GK5 101-1BX00-2AA3).

**) Note the reduced configuration limits in PROFINET CBA for cyclic interconnections (new: 250 bytes maximum).

Table 8- 1 Procedure when replacing a module

Originally configured module	Procedure when replacing a module (configuration unchanged)
6GK7 343-1GX11-0XE0 6GK7 343-1GX20-0XE0 6GK7 343-1GX21-0XE0 6GK7 343-1GX30-0XE0 6GK7 343-1EX21-0XE0	If you do not want to use any function beyond what you had with the previous CP, you do not need to make changes in the configuration. Note the following differences when commissioning: • CP configuration data on the CPU If the option of storing the configuration data of the CP on the CPU was selected for the CPU you are replacing, when the CP starts up the configuration data is loaded automatically from the CPU to the CP. Refer to the information in the section Replacing a module without a programming device (Page 97). • CP configuration data not on the CPU If the configuration data is not stored on the CPU, the following situations must be distinguished: – CP without C-PLUG Download the configuration data again from your PG/PC to the CP. – CP with C-PLUG: CP 343-1 (EX21), CP 343-1 Advanced (GX21/GX30) The configuration data is stored on the C-PLUG. The configuration data can be adopted by swapping the C-PLUG.

Upgrading

The following predecessor products can be upgraded to the CP 343-1 Advanced (6GK7 343-1GX31-0XE0) described here:

- All modules in "Replacing modules"
- CP 343-1 PN (6GK7 343-1HX00-0XE0) *)

*) Note that there is no longer an AUI interface as was available in these device types. To link to an AUI network, use the media converter SCALANCE X101-1 AUI (6GK5 101-1BX00-2AA3).

Table 8- 2 Procedure for upgrading

Originally configured module	Procedure for upgrading (adapted configuration)
6GK7 343-1GX11-0XE0 6GK7 343-1GX20-0XE0 6GK7 343-1GX21-0XE0 6GK7 343-1GX30-0XE0 6GK7 343-1EX21-0XE0	If you want to use the extended options of the new CP, follow the steps below: 1. Replace the previously configured CP with the new module in STEP 7. You will find this in the hardware catalog. 2. Change your configuration according to your requirements. 3. Save, compile and load the configuration data to the CPU or CP again.

Note

When replacing an older module with only one interface with the CP 343-1 Advanced (GX31), the previous port properties are adopted by port 1 of the PROFINET interface of the new CP. Port 2 is set to "Automatic settings". The gigabit interface is deactivated.

Note

Interface in the user program

You should always use the latest block versions for new user programs. You will find information on the current block versions and the current blocks for downloading on the Internet under:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15342/dl)

8.4.3 Replacing a module without a programming device

General procedure

The configuration data of the CP is stored optionally on the CPU or on the C-PLUG of the CP. This makes it possible to replace this module with a module of the same type (identical order number) without a PG.

If you replace in module with a previous module 6GK7 343-1GX21-0XE0, the gigabit interface is disabled.

For information on replacing with previous modules, refer to the information in section Module replacement / upgrading (Page 96).

Note

Reloaded IP access control list

Entries entered later in the IP access control list by HTTP / HTTPS are not saved on the CPU. Both following module replacement and each time the device is turned on or off previously loaded entries must be loaded in the IP access control list again.

Module replacement: Special feature with PROFINET CBA and with IT functions

For PROFINET CBA, interconnection information is stored only on the C-PLUG. The file system for the IT functions is also stored on the C-PLUG. For this reason, you must distinguish the following when replacing in module:

- C-PLUG of the predecessor module is adopted

  In this case, the CBA interconnection information and the data in the file system on the C-PLUG are directly available.

  A diagnostics buffer entry is generated indicating that the C-PLUG originates from a different device type. You can nevertheless continue to use the C-PLUG from the CP 343-1 Advanced (GX21/GX30) in the new CP 343-1 Advanced (GX31).

- A new C-PLUG is being used

  In this case, you will need to download the configuration again with STEP 7 and the CBA interconnection information with SIMATIC iMAP.

Module replacement: Special feature of IP address assignment from a DHCP server

When configuring in STEP 7, you can specify the IP configuration for the CP. One option here is that the CP obtains the IP address of one or both interfaces from a DHCP server.

Note

When replacing modules, please remember that the factoryset MAC address of the new module is different from the previous module. When the factoryset MAC address of the new module is sent to the DHCP server, this will return either a different or possibly no IP address.

Ideally, you should therefore configure IP as follows:

Always configure a client ID if you want to obtain the same IP address from the DHCP server after replacing the module.

If, in exceptional situations, you have configured a new MAC address instead of the MAC address set in the factory, the configured MAC address will always be transferred to the DHCP server and the CP also receives the same IP address as the replaced module.

Technical specifications

9

Table 9- 1 Technical specifications

Technical specifications		
Attachment to Industrial Ethernet		
Amount	1 x gigabit interface 1 x PROFINET interface with 2port switch	
Design of gigabit interface	Connector	1 x RJ-45 jacks
	Transmission rate	10/100/1000 Mbps
Design of PROFINET interface (2port switch)	Connector	2 x RJ-45 jacks
	Transmission rate	10 / 100 Mbps
		When working with PROFINET IO and PROFINET CBA with cyclic transfer, the transmission rate of 100 Mbps full duplex is mandatory.
	Aging time	5 minutes
	Special features of the X2P1R and X2P2R ports	Integration in ring topology / MRP possible
Electrical data		
Power supply	External power supply	24 VDC
	Permitted range	+19.2 V to +28.8 V
	From backplane bus	5 VDC
Current consumption	From external power supply	• 620 mA maximum • 480 mA typical
	From backplane bus	200 mA maximum
Effective power loss	Typical	11.5 W
	Maximum	14.9 W
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally	0 °C to +60 °C
	During operation with the rack installed vertically	0 °C to +40 °C
	During storage	-40 °C to +70 °C
	During transportation	-40 °C to +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Operating altitude	During operation	≤ 2,000 m above sea level at max. 60 °C ambient temperature
Contaminant concentration	Acc. to ISA-S71.04 severity level G1, G2, G3	
Design, dimensions and weight		
Module format	Compact module for S7-300, double width	
Degree of protection	IP20	
Weight	Approx. 450 g	

Technical specifications	
Dimensions (W x H x D)	80 x 125 x 120 mm
Installation options	Mounting in an S7-300 rack
Memory modules	
C-PLUG 32 (6GK1900-0AB00) Ships with the CP	• Memory – Total capacity: 32 MB – Freely capacity available: 30 MB • Number of write cycles: Max. approx. 100 000
C-PLUG 256 (6GK1900-0AB01) Can be ordered separately as an accessory	• Memory – Total capacity: 256 MB – Freely capacity available: 126 MB • Number of write cycles: Max. approx. 200 000
Product functions *	

* You will find the product functions in the section Properties and services (Page 13).

For further data, refer to section Performance data (Page 23)

In addition to this, all the information in the "SIMATIC S7-300 Automation System Module Data" see /18/ (Page 111) in the section "General Technical Specifications" on the topics listed below applies to the CP:

- Electromagnetic compatibility
- Transportation/storage conditions
- Mechanical and climatic environmental conditions
- Information on insulation checks, protection class and degree of protection

Approvals

A

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Approvals for shipbuilding are not printed on the device type plate.

Current approvals on the Internet

You will find the current approvals for the product on the Internet pages of Siemens Industry Online Support at the following link:
(https://support.industry.siemens.com/cs/ww/en/ps/15346/cert)

Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15346/cert)

You can see the current versions of the standards in the relevant certificate, which you will find on the Internet at the address specified above.

Address for declarations of conformity

The EU and the UK declarations of conformity are available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
P.O. Box 48 48
90026 Nuremberg
Germany

EC declaration of conformity

The product meets the requirements and safety objectives of the following EC directives and it complies with the harmonized European standards (EN) for programmable logic controllers which are published in the official documentation of the European Union:

- **2014/34/EU (ATEX explosion protection directive)**

  Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages 309-356

- **2014/30/EU (EMC)**

  EMC directive of the European Parliament and of the Council of 26 February 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, pages 79-106

- **2011/65/EU (RoHS)**

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

- **EU Directive 2014/35/EU**

  Electrical Equipment Designed for Use within Certain Voltage Limits (Low Voltage Equipment Directive)

  Applied standard: EN 61131–2 / IEC 61131–2 (programmable logic controllers, part 2: equipment requirements and verifications)

UK Declaration of Conformity

Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

The product meets the requirements of the following regulations:

- UKEX Regulations

  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments

- EMC Regulations

  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016

- RoHS Regulations

  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012

ATEX / IECEx / UKEX / CCC-Ex

Note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area", which you will find on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013)

The conditions must be met for safe usage of the product according to the section Important notes on using the device (Page 47).

WARNING

Observe installation guidelines

The product meets the requirements if you observe the following during installation and operation:

- The notes in the section Installation and commissioning (Page 47)
- The installation guidelines in the document /18/ (Page 111)

The product meets the explosion protection requirements outlined below.

IECEx

Classification: Ex ec IIC T4 Gc, Certificate no.: IECEx DEK 18.0019X

The product meets the requirements of the standards:

- EN IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

ATEX

Classification: II 3G Ex ec IIC T4 Gc, Certificate no.: DEKRA 18ATEX0027 X

The product meets the requirements of the standards:

- EN IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

UKEX

Classification: Ex ec IIC T4 Gc, Certificate no.: DEKRA 21UKEX0003 X

The product meets the requirements of the standards:

- EN IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

Importer UK: Siemens plc (see above)

CCC

Classification: Ex na IIC T4 Gc, Certificate no.: 2020322310002625

The product meets the requirements of the following standards:

- GB 3836.1

  Hazardous areas - Part 0: Equipment - General requirements

- GB 3836.8

  Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

EMC

The CP meets the requirements of the following directives:

- EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive)
- EMC Regulations SI 2016/1091 The Electromagnetic Compatibility Regulations 2016

Applied standards:

- EN 61000-6-2

  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments

- EN 61000-6-4

  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

RoHS

The CP meets the requirements of the following directives:

- EU directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.
- SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012

Applied standard: EN IEC 63000

cULus Hazardous (Classified) Locations

Underwriters Laboratories Inc.

cULus Listed 7RA9 IND. CONT. EQ. FOR HAZ. LOC.:

- UL 508 (Industrial Control Equipment)
- UL 1604 (Hazardous Location)
- CSA C22.2 No. 142 (Pocess Control Equipment)
- CSA C22.2 No. 213 (Hazardous Location)

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4A; Ta = 0 °C...60 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = 0 °C...60 °C

FM



Factory Mutual Research (FM):
Approval Standard Class Number 3611
APPROVED for Use in:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A; Ta = 0 °C...60 °C
Class I, Zone 2, Group IIC, Temperature Class T4; Ta = 0 °C...60 °C

Notice for Australia (C-TICK)



AS/NZS 2064 (Class A)

Notice for Korea (KCC)

KCC-REM-S49-S7300CP

References

B

Finding the SIMATIC NET documentation

- **Siemens Industry Mall**

  You will find the order numbers for the Siemens products of relevance here in the Siemens Industry Mall:
  Link: (https://mall.industry.siemens.com)

- **Documentation on the Internet**

  You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15247/man)

  Navigate to the desired product group there.

- **Documentation in the STEP 7 V5 installation**

  Manuals that are included in the online documentation of the STEP 7 installation on your PG/PC can be found in the start menu ("Start" > "All Programs" > "Siemens Automation" > "Documentation").

- **Manuals on the data storage medium**

  You will find manuals of SIMATIC NET products on the data storage medium that ships with many products.

  You will find all documentation related to "SIMATIC NET PC Software" on the "SIMATIC NET PC Software" DVD in the folder directory:
  <Installation folder>:\Programs\Siemens\SIMATIC.NET\doc

B.1 On configuring, commissioning and using the CP

/1/

SIMATIC NET
CP 343-1 Advanced
Manual Part B - device manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15346/man)

/2/

SIMATIC NET
S7 CPs for Industrial Ethernet
Configuring and Commissioning - configuration manual
manual Part A - General Applications
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/60053848)

/3/

SIMATIC NET
Version history / current downloads for the SIMATIC NET S7 CPs
History document
Siemens AG
(SIMATIC NET Manual Collection)
On the Internet under following entry ID:
Link: (https://support.industry.siemens.com/cs/ww/en/view/56699406)

/4/

SIMATIC NET
Diagnostics and configuration with SNMP
Diagnostics manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15392/man)

/5/

S7Beans / Applets for IT-CPs
Programming Tips
Siemens AG
24843906 (http://support.automation.siemens.com/WW/view/en/24843906)

B.2 For configuration and programming with STEP 7 / NCM S7

/6/

SIMATIC NET
Industrial Ethernet Security
Security basics and applications
Configuration manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/109747342)

/7/

SIMATIC NET
Commissioning PC Stations - Manual and Quick Start
Configuration Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/77377601)

/8/

SIMATIC NET
Industrial Communication with PG/PC Volume 1 - Basics
System Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/77376110)

SIMATIC NET
Industrial Communication with PG/PC Volume 2- Interfaces
Programming Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/77378184)

/9/

SIMATIC NET
NCM S7 for Industrial Ethernet
Primer
Siemens AG
(part of the online documentation in STEP 7)

/10/

SIMATIC
Configuring Hardware and Connections with STEP 7
Siemens AG
Part of the documentation package "STEP 7 Basic Knowledge"
(Part of the online documentation in STEP 7)

/11/

SIMATIC
Programming with STEP 7
Siemens AG
(Part of the STEP 7 documentation package STEP 7 Basic Knowledge)
(Part of the online documentation in STEP 7)
Link: (http://support.automation.siemens.com/WW/view/de/18652056)

/12/

SIMATIC
System and Standard Functions for S7-300/400
Programming manual
Siemens AG
Link: (http://support.automation.siemens.com/WW/view/de/1214574)

/13/

SIMATIC
Communication with SIMATIC
System Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/25074283)

/14/

Documentation package "STEP 7 Basic Knowledge"

- Working with STEP 7 Getting Started (ID: 18652511)
- Programming with STEP 7 (ID: 18652056)
- Configuring Hardware and Connections with STEP 7 (ID: 18652631)
- From S5 to S7, Converter Manual (ID: 1118413)

Siemens AG
Order number 6ES7 810-4CA08-8AW0

(part of the online documentation in STEP 7)

/15/

Automatisieren mit STEP 7 in AWL und SCL (ISBN: 978-3-89578-280-0) /
Automating with STEP 7 in STL and SCL (ISBN: 978-3-89578-295-4)
User manual, programming manual
Berger, Hans
Publicis KommunikationsAgentur GmbH, GWA, 2006

B.3 On program blocks

/16/

SIMATIC NET
Program blocks for SIMATIC NET S7 CPs
Programming Manual
Siemens AG
(SIMATIC NET Manual Collection)

On the Internet under the following entry ID:
Link: (https://support.industry.siemens.com/cs/ww/en/view/62543517)

/17/

SIMATIC NET
Program blocks for SIMATIC NET S7 CPs
Version history, reference document
Siemens AG
Entry ID: Link: (https://support.industry.siemens.com/cs/ww/en/view/109474421)

B.4 On installing and commissioning the CP

/18/

SIMATIC S7
S7-300 Automation System
Siemens AG

- CPU 31xC and 31x Installation: Operating instructions

  Link: (https://support.industry.siemens.com/cs/ww/en/view/13008499)
- Module Data: Reference manual

  Link: (https://support.industry.siemens.com/cs/ww/en/view/8859629)

B.5 For application and configuration of PROFINET IO

/19/

SIMATIC
PROFINET System Description
System manual
Siemens AG
(SIMATIC NET Manual Collection)
On the Internet under following entry ID:
19292127 (http://support.automation.siemens.com/WW/view/en/19292127)

/20/

SIMATIC
From PROFIBUS DP to PROFINET IO
Programming manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/19289930)

B.6 On setting up and operating an Industrial Ethernet network

/21/

SIMATIC NET
Industrial Ethernet / PROFINET
System manual
Siemens AG

- Volume 1: Industrial Ethernet
- Volume 2: Passive network components

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15248/man)

"System manual" keyword search

B.7 On configuration of PROFINET CBA (components and systems)

/22/

SIMATIC
Component Based Automation - configuring systems with SIMATIC iMap
manual
Siemens AG
18404678 (http://support.automation.siemens.com/WW/view/en/18404678)

/23/

SIMATIC
Component Based Automation - configuring systems with SIMATIC iMap
Siemens AG
22762190 (http://support.automation.siemens.com/WW/view/en/22762190)

You will find more information on SIMATIC iMap on the Internet at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/14366)

Index

A

Abbreviations/acronyms, 4

C

CPUs, released, 37

D

DHCP, 77
Diagnostics buffer entries, 21
Disposal, 8
Documentation, 6

F

FTP services, 5

G

Glossary, 8
GSDML file, 41

I

IP access control list, 98
IRT communication, 26

K

KNOW_HOW_PROTECT, 68

M

MAC address, 6, 95
Modes PROFINET IO, 26

P

Ping, 87
Port 8448, 89
Product names, 4
PROFIenergy, 15

R

Recycling, 8
RT communication, 26

S

Safety notices, 47
Security diagnostics, 89
Service & Support, 8
SIMATIC NET glossary, 8
STEP 7, 4
STEP 7 version, 40

T

Training, 8