SIEMENS

SIMATIC NET

S7-400 - Industrial Ethernet CP 443-1 Advanced

Equipment Manual

Manual Part B

03/2023

C79000-G8976-C256-07

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

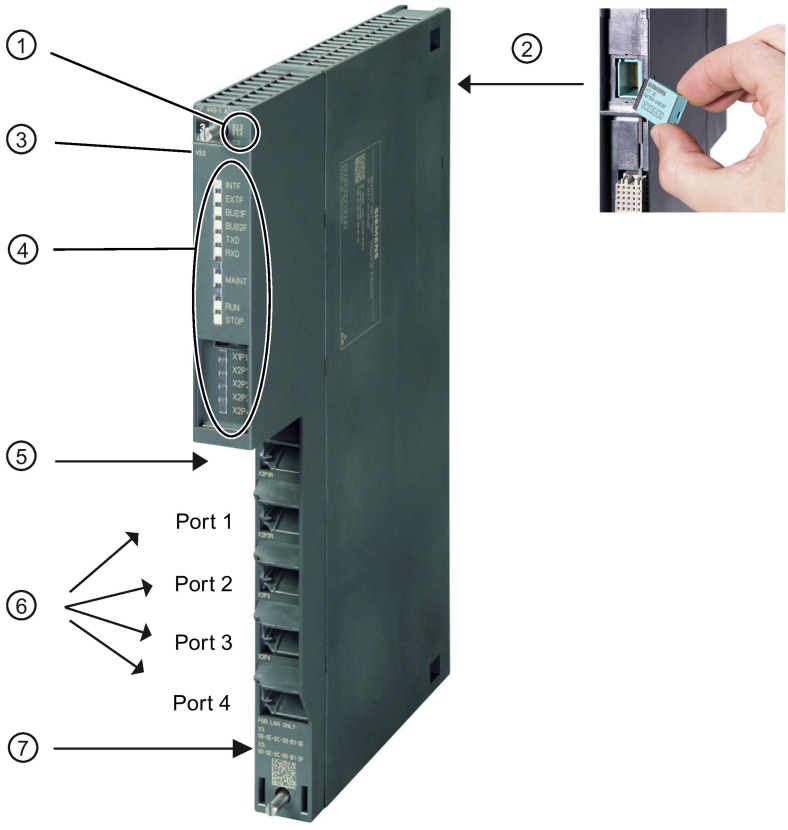
We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C256-07
Ⓟ 03/2023 Subject to change

Copyright © Siemens AG 2012 - 2023.
All rights reserved

Preface



Legend:

1 X = placeholder for hardware product version
2 CPLUG (at rear)
3 Firmware version
4 LEDs
5 Gigabit interface: 1 x 8-pin RJ-45 jack
Security function: The padlock symbol identifies the interface to the external subnet.
6 PROFINET interface: 4 x 8-pin RJ-45 jack
Security function: Interface to the internal, protected subnet
7 Printed text of MAC addresses of the interface

Figure 1 CP 443-1 Advanced

Validity

This description contains information on the following product:

- CP 443-1 Advanced

  Article number 6GK7 443-1GX30-0XE0

Hardware product version 2

Firmware version V3.3

Communications processor for SIMATIC S7-400 / S7-400H

New in this edition

- New functions of the firmware:
  - Read out service data (via the online functions of STEP 7 Professional)
  - Load firmware via the CPU (for future firmware versions)
  - PROFINET CBA and Beans / Applets no longer supported
  - Security fixes
- New approvals (CCC / UKEX)
- Editorial revision

Note the restrictions of the security functions; see security note on firmware below.

Documentation on PROFINET CBA / S7-Beans / Applets

This edition of the manual no longer contains information on PROFINET CBA / S7-Beans / Applets.

If you require information on these topics, please refer to the 06/2021 edition of the manual, which is available on the following Siemens Industry Online Support page:
Link: (https://support.industry.siemens.com/cs/ww/en/view/59187252)

Replaced manual edition

Edition 06/2021

New functions of the firmware V3.2.17:

- H-connections over VPN

Notes on this document

Product names/abbreviations

- CP

  In this document, the term "CP" is also used instead of the full product name CP 443-1 Advanced.

- EX11 / EX41 / GX20 / GX30

  The abbreviations used in this manual for the modules (for example "GX20" or "EX41") correspond to the last four characters of the mid-section of the article number of the respective module.

- STEP 7

  The name STEP 7 is used for the configuration tool instead of the names STEP 7 V5 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 return to the original 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>.

Structure of the documentation

The documentation for this device consists of the following parts:

- Manual Part A: Configuration manual "Configuring and Commissioning S7 CPs for Industrial Ethernet", see /2/ (Page 103).

  Relevant for configuration with STEP 7 V5

- Manual Part B: Manual "CP 443-1 Advanced" (this manual)

- SIMATIC NET Industrial Ethernet Security - Basics and Application, configuration manual, see /11/ (Page 105)

  Relevant for configuration with STEP 7 V5

- Program blocks for SIMATIC NET S7 CPs - programming manual, see /14/ (Page 106)

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

  – Open communications services
  – Access coordination with FETCH/WRITE
  – Connection and system diagnostics
  – FTP services
  – Programmed connections and IP configuration
  – PROFINET

  Relevant for configuration with STEP 7 V5

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 additional 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/15353)

Select the appropriate entry type in the filter settings.

CP documentation on DVD

You can find the documentation on the product and the configuration on the DVD supplied with the product. 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 6 default MAC addresses with the following assignment:

- Gigabit interface
- PROFINET interface
- 1 MAC address for each port of the PROFINET interface

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 address of the relevant interface 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.

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_CP4431_99.pdf

Firmware

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

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Note

The CP contains third-party software components that are no longer supported.

Therefore, Siemens can no longer ensure that the firmware/software does not contain any known security-critical vulnerabilities.

Siemens will provide software updates for the CP until the official end of the software support (date not yet known). This entails examining new vulnerabilities that could also affect the CP, correcting such vulnerabilities and/or providing instructions on how to eliminate or mitigate the vulnerabilities. However, due to possible missing vulnerability information relating to the third-party software that is no longer supported, these measures are incomplete.

For this reason, Siemens recommends the following supplementary measures when using the CP:

- Keep an eye on the Security Advisories that could have effects on the CP
- Always use the latest firmware version of the CP
- Protect additional access to the Internet with suitable additional measures and components, such as SCALANCE S
- Implement a state-of-the-art security concept for your entire network.

You can find additional information on this under:
Link: (https://www.siemens.com/industrialsecurity)

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: (https://www.siemens.com/industrialsecurity)

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

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

SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/view/50305045)

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)

Training, Service & Support

You will find information on training, service and support in the multilanguage document "DC_support_99.pdf" on the Internet pages of Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/en/view/38652101)

Table of contents

Properties and services

1

1.1 Properties of the CP

Application

The CP is intended for use in an S7-400 or S7400H (high availability) automation system. It allows the S7400 / S7400H to be connected to Industrial Ethernet.

For information on the special features of tunneled H-connections, see section H-connections over VPN (Page 78).

Security

Observe the security note on the CP firmware in Preface (Page 3).

The CP has the following interfaces:

- PROFINET interface (Ethernet interface)

  A 4-port switch with IRT capability and with autocrossing, autonegotiation and autosensing is integrated in the CP. The 4-port switch allows the integration of the CP in a bus or a ring with media redundancy.

  Each port of the switch is designed for simple diagnostics and is equipped with a combined RXD/TXD / LINK dual LED. For special situations, each port can also be set to a fixed mode manually using STEP 7, for example 10 or 100 Mbps half duplex / full duplex.

- Gigabit interface with security access

  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 gigabit interface allows a secure connection to external networks via a firewall and VPN. The CP provides the following protective function:

  – Protection of the S7-400 station in which the CP is operated.

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

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).

1.2 Enhanced functions

Compatibility with predecessor modules

The CP 443–1 Advanced (6GK7 443–1GX30–0XE0) with firmware version V3.3 supports all functions of the following predecessor modules:

- 6GK7 443–1GX30–0XE0, Firmware version V3.0 / V3.1 / V3.2
- 6GK7 443–1GX20–0XE0, Firmware version V2.4 / V2.3 / V2.2 / V2.1 / V2.0 / V1.0

For information on replacing modules, read the section Replacing older modules: module replacement / upgrading (Page 84).

Functional expansions of the current firmware version V3.3

- Read out service data (via the online functions of STEP 7 Professional)
- Load firmware via the CPU

You can find details on other firmware versions on the Siemens Industry Online Support pages. Refer to the preface for the link.

Functional expansions of the older firmware versions V2.1 to V3.2

Functions

- Expansion of the block "FTP_CMD" for FTP client operation with the addition of the function "Passive FTP" (client establishes connection) in STEP 7 V5.x. You will find the description in the manual /14/ (Page 106).
- Sending e-mails with STARTTLS, see Characteristics of e-mail mode (Page 26).
- Use of the CP as a purely diagnostics CP via the gigabit interface without networking the PROFINET interface, see Diagnostics options (Page 81).
- Configuration of passive TCP connections between a CP and a redundant partner with the identical number of the local port, see Port configuration with redundant partners (Page 63).
- Expansion of the protection concept of the CP when a protection level of the CPU is activated, see Effects of protection levels (Page 57).
-
- Security functionality
- Advanced Web diagnostics; among other things with the following additional options:
  - Update center for firmware download, updating of the IP access control list and language settings
  - Topology representation
  - Diagnostics of S7 connections
  - Status of the configured security functions
  - Module identification

- PROFINET IO
  - IRT with the option "high performance"
  - Full PROFINET IO diagnostics on the gigabit interface
  - Full PROFINET IO diagnostics on all interfaces also in the expansion rack
- Use in fault-tolerant systems (H systems) is also possible on the gigabit interface.

Expansions on the interface to the user program

- New program block AG_CNTEX for connection and system diagnostics with PING functionality
- Expanded program block FTP_CMD for FTP services allows the establishment of secure SSL connections.

Functional improvements

The overall communication speed of the CP during simultaneous operation of standard communications functions and PROFINET IO controller mode was further improved.

1.3 Communication services

The CP supports the following communication services:

- **PROFINET IO controller**

  PROFINET IO allows direct access to PROFINET IO devices over Industrial Ethernet. PROFINET IO can only be used via the ports of the PROFINET interface.

  - Prioritized startup

    The CP supports prioritized startup. Per PROFINET IO controller, a maximum of 32 PROFINET IO devices can be configured that support prioritized startup. Of these 32 IO devices, simultaneous startup times with values as low as 0.5 s can be achieved by up to 8 IO devices.

  - IRT communication (Isochronous Real Time) with IRT option "high performance"

    IRT communication with the IRT option "high-performance" is possible with PROFINET IO. The IRT option "high-performance" optimizes data traffic as the result of topology planning.

    Note: IRT with the option "high flexibility" is now only supported when a CP GX20 is replaced.

    Note

    IRT communication or MRP

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

  - Shared device

    As a PROFINET IO controller, individual submodules of an IO device can be assigned to the CP. Read the information in /16/ (Page 106) regarding configuration of PROFINET IO systems and shared IO devices.

- **S7 communication with the following functions:**
  - PG functions
  - Operator monitoring and control functions
  - Data exchange over S7 connections
- **Open communication services with the following functions:**
  - SEND/RECEIVE interface over ISO transport connections
  - SEND/RECEIVE interface over TCP connections, ISO-on-TCP and UDP connections

    With the SEND/RECEIVE interface via TCP connections, the CP supports the socket interface to TCP/IP available on practically every end system.

    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 services; corresponding to S5 protocol) via ISO transport connections, ISO-on-TCP connections and TCP connections;

    Here, the SIMATIC S7-400 with the CP is always the server (passive connection establishment) while the read or write access (client function with active connection establishment) is always initiated by a SIMATIC S5 or a third-party device / PC.
  - LOCK/UNLOCK with FETCH/WRITE services (CPU-dependent; see section Requirements for use (Page 31))
- **Open TCP/IP communication**

  Open TCP/IP communication provides a program interface for the transfer of connection-oriented and connectionless services. The establishment and termination of connections is initiated here only via the "dynamic" program interface.

  STEP 7 provides a UDT for the connection description as well as four FBs for data exchange.

  The CP supports communication via ISO-on-TCP connections for this interface.
- **SIMATIC Safety - Fail-safe communication**

  The CP supports fail-safe communication via S7 connections. A fail-safe connection can run from the local CPU via the CP to the relevant communications partner, for example another F-CPU or a fail-safe distributed I/O system.

  You do not need to configure any special safety relevant properties for the CP.
- **IT functions**
  - **HTTP**
  - Web server: Monitoring devices and process data (HTML process control)

– **FTP**

  FTP functions (File Transfer Protocol) for file management and access to data blocks in the CPU (client and server functions)

– **E-mail**

  Sending e-mail via SMTP or ESMTP. The CP supports t SMTP-Auth for authentication on an email server and STARTTLS.

1.4 Further services and characteristics of the CP

- **Security functions**

Note
Restrictions of the security functions

Refer to the notes in Preface (Page 3).

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.

– **SMTPS with STARTTLS**

  Support of SSL/TLS encryption for the secure transfer of e-mails

Note
UDP multicast

UDP multicast via a VPN channel is not supported.

You need to enable the security functions in the configuration.

- **Media redundancy**

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

- **Timeofday synchronization over Industrial Ethernet using the following configurable 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.

- **Addressable with the 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. 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 functions are enabled, the CP supports SNMPv3 for transfer of network analysis information protected from eavesdropping.

- **Module access protection**

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

  For more information, refer to the section Effects of protection levels (Page 57).

- **IP access protection (IPACL)**

  Using IP access protection gives you the opportunity of restricting communication over the CP of the local S7 station to partners with specific IP addresses.

- **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, the subnet mask and the address of a gateway.

  For the PROFINET interface, the IP configuration and the connection configuration can also be assigned to the CP by the user program (program block IP_CONFIG; see /14/ (Page 106)).

  Note: Does not apply to S7 connections.

- **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. From the integrated Download Center, you can download firmware updates.

  The Web pages contain the following information:

  – Module and status information

  – Information on security functions

  – Special information on S7 connections

- **Diagnostics buffer extract request**

  With the aid of a Web browser, the CP supports the option of obtaining an extract of the diagnostics buffer containing the most recent diagnostics events of the CPUs and CPs located in the same S7 station as the CP.

- **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.

- **S5/S7 addressing mode**

  The addressing mode can be configured for FETCH/WRITE access as the S7 or S5 addressing mode (S7 addressing mode only for data blocks / DBs).

- **Detection of double IP addressing in the network**

  To save you timeconsuming troubleshooting in the network, the CP detects double addressing in the network.

  The reaction of the CP when double addressing is detected varies as follows:

  Characteristics of the PROFINET interface

  – CP during startup

    The CP remains in STOP mode.

  – CP in RUN mode

    There is an LED indication (BUS2F LED) and an entry in the diagnostics buffer; the CP remains in RUN mode.

  Characteristics of the gigabit interface

  – CP during startup

    The CP changes to RUN, the BUS1F LED is lit and the CP cannot be reached via the gigabit interface.

  – CP in RUN mode

    There is an LED indication (BUS1F LED) and an entry in the diagnostics buffer; the CP remains in RUN mode.

- **Support in the fault-tolerant system (H system)**

  S7 communication is supported in the H system with the following protocols:

  – ISO transport

  – ISO-on-TCP (RFC1006)

  For details, see section Use in the H system (Page 77).

Performance data

2

Note

Measured values of transfer or reaction times

Measured values of transmission and reaction times in 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)

2.1 General characteristic data

Note that the maximum configuration limits of the CP also depend on the CPU type used.

Characteristic	Explanation / values
Total number of connections on Industrial Ethernet	128 The value applies to the total number of connections of the following types: • S7 connections • SEND/RECEIVE connections • FTP (FTP client) Note: FTP connections occupy 2 TCP connections.

Example

You can, for example, operate the following combination of connections:

- 62 S7 connections or 62 H connections
- 30 ISO-on-TCP connections
- 10 TCP connections
- 10 UDP connections
- 8 ISO transport connections
- 4 FTP connections (for FTP client mode)

  See section Characteristic data for FTP / FTPS mode (Page 27).

2.2 Characteristics of S7 communication

S7 communication provides data transfer via the ISO Transport or ISO-on-TCP protocols.

Characteristic	Explanation / values
Total number of S7 connections on Industrial Ethernet	128 max., of those max. 62 H connections
LAN interface - data field length generated by CP per protocol data unit • sending • receiving	 480 bytes / PDU 480 bytes / PDU
• Number of PG connections • Number of OP connections	2 max. 30 max.

Note

Effects of connections in the SPEED SEND/RECV mode

Note the effects of connections on the SEND/RECEIVE interface that are used in the SPEED SEND/RECEIVE mode.

The maximum configuration limits of S7 communication are reduced by each configured connection using the SPEED SEND/RECV mode.

2.3 SEND/RECEIVE interface

2.3.1 Characteristic data

The SEND/RECEIVE interface provides access to communication over the connection types listed below. The following characteristics are important:

Characteristic	Explanation / values
Number of SEND/RECEIVE connections	• TCP connections: 1...64 * • ISO-on-TCP connections: 1...64 • ISO transport connections: 1...64 • Total number of UDP connections (specified and free) that can be configured: 1 to 64 (of those up to 48 in multicast mode) • E-mail connection: 1 • Max. number of connections (ISO-Transport + ISO-on-TCP + TCP + UDP + Email) total: 64 Refer to the example in the section General characteristic data (Page 21).
Number of SEND/RECV connections in SPEED SEND/RECV mode	The number depends on the CPU type being used. • Per CPU 412/414 maximum 30 • Per CPU 416/417 maximum 62

Characteristic	Explanation / values
Maximum data length for AG_SEND and AG_RECV program blocks	AG_SEND and AG_RECV were shipped with predecessors of the CP and allow the transfer of user data with a length from 1 to 240 bytes. The version of the CP described here continues to support these blocks.
Maximum data length for AG_LSEND and AG_LRECV program blocks	AG_LSEND and AG_LRECV allow the transfer of user data with the following lengths: 1. ISO-on-TCP, TCP, ISO transport: 1 to 8192 bytes 2. UDP: 1 to 2048 bytes 3. E-mail (job header + user data): 1 to 8192 bytes
Maximum data length for AG_SSEND and AG_SRECV program blocks	AG_SSEND and AG_SRECV allow the transfer of user data with the following lengths: 1. ISO-on-TCP, TCP, ISO transport: 1 to 1452 bytes 2. UDP: 1 to 1452 bytes
LAN interface max. data field length generated by CP per protocol data unit	• sending ISO transport, ISOonTCP, TCP: – 400 bytes / TPDU with AG_SEND / AG_LSEND – 1452 bytes / TPDU with AG_SSEND • receiving – ISO transport: 512 bytes / TPDU – ISO-on-TCP: 1452 bytes / TPDU – TCP: 1452 bytes / TPDU

* Notes on TCP connections:

- Avoid receive overload
  The flow control on TCP connections cannot control permanent overload of the recipient. You should therefore make sure that the processing capabilities of a receiving CP are not continuously exceeded by the sender (approximately 150200 messages per second).
- TCP connections for FTP
  Of the available TCP connections, a maximum of 20 TCP connections can be configured / used with the "Use FTP protocol" option; see Characteristic data for FTP / FTPS mode (Page 27).

Restrictions for UDP

- Transfer is not confirmed

  The transmission of UDP frames is unconfirmed, in other words the loss of messages is not detected or displayed by the send blocks (AG_SEND or AG_LSEND).

- No receipt of UDP broadcast

  To avoid overload due to high broadcast load, the CP does not allow reception of UDP broadcasts.

  As an alternative, use the multicast function over a UDP connection. This allows you to register the CP as a node in a multicast group.

- UDP frame buffering

  Length of the frame buffer with buffering enabled:

  2 KB

  Note:

  Following a buffer overflow, newly arriving frames are discarded.

2.3.2 Number of simultaneous SEND/RECEIVE calls

The number of SEND/RECEIVE calls that can be used at the same time is limited both by the CPU and by the CP.

If the maximum number of simultaneous SEND/RECEIVE calls is exceeded, the value 8302H (no receive resources) is indicated in the STATUS of the surplus SEND functions. This can, for example, happen when too many SEND/RECEIVE calls are sent at the same time in OB1.

Limitation by the CPU

In productive operation, the number of SEND/RECEIVE calls that can be used at one time depends on the CPU resources being used. Note the information on the available CPU resources in section System environment (Page 31). The following CPU resources are required:

- Per SEND job short (AG_SEND) or long (AG_LSEND): 1 send resource
- Per RECEIVE job short (AG_RECV): 1 receive resource
- Per RECEIVE job long (AG_LRECV): 1 send resource, 1 receive resource
- Per SPEED SEND/RECV job (AG_SSEND, AG_SRECV): 0 resources

Limitation by the CP

A maximum of 64 SEND/RECEIVE connections can be operated by the CP. At an assignment of 1 CP per CPU, the maximum number of SEND/RECEIVE calls that can be used at one time is limited as follows:

- SEND calls short (AG_SEND):
  CPU 416/417: max. 64 calls per CPU
  CPU 412/414: max. 24 calls per CPU
- SEND calls long (AG_LSEND):
  CPU 416/417: max. 32 calls per CPU
  CPU 412/414: max. 12 calls per CPU
- RECEIVE calls short (AG_RECV):
  CPU 416/417: max. 64 calls per CPU
  CPU 412/414: max. 24 calls per CPU
- RECEIVE calls long (AG_LRECV): variable
  The number of AG_LRECV program blocks that can be used at the same time depends on the number of SEND calls active at the same time (see tables below).

Table 2- 1 Dependency of the maximum number of RECEIVE calls long (AG_LRECV FC60) used at the same time on the number of SEND calls (CPU 412/414)

Number of simultaneous SEND calls	**0**	**1**	**2**	**3, 4**	**5**	**6**	**7**	**8, 9**	**10**	**11**	**12**
Max. number of simultaneous FC60s per CPU 412/414	19	18	17	16	15	14	13	12	11	10	9

Table 2- 2 Dependency of the maximum number of RECEIVE calls long (AG_LRECV FC60) used at the same time on the number of SEND calls (CPU 416/417)

Number of simultaneous SEND calls	**0**	**1**	**2**	**3, 4**	**5**	**6**	**7**	**8, 9**	**10**	**11**	**12**	**13, 14**	**15**	**16**
Max. number of simultaneous FC60s per CPU 416/417/41x-H	51	50	49	48	47	46	45	44	43	42	41	40	39	38
Number of simultaneous SEND calls	**17**	**18, 19**	**20**	**21**	**22**	**23, 24**	**25**	**26**	**27**	**28, 29**	**30**	**31**	**32**	
Max. number of simultaneous FC60s per CPU 416/417/41x-H	37	36	35	34	33	32	31	30	29	28	27	26	25	

The maximum number of SPEED SEND/RECEIVE calls that can be used simultaneously (FC53, FC63) depends only on the CPU (see above).

2.4 Characteristics of open TCP/IP communication

Open TCP/IP communication provides a program interface for the transfer of connection-oriented and connectionless services. The establishment and termination of connections is initiated here only via the "dynamic" program interface.

The CP supports communication via ISO-on-TCP connections for this interface.

Table 2- 3 Open TCP/IP communication

Characteristic	**Explanation / values**
Number of dynamically generated connections over Industrial Ethernet	• ISO-on-TCP connections: 1...64
Max. data length	1452 bytes

2.5 Characteristic data for PROFINET IO

PROFINET IO communication of the CP is IRTcompliant. The CP supports the following maximum configuration as a PROFINET IO controller:

Characteristic	Explanation / values
Number of CPs that can be operated as PROFINET IO controllers within an S7400 station	4
Number of possible PROFINET IO devices *)	128 *), of which • up to 64 in IRT mode • up to 32 in "prioritized startup" mode
Size the input area over all PROFINET IO devices	4 KB max.
Size of the output area over all PROFINET IO devices	4 KB max.
Size of the IO data area per submodule of a module in an IO device • Inputs • Outputs	 • 240 bytes • 240 bytes
Size of the consistency area for a submodule	240 bytes

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

Note

Note the following for PROFINET IO:

If you use modules with ≥ 32 bytes of input/output data, this can lead to I/O access errors; access errors are entered in the diagnostics buffer of the CPU.

These I/O access errors occur during operation only in the "consistent user data" mode and with a low OB1 cycle time.

2.6 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 103).

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 72)

2.7 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 20 FTP connections. Up to 2 TCP connections are occupied per configured FTP connection.

- FTP in server mode:

  You can operate a maximum of 10 FTP sessions at the same time. Up to 2 TCP connections are occupied per FTP session (1 control connection and 1 data connection).

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 72)

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..

2.8 Characteristic data of TCP connections for HTTP / HTTPS

Characteristic data of TCP connections for HTTP / HTTPS

For HTTP access, up to 32 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.

2.9 Memory organization in the CP 4431 Advanced

The data areas of the CP 443-1 Advanced are organized as follows:

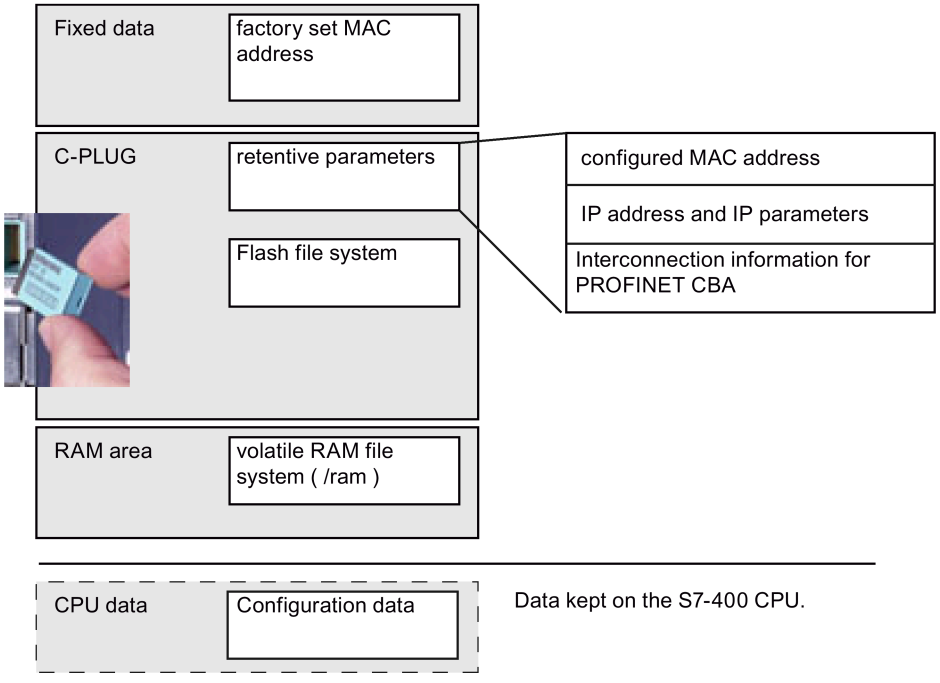


Figure 2-1 Data areas of the CP

Meaning of the memory areas

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

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

  Note

  The flash area of the file system allows a limited number of write cycles (approximately 100 000). 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. This means that all files and folders below this folder are lost when there is a power down.

Note the following configuration limits:

Table 2- 4 Configuration limits

Characteristic	Explanation / values
File names	The length of the file names is limited; the following are permitted: Up to 64 characters for the file name, up to 256 characters for the path. It is possible to make the file name casesensitive in the "Options" tab of the CP properties dialog.
File size	The file size is limited to a maximum of 8 MB.
Memory area for the file system	• Flash area (nonvolatile memory) 30 MB • RAM area (volatile memory) 30 MB

2.10 Characteristic data of the integrated 4port switch

Learning addresses / deleting addresses (aging time)

The switch integrated in the CP 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. The aging time is 5 minutes.

Ports can be deactivated individually

The ports of the switch integrated in the CP 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 (for example X2P1) is then turned off.

Requirements for use 3

3.1 Configuration limits

When using the CP type described here, the following limits apply:

- Number of operable CPs within a rack: 14

  The CP can only be inserted in expansion racks up to number 6.

- Number of CPs operating as PROFINET IO controllers within an S7 station: 4

  The CP cannot be used as PROFINET IO controller in an expansion rack.

Note

Number of CPs that can be operated as PROFINET IO controller

The number of CPs operating as PROFINET IO controllers depends on the number of CP 443-5 Extended modules operating as DP masters in the S7-400 station. A total of 10 CPs can be operated as controllers for the distributed I/O (PROFINET IO controllers or DP masters); of those, however, only up to 4 as PROFINET IO controllers.

Note the following regarding multiprocessor mode: When operating the CP as a PROFINET IO controller, only the process image of the assigned CPU can be distributed via the CP.

3.2 System environment

General requirements

- The CP is released with CPUs as of firmware version V4.1.
  - CPUs with firmware version 4.0 must be upgraded to V4.1.
  - CPUs with firmware version 5.0 must be upgraded to V5.1.
- Open TCP/IP communication is supported by all CPUs as of firmware version V4.1.
- H communication

  Supported with an H-CPU as of firmware version 4.5. For CPUs with firmware version < V6, the CP works as a CPU proxy.
- The full range of functions (MRP, IRT, prioritized startup) is only available with CPUs as of firmware version V5.2.

  For more information about the required version of the STEP 7 configuration tool, refer to section Project engineering (Page 34).

Restrictions for CPUs with older firmware versions

- With CPUs with firmware version V4.1, the CP only has the range of functions of the predecessor module CP 443-1 Advanced (6GK7 443-1EX41-0XE0).
- The use of the program blocks AG_SSEND (FC53) and AG_SRECV (FC63) is only possible with CPUs as of firmware version V5.1.
- With CPUs with firmware versions up to and including V5.1, no PROFINET IO operation is possible.

Table of compatible CPUs

The CP is supported by the S7400 CPUs with the article numbers and firmware versions as shown in the following table.

The table also contains the following information:

- The number of CPs that can be operated with one CPU
- The number of CPU resources for SEND/RECEIVE calls
- CPUs that support the LOCK/UNLOCK function with the FETCH/WRITE services.
- CPUs that support operation of the CP as a PROFINET IO controller.

CPU	Article number of the CPU: 6ES7...	As of CPU firmware version	a = multiprocessor mode b = number of operable CPs c = CPU resources for SEND/RECEIVE jobs [1] d = LOCK/UNLOCK e = PROFINET IO [4]				
			a	b	c	d	e
CPU 412-1	..412-1XF04-0AB0	V4.1	+ [2]	14	24/24	+	-
CPU 412-1	..412-1XJ05-0AB0	V5.1	+ [2]	14	24/24	+	-
		5.2 or higher	+ [2]	14	24/24	+	+
CPU 412-1	..412-1XJ07-0AB0	V7.0	+ [2]	14	24/24	+	+
CPU 412-2	..412-2XG04-0AB0	V4.1	+ [2]	14	24/24	+	-
CPU 412-2	..412-2XJ05-0AB0	V5.1	+ [2]	14	24/24	+	-
		As of V5.2	+ [2]	14	24/24	+	+
CPU 412-2	..412-2XK07-0AB0	V7.0	+ [2]	14	24/24	+	+
CPU 412-2PN	..412-2EK06-0AB0	V6.0	+ [2]	14	24/24	+	+
CPU 412-2PN	..412-2EK07-0AB0	V7.0	+ [2]	14	24/24	+	+
CPU 414-2	..414-2XK05-0AB0	V5.1	+ [2]	14	24/24	+	-
		As of V5.2	+ [2]	14	24/24	+	+
CPU 414-2	..414-2XL07-0AB0	V7.0	+ [2]	14	24/24	+	+
CPU 414-3	..414-3XJ04-0AB0	V4.1	+ [2]	14	24/24	+	-
CPU 414-3	..414-3XM05-0AB0	V5.1	+ [2]	14	24/24	+	-
		As of V5.2	+ [2]	14	24/24	+	+
CPU 414-3	..414-3XM07-0AB0	V7.0	+ [2]	14	24/24	+	+
CPU 414-3 PN/DP	..414-3EM05-0AB0	V5.1	+ [2]	14	24/24	+	-
		As of V5.2	+ [2]	14	24/24	+	+

CPU	Article number of the CPU: 6ES7...	As of CPU firmware version	a = multiprocessor mode b = number of operable CPs c = CPU resources for SEND/RECEIVE jobs [1]) d = LOCK/UNLOCK e = PROFINET IO [4)]				
CPU 414-3 PN/DP	..414-3EM06-0AB0	as of V6.0.2	+ [2)]	14	24/24	+	+
CPU 414-3 PN/DP	..414-3EM07-0AB0	V7.0	+ [2)]	14	24/24	+	+
CPU 414F-3 PN/DP	..414-3FM06-0AB0	as of V6.0.2	+ [2)]	14	24/24	+	+
CPU 414F-3 PN/DP	..414-3FM07-0AB0	V7.0	+ [2)]	14	24/24	+	+
CPU 416-2	..416-2XK04-0AB0	V4.1	+ [2)]	14	64/64	+	-
CPU 416-2	..416-2XN05-0AB0	V5.1	+ [2)]	14	64/64	+	-
		As of V5.2	+ [2)]	14	64/64	+	+
CPU 416-2	..416-2XP07-0AB0	V7.0	+ [2)]	14	64/64	+	+
CPU 416F-2	..416-2FP07-0AB0	V7.0	+ [2)]	14	64/64	+	+
CPU 416-3	..416-3XL04-0AB0	V4.1	+ [2)]	14	64/64	+	-
CPU 416-3	..416-3XR05-0AB0	V5.1	+ [2)]	14	64/64	+	-
		As of V5.2	+ [2)]	14	64/64	+	+
CPU 416-3	..416-3XS07-0AB0	V7.0	+ [2)]	14	64/64	+	+
CPU 416-3 PN/DP	..416-3ER05-0AB0	V5.1	+ [2)]	14	64/64	+	-
		As of V5.2	+ [2)]	14	64/64	+	+
CPU 416-3 PN/DP	..416-3ES06-0AB0	V6.0	+ [2)]	14	64/64	+	+
CPU 416-3 PN/DP	..416-3ES07-0AB0	V7.0	+ [2)]	14	64/64	+	+
CPU 416-3F PN/DP	..416-3FR05-0AB0	V5.1	+ [2)]	14	64/64	+	-
		As of V5.2	+ [2)]	14	64/64	+	+
CPU 416F-3 PN/DP	..416-3FS06-0AB0	as of V6.0.2	+ [2)]	14	64/64	+	+
CPU 416F-3 PN/DP	..416-3FS07-0AB0	V7.0	+ [2)]	14	64/64	+	+
CPU 417-4	..417-4XL04-0AB0	V4.1	+ [2)]	14	64/64	+	-
CPU 417-4	..417-4XT05-0AB0	V5.1	+ [2)]	14	64/64	+	-
		As of V5.2	+ [2)]	14	64/64	+	+
CPU 417-4	..417-4XT07-0AB0	V7.0	+ [2)]	14	64/64	+	+
CPU 412-3H [3)]	..412-3HJ14-0AB0	V4.5	+ [2)]	14	64/64	+	-
CPU 414H [3)]	..414-4HM14-0AB0 ..414-4HR14-0AB0	V4.5	+ [2)]	14	64/64	+	-
CPU 417H [3)]	..417-4HR14-0AB0	V4.5	+ [2)]	14	64/64	+	-
CPU 417-4H [3)]	..417-4HT14-0AB0	V4.5	+ [2)]	14	64/64	+	-
CPU 412-5H [3)]	..412-5HK06-0AB0	V6.0	+ [2)]	14	64/64	+	-
CPU 414-5H [3)]	..414-5HM06-0AB0	V6.0	+ [2)]	14	64/64	+	-
CPU 416-5H PN/DP [3)]	..416-5HS06-0AB0	V6.0	+ [2)]	14	64/64	+	-
CPU 417-5H PN/DP [3)]	..417-5HT06-0AB0	V6.0	+ [2)]	14	64/64	+	-

CPU	Article number of the CPU: 6ES7...	As of CPU firmware version	a = multiprocessor mode b = number of operable CPs c = CPU resources for SEND/RECEIVE jobs [1] d = LOCK/UNLOCK e = PROFINET IO [4]				
CPU 410-5H [3] [5]	..410-5HX08-0AB0	As of V8.0.x	+ [2]	14	64/64	+	-
CPU 410-5H [3] [6]	..410-5HX08-4AB0	As of V10	+ [2]	14	64/64	+	-
CPU 410 SMART [3]	..410-5HN08-0AB0	As of V8.1.x	+ [2]	14	64/64	+	-
CPU 410E [3]	..410-5HM08-0AB0	V8.2	+ [2]	14	64/64	+	-

Legend:

+ → The feature is supported / the specified mode is possible.

- → The feature is not supported / the specified mode is not possible.

1) The calculation of the maximum number of SEND/RECEIVE calls that can be used simultaneously per CP is described in the section "Characteristic data".

2) When operating the CP as a PROFINET IO controller, the multiprocessor mode is not supported, i.e. only the process image of the assigned CPU can be distributed via the CP (note: this has no influence on communications protocols operating at the same time in multiprocessor mode).

3) When operating with H-CPUs with a firmware version lower than V6.0, the SSEND / SRECV mode on the SEND/RECV interface is not supported.

4) The PROFINET IO mode Shared Device requires a CPU as of V5.3.

5) Only for use with PCS 7

6) Only for use with PCS neo

For the maximum possible number of SEND/RECEIVE calls for the CP, refer to the section Number of simultaneous SEND/RECEIVE calls (Page 24).

3.3 Project engineering

Configuration and downloading the 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. You require STEP 7 with additional modules in the following version:

Table 3- 1 Lowest required STEP 7 version

Either STEP 7 V5 or STEP 7 Professional		CP 443-1 Advanced functionality
STEP 7 V5		
	• STEP 7 V5.6 • Security Configuration Tool (SCT) V4.1 *** SCT is used in the configuration of the security function from within STEP 7. • Program block library "SIMATIC NET CP" version V5.5.4 **	The functionality of firmware version V3.1.x can be used.

Either STEP 7 V5 or STEP 7 Professional		CP 443-1 Advanced functionality
	• STEP 7 V5.7 + Service Pack 1 + HF 2 and • HSP 1105 (Hardware Update) *	The functionality described in this document can be used.
STEP 7 Professional		
	STEP 7 Professional V13	The following are not supported: • Innovations of firmware version V3.2
	STEP 7 Professional V15	The functionality of firmware version V3.2 can be used, with the following exception. PROFINET CBA is not supported
	STEP 7 Professional V18 SP1	The functionality described in this document can be used.

* You can find the HSP at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/view/23183356)

** You will find the SCT on the STEP 7 DVD.

*** You can find updates of the program block library at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15353/dl)

3.4 SOFTNET Security Client for VPN tunnels with PCs

SOFTNET Security Client for VPN tunnels with PCs

The operation of VPN tunnels between a SOFTNET Security Client and the CP 443-1 (GX30) has been released as of the following version of the SOFTNET Security Client:

SOFTNET Security Client V4.0 Hotfix 1

3.5 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.

Refer to the documentation of the program blocks in the online help of STEP 7 or in the manual /14/ (Page 106).

Note
Using current block versions

We recommend that you always use the latest block versions for all module types. You will find the current blocks to download from the Internet in Siemens Industry Online Support at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15335/dl)

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

Using program blocks for the SEND/RECEIVE interface

For data transfer on the SEND/RECEIVE interface, there are program blocks for short and long blocks of data.

For fast data transmission up to a data length of 1452 bytes, the SPEED SEND/RECEIVE program blocks AG_SSEND (FC53) and AG_SRECV (FC63) are supported.

Functionality	Requirement
Transfer of data fields <= 240 bytes	• You require the program blocks AG_SEND (FC5) and AG_RECV (FC6) or alternatively the program blocks AG_LSEND (FC50) and AG_ LRECV (FC60).
Transfer of blocks of data > 240 bytes to <= 8192 bytes *)	• You require the program blocks AG_LSEND (FC50) and AG_LRECV (FC60).
Accelerated transfer of blocks of data <= 1452 bytes	• You require the program blocks AG_SSEND (FC53) and AG_SRECV (FC63).

*) The length depends on the protocol

Note
Multicomputing mode

Note that in multicomputing mode, communication using SPEEDSEND/RECV is possible only via the CP assigned to the CPU.

Note
Operation with a high communication load

Note the recommendations in section Recommendation for use with a high communications load (Page 70) for operation with a high communications load.

LEDs

4

LED display

The following LEDs on the front panel show the operating and communication status of the CP:

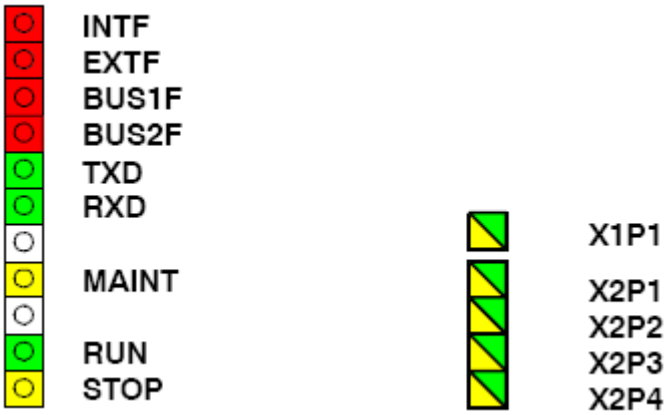


Figure 4-1 LEDs front panel CP 443-1 Advanced

The LEDs have the following meaning:

- INTF: Internal error
- EXTF: External error
- BUS1F: Gigabit interface bus fault
- BUS2F: PROFINET interface bus fault
- TXD: Frame traffic (sending) over Ethernet
  (not relevant for PROFINET IO data)
- RXD: Frame traffic (receiving) over Ethernet
  (not relevant for PROFINET IO data)
- MAINT: Maintenance necessary (diagnostics buffer)
- RUN: RUN mode
- STOP: STOP mode
- X1P1: Link status / activity of the port of the gigabit interface
- X2P1, X2P2, X2P3, X2P4: Link status / activity of PROFINET port 1, 2, 3, 4

Table 4- 1 Legend: Meaning of the LED symbols in the following tables

Symbol				-
Meaning	ON	OFF	Flashing	Any

Table 4- 2 Meaning of the LED displays

INTF (red)	EXTF (red)	BUSxF (red) *)	RUN (green)	STOP (yellow)	MAINT (yellow)	CP operating mode
○	○	○	☼	●	-	Starting up (STOP->RUN)
●	●	●	●	●	●	• Temporary LED pattern during startup (a few seconds) • With permanent LED pattern: Hardware fault in the CP
○	○	○	●	○	-	Running (RUN)
○	○	○	●	☼	-	Stopping (RUN->STOP)
○	○	○	○	●	-	Stopped (STOP) In STOP mode, configuring and performing diagnostics on the CP remain possible.
●	○	○	○	●	-	STOP with internal error or memory reset. (for example IP double addressing detected during startup of the CP in network) The cause can also be a bad C-PLUG (defective, wrong C-PLUG type or not inserted). The following applies in this status: • The CPU or intelligent modules in the rack remain accessible using PG functions (over MPI or the ISO protocol). • SNMP functionality and access over HTTP or FTP are not possible.
-	○	●	-	-	-	• No link (on any port) **) or • Double IP address detected during CP operation.
○	●	☼	●	○	-	RUN with external error; one or more IO devices are not obtainable. (only BUS2F)
○	●	○	●	○	-	• RUN with external error; Diagnostic interrupt from one or more IO devices is pending. IO device diagnostics will provide detailed information. or • Event indication in conjunction with the MRP function; The CP diagnostics buffer contains detailed information.

INTF (red)	EXTF (red)	BUSxF (red) *)	RUN (green)	STOP (yellow)	MAINT (yellow)	CP operating mode
○	○	●	●	○	-	• The gigabit interface is networked in STEP 7 but no Ethernet cable is connected. or • A duplicate IP address was detected after the CP was in RUN. or • Difference in the transmission medium or the duplex settings between the configuration and the actual system
●	●	●	☼	●	○	Loading using the Firmware Loader is active. Note: does not apply to loading via the update center in Web diagnostics.
●	●	●	☼	☼	○	The firmware download was aborted. (STOP LED and RUN LED flash alternately)
●	●	●	●	●	○	Firmware activation after loading using the Firmware Loader is active. (does not apply to loading via the update center in Web diagnostics)
☼	☼	☼	☼	☼	-	Module fault / system error

*) The behavior applies to BUS1F and BUS2F if there is no restriction listed in the "CP mode" column.

**) See also the section Unused PROFINET interface without BUS2F indicator (Page 63).

The "MAINT" LED (yellow)

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.

CP communications status / LED display patterns

LED	Display	Meaning
TXD (green)		CP sending over Ethernet. Note: Sending over PROFINET IO is not signaled here.
RXD (green)		CP is receiving over Ethernet. Note: Receiving over PROFINET IO is not signaled here.
X1P1 X2P1 / X2P2 / X2P3 / X2P4 (green / yellow)		Port has no connection over Ethernet.
		Existing connection over port to Ethernet (LINK status).
		LED flashes yellow (constant light green): Port sending / receiving over Ethernet or PROFINET IO. Note: All received / sent frames are signaled for each specific port including those simply forwarded by the switch.
		Continuous data transfer at the port over Ethernet (on PROFINET ports, for example PROFINET IO).

Module identification with flashing LED (PROFINET interface)

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:

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

- 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.

Installation, connection, commissioning, removal 5

5.1 Important notes on using the device

The following safety notices must be adhered to when setting up and operating the device and during all associated work such as installing, connecting, replacing or removing devices.

5.1.1 Notices on use in hazardous areas

⚠ WARNING

The device may only be operated in an environment with pollution degree 1 or 2 as described in EN/IEC 60664-1, GB/T 16935.1.

⚠ WARNING

EXPLOSION HAZARD

You may only connect or disconnect cables carrying electricity when the power supply is switched off or when the device is in an area without inflammable gas concentrations.

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

⚠ WARNING

Requirements for the cabinet

To comply with EU Directive 2014/34 EU (ATEX 114), UK Regulation SI 2016/1107 or the conditions of IECEx or CCC-Ex, the housing or cabinet must meet the requirements of at least IP54 (according to EN/IEC 60529, GB/T 4208) in compliance with EN IEC/IEC 60079-7, GB 3836.8.

WARNING

Suitable cables at high ambient temperatures in hazardous area

Use heat-resistant cables with an ambient temperature ≥ 60 °C; these cables must be rated for an ambient temperature that is at least 20 °C higher. The cable entries used on the housing must comply with the IP degree of protection required by EN IEC 60079-0 / GB 3836.1.

WARNING

Transient overvoltages

Take measures to prevent transient overvoltages of more than 40% of the rated voltage (or more than 119 V). 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

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.

WARNING

EXPLOSION HAZARD

Replacing components may impair suitability for Class 1, Division 2 or Zone 2.

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.

WARNING

If the device is installed in a cabinet, the inner temperature of the cabinet corresponds to the ambient temperature of the device.

WARNING

EXPLOSION HAZARD

The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

5.2 Installation, removal and repairs in hazardous areas

WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories and original spare parts.
- Observe all relevant installation and safety instructions described in the manuals for the device or supplied with the accessories or spare parts.

WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

- Only use connectors that meet the requirements of the relevant type of protection.
- If necessary, tighten the connector screw connections, device fastening screws, grounding screws, etc. according to the specified torques.
- Close unused cable openings for electrical connections.
- Check the cables for a tight fit after installation.

WARNING

Improper installation of shielded cables

There is a risk of explosion due to equalizing currents between the hazardous area and the non-hazardous area.

- Ground shielded cables that cross hazardous areas at one end only.
- Lay a potential equalization conductor when grounding at both ends.

WARNING

Lack of equipotential bonding

If there is no equipotential bonding in hazardous areas, there is a risk of explosion due to equalizing current or ignition sparks.

- Ensure that equipotential bonding is available for the device.

WARNING

Unprotected cable ends

There is a risk of explosion due to unprotected cable ends in hazardous areas.

- Protect unused cable ends according to IEC/EN 60079-14.

WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

- When connecting intrinsically safe and non-intrinsically safe circuits, ensure that the galvanic isolation is performed properly in compliance with local regulations (e.g. IEC 60079-14).
- Observe the device approvals applicable for your country.

WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.

5.3 Installing and connecting

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

- Before mounting the device, always ensure that there is no visible damage to the device.
- Mount the device using suitable tools. Observe the information in the respective section about mounting.

WARNING

Open equipment

The devices are "open equipment" acc. to the standard IEC 61010-2-201 or UL 61010-2-201 / CSA C22.2 No. 61010-2-201. 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.

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).

If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

Installing and connecting up the CP

The steps for installing and connecting up the CP are explained below.

1. Turn off the power supply when you have configured the CP for PROFINET IO communication.

   Note

   CP as PROFINET IO controller when used with a CPU version < V6.0

   If you operate the CP as a PROFINET IO controller with a CPU version < V6.0, note the following points during installation with respect to the power supply:

   When using the CP in the central rack or in a universal rack operating as central rack, you should not insert or remove the CP when the power is on. If you remove the CP when the power supply is on, the CPU changes to STOP and indicates "I/O error".

   After inserting the module with power applied, it is essential to turn the power supply off and on again.

   Note:

   If the CP is operated without PROFINET IO, it is possible to insert and remove the CP when the power is on without affecting the CPU.

2. Plugging in the CP:
   Fit in the CP onto the rack from the top and push it in at the bottom.

   Note

   Racks / suitable slots in the rack

   - The CP can be plugged into all racks with slots for P and K bus connection.
   - With the exception of the slots reserved for the power supply, the CP can be operated in all slots with a P and K bus connection.
   - When using the universal rack UR1 or UR2 as an expansion rack, a communication bus transceiver is necessary!

3. Secure the CP with screws.
4. Turn on the power supply.
5. Connect the CP to Industrial Ethernet via one of the RJ45 jacks.

   Note

   Operation with security 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 X1P1 to the network after the configuration with security enabled has been loaded.

   You can find connection examples in the general Part A of this manual /2/ (Page 103).

6. Where necessary, connect other components to the remaining free RJ45 jacks.

Result: The CP is installed in the rack and the interfaces have been networked.

Note

Autocrossing mechanism - effects on the connections

For small local area networks or for connecting several Ethernet devices, a 4port switch has been integrated in the CP 443-1 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 59).
- Connecting switches

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

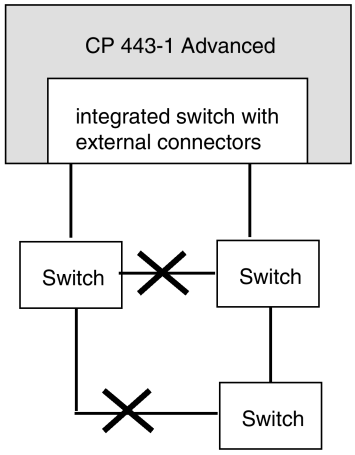


Figure 5-1 Connecting switches (a cross denotes an impermissible connection)

Note

MRP configuration

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

You can find connection examples and MRP setup guidelines in the general Part A of this manual /2/ (Page 103).

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

5.4.1 Commissioning

The steps for commissioning the CP are explained below. Commissioning involves the address assignment and downloading the configuration data and user programs.

Result: The CP is reachable in the network and has been supplied with configuration data.

Follow the steps outlined below:

1. Download the configuration data from your STEP 7 project to the S7-400 station.

   Requirement: You have configured the CP in a STEP 7 project for the properties and services you want to use.

   You can connect the PG when configuring the CP as follows:

   – Via MPI

   – Via Industrial Ethernet

   For further details, refer to the general part /2/ (Page 103) of this manual:

   – For initial addressing (node initialization)

   – For downloading the defined configuration

   The PG / PC requires a LAN attachment, for example via a CP 1613 or CP 1411 and must have the necessary software (for example the S71613 package or SOFTNET IE). The TCP/IP protocol or ISO protocol must be installed. The protocol used must then be applied to the S7ONLINE access point.

2. Use the diagnostics functions during commissioning and to analyze problems.

   You will find an overview of the options in the section Diagnostics options (Page 81).

Note

Module replacement - adapting the cycle load with an older CPU

If you use the CP as a replacement (for example for a CP 443–1 "GX11") with an older CPU, the default communication load setting of 20% for the CPU can lead to overload. In this case, you should set the communication load for the CPU in STEP 7 (parameter "Scan cycle load from communication") to a lower value - for example 10%.

With CPUs as of version V5.1, changing the setting is unnecessary.

5.4.2 CPLUG (configuration plug)

Exchangeable C-PLUG

The CP has an exchangeable configuration plug (CPLUG). This can store up to 32 MB of data in nonvolatile memory.

- The retentive parameters include:
  - IP address and IP parameters
  - Newly set MAC address
  - SNMP variables (modifiable)
- Data in the flash file system; see also Flash area in the section Memory organization in the CP 4431 Advanced (Page 28).

This configuration plug simplifies replacement of modules. By simply exchanging the plug, all the data can be transferred to a replacement device with the same or a higher firmware version, without using a programming device.

Note

Startup

The CP will not start up without a CPLUG!

Area of application

The C-PLUG is an exchangeable medium for storage of the configuration data of the basic device (CP 443-1 Advanced). This means that the configuration data remains available if the basic device is replaced.

How it works

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

Inserting the C-PLUG

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

The C-PLUG is inserted in the compartment.

Figure 5-2 Inserting a C-PLUG

Removing the C-PLUG

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

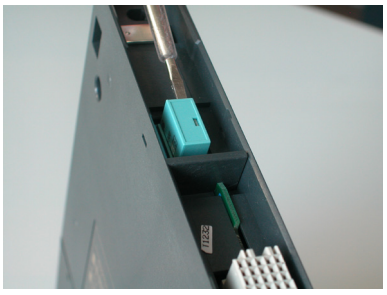


Figure 5-3 Removing the C-PLUG

It is only necessary to remove the C-PLUG if a fault occurs on the CP.

Function

If the C-PLUG has not been written to (factory status), when the device starts up all configuration data of the CP is automatically backed up.

A basic device with an inserted C-PLUG automatically uses the configuration data of the inserted C-PLUG when it starts up. 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 component and inserted in the replacement. As soon as it starts up, the replacement automatically has the same device configuration as the failed device.

Using a CPLUG with old configuration data

Use only C-PLUGs that are formatted for the CP 443-1 Advanced. CPLUGs that have already been used and formatted in other device types must first be formatted for the CP 4431 Advanced.

You do this with STEP 7 / special diagnostics. 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 by the CPU only after reloading or after turning on the power supply again.

Formatting a C-PLUG

Note the restrictions when a protection level is configured for the CPU. See section Effects of protection levels (Page 57) for information on this.

Diagnostics / displays on the device

General malfunctions of the C-PLUG are signaled by the diagnostics mechanisms of the CP (LED display). If you insert a C-PLUG containing the configuration of an incompatible device type, this is also indicated by the LED display. See section LEDs (Page 37)

5.4.3 Controlling the mode

You can change the mode of the CP between RUN and STOP using the STEP 7 configuration software or using STEP 7 special diagnostics.

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").

The reaction is as follows in STOP:

- Established connections (ISO transport, ISOonTCP, TCP, UDP connections) are terminated
- The following the functions are disabled:
  - Time-of-day synchronization
- The following functions remain enabled:
  - The configuration and diagnostics of the CP (system connections for configuration, diagnostics, and PG channel routing are retained);
  - Web diagnostics

5.5 Disassembly

⚠ WARNING

Improper disassembly

Improper disassembly may result in a risk of explosion in hazardous areas.

For proper disassembly, observe the following:

- Before starting work, ensure that the electricity is switched off.
- Secure remaining connections so that no damage can occur as a result of disassembly if the system is accidentally started up.

Configuration and operation

6

6.1 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 the Siemens Web pages regularly for the latest information.
  - 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 connection

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 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

Also note the ports for configured and programmed connections. See section 5.6, item 5.7 in the configuration manual /2/ (Page 103).

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)

6.2 Controlling the mode

You can change the mode of the CP between RUN and STOP using the STEP 7 configuration software or using STEP 7 special diagnostics.

Note the restrictions when a protection level is configured for the CPU. See section Effects of protection levels (Page 57) for information on this.

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").

The reaction is as follows in STOP:

- Established connections (ISO transport, ISOonTCP, TCP, UDP connections) are terminated.
- The following the functions are disabled:
  - Time-of-day synchronization
  - PROFINET IO
- The following functions remain enabled:
  - The configuration and diagnostics of the CP (system connections for configuration, diagnostics, and PG channel routing are retained).
  - Web diagnostics
  - FTP / FTPS access to the file system
  - HTTP / HTTPS access
  - Routing function

6.3 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 via PST / SINEC PNI.

- **Formatting the C-PLUG**

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

  Set the CPU to STOP to perform this action.

- **Resetting / memory reset**

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

  Set the CPU to STOP to perform this action.

- **Downloading configuration data to the CP (EX11, GX11)**

  The following restriction applies only to a CP 343-1 Advanced (GX30) that is configured as CP "EX11" or "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.

6.4 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 Project engineering (Page 34).

The following information on configuration applies to both configuration tools.

6.5 Interface configuration

6.5.1 Network settings

6.5.1.1 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.

6.5.1.2 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 section Transmission speed of the gigabit interface (Page 61).

The configuration of the network settings "Transmission medium / duplex" is made for both interfaces in the properties of the port of the relevant interface in the "Port parameters" parameter group:

- Row "X1P1": Port properties of the gigabit interface
- Row "X2P1/2/3/4": Properties of port 1, 2, 3 or 4 of the PROFINET interface

Automatic setting or individual network settings

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

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 and disable the autonegotiation option, the automatic negotiation of the network settings (autonegotiation) is no longer effective.

If, on the other hand, the communications partner works with autonegotiation, it is not certain that communication will be established.

Autocrossing mechanism

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

Note

Manual configuration

If you have set a port to manual configuration and select the "Disable autonegotiation" option, the autocrossing mechanism is also disabled for this port. The port then behaves like the interface of a switch. In this case, the following applies:

- Connecting an end device

  To connect an end device that does not have the autocrossing mechanism (for example CP 4431 with article number 6GK7 443-1EX11-0XE0), do not use a crossover cable.
- Connecting a switch

  To connect a switch, that does not support the autocrossing mechanism, use a crossover cable.

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 diagnostics buffer using 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:

- 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.

- Forcing a specific mode instead of "Automatic settings"

  If your application requires a specific mode instead of the automatic settings, you will need to match up the partner devices.

- No reaction to Autonegotiation query with manual configuration

  Remember that if you configure the CP manually and the "Autonegotiation" option is disabled, it will not react to an autonegotiation query! As a result, a connected partner may not be able to set the required mode and communication will not be ideal.

  Example:
  If the CP is set to "100 Mbps - full duplex" and autonegotiation is disabled, a CP connected as partner will set "100 Mbps - half duplex". Reason: Due to the fixed setting, an autonegotiation reply is not possible. Although the connected partner detects 100 Mbps with autosensing, it remains at half duplex.

- Recommendation: Change individual network settings only over MPI

  If you modify the LAN settings in the properties dialog of the CP in the "Options" tab using the "Transmission medium/Duplex" drop-down list, these changes will be adopted by the CP and activated when the configuration data is downloaded to the target system (STEP 7). 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 settings" are now changed to 100 Mbps full duplex, the download cannot be completed.

6.5.1.3 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 "1 Gbps full duplex" or with "Automatic settings". If the connection partner does not support gigabit Ethernet, the data will be transferred at the next lower speed (100 or 10 Mbps).

6.5.2 IP configuration and DHCP

6.5.2.1 S7 connections and DHCP

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.

6.5.2.2 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). This also applies to the default router.

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 57) for information on this.

6.5.2.3 Restart after detection of a duplicate IP address in the network

To save you timeconsuming troubleshooting in the network, the CP detects double addressing in the network.

Behavior during operation (CP in RUN)

If the CP detects double addressing on the network (new node with an IP address that has already been assigned), a message is generated in the diagnostics buffer and the bus fault LED lights up.

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

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

Behavior when the CP starts up

If duplicate addressing is detected when the CP starts up, the CP remains in STOP. The bus fault LED is lit and a diagnostics buffer entry is generated. The CP only starts up after the duplicate addressing problem has been eliminated.

6.5.3 Unused PROFINET interface without BUS2F indicator

BUS2F display for a PROFINET interface that is not connected

If no cable is connected to any port of the PROFINET interface, with a networked PROFINET interface in the configuration this causes the "BUS2F" LED to light up.

If none of the ports should be used and the lighting up of the “BUS2F” LED is unwanted, delete the networking of the PROFINET interface in the configuration.

6.5.4 Using 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 the STEP 7 interface configuration.

Note

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

6.6 Port configuration with redundant partners

Using the same port number with redundant partners

As of firmware version V3.2 of the CP, when configuring passive TCP connections between the CP and a redundant partner, you can configure the local port number of the CP identically twice.

This is, for example, necessary if the partner is a redundant IEC master.

6.7 PROFINET IO mode

6.7.1 How PROFINET IO devices start up in a large configuration

When operating the module with a large configuration (up to 128 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 parameter assignment monitoring time must be increased on the CPU.

Possible remedies: Reduce the size of the configuration (for example, distribution on several CPs).

6.7.2 Reduce the communication allocation reserved for PROFINET IO when operating alongside other services.

If cyclic data exchange over PROFINET IO is operating at the same time on the same Ethernet subnet, set the communications allocation for PROFINET IO in the properties dialog of the PROFINET IO system to a value <100%.

Reason: At the (default) setting 100%, the communication time is reserved primarily for PROFINET IO data exchange. Reducing the communications allocation for PROFINET IO increases the systemwide update time for PROFINET IO and creates additional time on the CP for processing other communication services.

6.7.3 Prioritized startup in PROFINET IO

Functions

If you use RT or IRT communication, the CP supports the PROFINET functionality "prioritized startup" for PROFINET IO devices that also support this function. A maximum of 32 PROFINET IO devices can be configured per I/O controller. With these IO devices, simultaneous startup times with values as low as 0.5 s can be achieved for a maximum of 8 devices.

Prioritized startup is used in fast processes when IO devices change quickly, for example fast tool changes with a robot.

There is a significant improvement in speed even in the following situations:

- Applications that generally require a fast start-up time for the IO devices after turning on the power or following station failure/station return.
- When activating PROFINET IO devices.

Note

Longer start-up times despite prioritized startup

In the following situations, start-up times of up to 8 s may be experienced despite prioritized startup:

- A PROFINET IO device is disconnected and reconnected within 8 s.
- At a docking point, several physical PROFINET IO devices are docked as one IO device with one specific device name and one specific IP configuration (for example at a docking point for a driverless transport system).

Configuration for IO devices

You configure prioritized startup for the IO devices configured in the PROFINET IO system. In STEP 7 select the properties of the PROFINET interfaces for the relevant IO devices.

Prioritized startup requires fixed port settings.

You will find further information on this in the system descriptions of PROFINET IO /16/ (Page 106) /17/ (Page 106).

Note

Changing the configuration - behavior on startup

After changing the configuration of an IO device to prioritized startup, the time required for the first startup is just as long as without prioritized startup. All subsequent startups will then be completed in the reduced time.

Note

Inclusion in the MRP ring topology impractical

Including an IO device with prioritized startup in a ring topology with media redundancy serves no practical purpose since the ring is interrupted at each device change.

6.7.4 IRT communication: Types of synchronization

Within an IRT domain (Isochronous Real Time), 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.

The IRT option "high flexibility" is now only supported when a CP GX20 is replaced.

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.

6.7.5 Operating PROFINET IO devices with a current firmware version

Using current firmware versions

For the PROFINET IO devices listed below, you should use the current firmware versions to operate the CP.

- IM151-3PN with article number 6ES7151-3AA20-0AB0
- IM151-3PN with article number 6ES7151-3BA20-0AB0

You will find the current firmware versions on the Internet at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/14081/dl)

6.7.6 Shared device - using the router address

Shared devices allow more than one PROFINET IO controller to access different submodules of the same PROFINET IO device.

CP as PROFINET IO controller with shared device

The information below applies if all the following requirements are met:

- The CP is used as a PROFINET IO controller with an assigned shared device.
- No router is configured on the PROFINET interface.
- The gigabit interface of the CP is networked.

Problem / behavior

In this case, the shared device is automatically assigned the IP address of the PROFINET interface of the CP as the router address.

This assignment leads to a conflict when other IO controllers assigned to the shared device use other router addresses or no router address.

Remedy

The IO device being used as a shared device will only take part in data exchange if the higher-level I/O controllers are configured identically in terms of using routers.

You should therefore configure the PROFINET interfaces on the other IO controllers as follows:

- The IP address of the PROFINET interface of the CP is used as the router address.

  or

- The CP being used as the IO controller and all other IO controllers use the same IP address as the router address.

6.8 Media redundancy

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

For more detailed information on configuration, refer to the online help of the "Media redundancy" parameter group and in Part A of the manual /2/ (Page 103).

Note

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

6.9 Interface in the user program

6.9.1 Call interface for open communications services SEND/RECV

Change call parameters only after job confirmation

Note

Note the following for the call interface of the program blocks AG_SEND / AG_LSEND / AG_SSEND or AG_RECV / AG_LRECV / AG_SRECV:

Once the job has been triggered, you can only make changes again after the program block has confirmed completion of the job with DONE=1 or with ERROR=1.

If this is ignored, it is possible that the execution of the job will be aborted with an error and resources could be permanently occupied on the CPU.

6.9.2 Programmed communication connections with IP_CONFIG

Downloading the configuration using FB55

FB55 allows programcontrolled transfer of the configuration data.

Note

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

Special features / restriction

Simultaneous operation of configured and programmed connections is not possible. As soon as an IP address is set via the FB55, all configured connections are removed.

Note

No use of IP_CONFIG (FB55) when operating the CP with fault-tolerant S7 connections.

If you configure fault-tolerant S7 connections via the CP, you cannot use program block IP_CONFIG (FB55) for IP configuration of the CP.

You will find further information on special features and use in fault-tolerant systems in the section on program-controlled IP configuration in /14/ (Page 106)/.

6.9.3 IP access protection with programmed communications 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 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 security is enabled are described in the general part of this manual /2/ (Page 103).

6.9.4 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.

6.9.5 Open TCP/IP communication

Use

To allow the user program to exchange data with other TCP/IPcompliant communication partners, STEP 7 provides a UDT for the connection parameter assignment and four program blocks (FBs):

- UDT 65 "TCON_PAR" with the data structure for connection parameter assignment
- FB65 "TCON" for connection establishment
- FB66 "TDISCON" for connection termination
- FB63 "TSEND" for sending data
- FB64 "TRCV" for receiving data

TCP/IP communication is connectionoriented. Data can be transmitted only when a connection has been established to the communications partner. The CPU can use several connections to a communications partner at the same time.

The following protocol variants are supported:

- ISO on TCP according to RFC 1006

Parameterization

Make the following parameter settings in the connection description (UDT 65):

- local_tsap_id: Byte 1 = 0xE0 (value mandatory for correct functionality)
- local_tsap_id: Byte 2 = rack/slot number
- remote_tsap_id: Byte 1 = 0xE0 (value mandatory for correct functionality)
- remote_tsap_id: Byte 2 = rack/slot number

Note: The TSAPs can be 2-16 bytes long. The first two bytes must be occupied as described, you can use the other bytes to suit your task.

Note

Note that the number of dynamically established connections also depends on the number of configured, statically established connections.

You will receive corresponding condition codes on the call interface of the FBs.

Refer to the documentation of the program blocks in the online help and in the documentation for STEP 7. You will also find examples of parameter assignment there.

6.9.6 Recommendation for use with a high communications load

Reason

When using the CP described here, the points below will help you to avoid overload situations on your CPU.

In particular when you replace an older CP with the CP described here and are then confronted with overload problems, you should check your application for the pitfalls outlined below.

Known problems

- The program blocks for sending and receiving AG_SEND / AG_RECV (FC5/FC6, FC50/60 or FC53/63) are often called cyclically in OB1. This leads to constant communication between the CPU and CP. As a result, other types of communication such as PG functions cannot be executed or only very slowly.
- HMI systems access data of the CPU too often using S7 functions. This slows down communication in general and resource bottlenecks on the CPU can occur if SEND/RECEIVE FCs are called cyclically in OB1 (effect: reduced data throughput or increased reaction time).

Remedy

Note the following recommendations:

- Do not call communication program blocks cyclically in OB1!

  Communication should be called timecontrolled in a suitable cyclicinterrupt OB. The call interval of this OB should be significantly higher than the average cycle time of OB1.
- You should set a minimum cycle time that is higher than the average runtime of OB1. This frees resources for communication on the CPU. This is, for example, a solution for existing applications when communication already takes place cyclically in OB1.
- If necessary, reduce the time taken for communication processing on the CPU by changing the parameter "Scan cycle load from communication" in the properties of the CPU.

6.10 Security

Note

Restrictions of the security functions

Refer to the notes in Preface (Page 3).

6.10.1 Settings for online security diagnostics and downloading to station with the firewall activated

Note

Additional services for online security diagnostics and download

If you wish to use the "Online security diagnostics" or "Download to device" functions, you need to create additional rules or disable the "Echo Request" / "Echo Reply" services.

Setting the firewall for online functions

With the security functions enabled, follow the steps outlined below.

Global security functions:

1. Select the entry "Firewall > Services > Define services for IP rules".
2. Select the "ICMP" tab.
3. Insert a new entry of the type "Echo Reply" and another of the type "Echo Request".

Local security functions of the CP:

Now select the CP in the S7 station.

1. Enable the advanced firewall mode in the local security settings of the CP in the "Security > Firewall" parameter group.
2. Open the "IP rules" parameter group.
3. In the table, insert a new IP rule for the previously created global services as follows:
   - Action: Accept; From:: External; To: Station; Service > ICMPv4/6 service > Echo Request (the previously globally created service)
   - Action: Accept; From:: Station; To: External; Service > ICMPv4/6 service > Echo Reply (the previously globally created service)
4. For the IP rule for the "Echo Request" service, enter the IP address of the engineering station under "Source IP address".

With these rules, the CP can only be reached from the engineering station with ICMP packets (ping) via the firewall.

6.10.2 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.

6.10.3 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.

6.10.4 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.

6.10.5 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).

6.10.6 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.

6.11 Time-of-day synchronization

General rules

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

- SIMATIC mode
- NTP / NTP (secure)

  The secure method NTP (secure) uses authentication with symmetrical keys according to the hash algorithms MD5 or SHA-1. The method NTP (secure) can only be selected if the security functions are enabled.

  – STEP 7 Professional

    In the global Security settings of the STEP 7 project, you can create and manage additional NTP servers also of the type NTP (secure).

  – STEP 7 V5

    In the extended NTP configuration, you can create and manage additional NTP servers including those of the type NTP (secure).

Note

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

If an NTP frame is detected by the CP as "not exact", the time-of-day frame is not forwarded on the K bus. This can occur with time-of-day frames from non-synchronized NTP servers with stratum 16. In this case, none of the NTP servers is displayed as "NTP master" in the diagnostics; but rather only as being "reachable".

Note

Ensuring a valid time of day

If you have enabled the security functions, 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).

Project engineering

For more detailed information on configuration, refer to the online help of the "Time-of-day synchronization" parameter group and in the manual /2/ (Page 103).

6.12 SNMP

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).

Supported MIBs

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

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

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

    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

The "Interfaces" MIB object provides status information on the CP interfaces, with the following assignment:

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 6- 1 ifIndex

ifIndex	Type of interface
1 *)	Gigabit interface
2-5 (1-4) *)	Port 1-4 (PROFINET interface)
6 (5) *)	Internal CP interface

*) If the gigabit interface is not configured, the value 1 is assigned to the first port of the PROFINET interface; the next values then move accordingly by one position.

Access permissions using community name

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

Table 6- 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 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.

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

Further information

You will find further information in the manual /6/ (Page 104).

6.13 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.

A ping simply serves to check reachability. There is therefore no need to support extremely long ICMP packets.

6.14 Use in the H system

S7 connections as H connections via ISO-on-TCP - adapting the monitoring time

When using the CP in the H system V4.5, you also have the option of creating fault-tolerant S7 connections via ISO-on-TCP. When operating large numbers of connections via the CP, it may be necessary to increase the monitoring time. Otherwise it is possible that some connections cannot be established.

Depending on the firmware version of the CPU you are using, set the monitoring time with the following method:

- H CPU with firmware as of V6.0

  The setting is made in the properties parameters of the configured connection.

- H CPU with firmware < V6.0

  The setting is made in the properties parameters of the CP.

6.15 H-connections over VPN

Scope of services

The CP does not support operation of fault-tolerant S7 connections (H-connections) within a VPN tunnel.

A maximum of 10 fault-tolerant S7 connections are supported per CP.

Restrictions

The following restrictions apply to operation:

- Due to the additional load through the VPN, a lower transmission speed over the H-connection must be expected.
- When operating large numbers of connections via the CP, it may be necessary to increase the monitoring time of the H-connections.

  With monitoring times that are too short, it is possible that some connections cannot be established or that breakdowns occur during operation.

  You are recommended to set the monitoring time to at least one second.

  Depending on the number of VPN groups, number of H-connections and the communication load, it may be necessary to increase the monitoring times further.
- An H-connection can only be established after the VPN group is created.
- The first connection establishment of an H-connection via VPN takes longer than without VPN tunneling.
- If you use a CP for H-connection via VPN, it cannot operate any of the following services in parallel:
  - S7 communication
  - SEND/RECV communication (TCP, ISO-on-TCP, UDP or ISO)
- Only the H-connections operated with the CP itself can be established within the VPN tunnel.

  No other SEND/RECV communication (TCP, ISOonTCP, UDP, ...) can run over the VPN tunnel, even over routing.
- The operation of H-connections over VPN with SCALANCE S / SCALANCE SC as VPN connection endpoint is not released.

When using the CP in SIMATIC PCS 7, observe the restrictions and guidelines for PCS 7.

Requirements

- Software versions:
  - STEP 7 as of version V5.6
  - Security Configuration Tool (SCT) as of Version V5.0
- S7-400H CPU firmware
  - H-CPU with firmware as of V4.5: V4.5.7
  - H CPU with firmware as of V6.0: V6.0.8
  - CPU 410-5H with firmware as of V8.0: V8.2.1
- CP firmware
  - CP 443-1 Advanced: As of firmware version V3.2.17
- The firmware versions of the modules within an H-station must be identical for the respective module type.

  You are recommended to operate all CPs within a VPN group with identical firmware.
- To establish the VPN connections correctly, all VPN nodes need the current time.

  Make sure that time synchronization is enabled for all nodes and that the same time source is used, if possible.

Configuration

General

- Configure the nodes of VPN groups in such a way that each sub-connection and each connection path of an H-connection can be established over the VPN.
- You are recommended to create a logical network in NetPro for each physical network.
- Create a VPN group with all required nodes for each logical network.
- Multiple H-connections can communicate through the same VPN group.

Rules for configuring the VPN groups

The following conditions apply:

- A maximum of 10 VPN groups are permissible per CP.
- The mode of authentication of the VPN group must be certificate-based.

  Pre-shared key-based authentication is not permissible.
- The VPN group must be configured in IKE mode "Main".

  IKE mode "Aggressive" is not permissible.
- For key exchange, use only "DH group 14" or "DH group 15".
- In Phase 1 during encryption, use only AES-256 with SHA1 authentication.
- In Phase 2 during encryption, use only AES-128 with SHA1 authentication.

- "Perfect Forward Secrecy" can be enabled.
- All nodes of a VPN group must be able to reach one another.

  If you insert modules that are connected to different physical networks in a VPN group, the VPN group cannot be successfully established.

Possible VPN groups

- With H-connections via 2 paths with a physical network, at least one VPN group is required.

  Alternatively, 2 VPN groups can be used.
- With H-connections via 2 paths with 2 physically separated networks, 2 VPN groups are required.
- With H-connections via 4 paths with a physical network, at least one VPN group is required.

  Alternatively, 2 or 4 VPN groups can be used.
- With H-connections via 4 paths with 2 physically separated networks, at least 2 VPN groups are required.

  Alternatively, 4 VPN groups can be used.
- With H-connections via 4 paths with 4 physically separated networks, 4 VPN groups are required.

Configuration of the H-connection

- The H-connection can only be configured via the X1 interface (GBIT) of the CP.
- For fault-tolerant S7 connection, only the ISO-on-TCP type can be used.

  The ISO type must not be used.

Diagnostics and upkeep 7

7.1 Diagnostics

7.1.1 Diagnostics options

Overview of the Diagnostics options

The following diagnostics options are available:

- **LEDs of the module**

  For information on the LED displays, refer to the section LEDs (Page 37).

- **Web diagnostics**

  For information on Web diagnostics using HTTP, refer to the section The CP as Web server (Page 82).

- **STEP 7 V5.5**
  - Hardware diagnostics and troubleshooting
  - Communication diagnostics with special diagnostics

- **STEP 7 Professional**

  In the "Diagnostics" tab in the Inspector window, you will see the following information:
  - Entries in the diagnostics buffer of the CPU
  - Information on the online status

  In the "Online > Online and diagnostics" menu, you obtain the static information about the module:
  - General information on the module
  - Diagnostics status
  - Information on the interfaces
  - Information relating to special diagnostics (folder "Functions" > Special diagnostics)

  You will find further information on the diagnostics functions of STEP 7 in the STEP 7 information system.

- **Security-Online diagnostics**

  Using this special diagnostics that can be called up from SCT or STEP 7, you will obtain detailed information about the Security functions of the CP.,

Using the CP as an intermediary for diagnostics data

If you only want to use the CP as an intermediary for diagnostics data of the station, as of firmware version 3.2 you can network only the gigabit interface and, for example, establish a VPN tunnel to a PC via this interface. The PROFINET interface does not need to be networked.

7.1.2 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.

For more information, refer to section Settings for online security diagnostics and downloading to station with the firewall activated (Page 71).

7.2 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 + PROFINET IO) always has a higher priority than data exchange with the Web browser. This can lead to delays in the HTML process control in the Web browser.

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 103).

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.

For detailed information on the Web server and Web diagnostics, refer to the general Part A of this manual /2/ (Page 103)

Web browser

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

- Chrome
- Firefox

Use a browser version that is up-to-date at the time of publication of this manual.

7.3 Maintenance

⚠ CAUTION

Hot surfaces

Risk of burns during maintenance work on parts with a surface temperature above 70 °C (158 °F).

- Take appropriate protective measures, for example, wear protective gloves.
- Once maintenance work is complete, restore the touch protection measures.

⚠ 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.

7.3.1 Replacing older modules: module replacement / upgrading

Distinction

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

- Replacing a device

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

  Note the information in section Installing and connecting (Page 44) on plugging and pulling the module. This applies in particular if you operate the CP as a PROFINET IO controller.

- 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.

Note

The modules CP 443-1 EX30 and CP 443-1 Advanced GX30 cannot be used as spares to replace each other (see below). You can, however, upgrade the EX30 with a GX30 if you change the configuration.

Replacing a device

The CP described here with the current firmware version can be used as a replacement for the following predecessor products, with the exception of the PROFINET CBA, Beans and Applets functions:

- CP 443-1 Advanced 6GK7 443-1GX20-0XE0
- CP 443 1 Advanced (6GK7 443-1EX41-0XE0) with CPUs as of firmware version 4.1
- CP 443-1 IT (6GK7 443-1GX11-0XE0) with CPUs as of firmware version 4.1

CPUs with firmware version 4.0 must be upgraded to 4.1.

When replacing modules with CPUs with a firmware version lower than V4.0, the 6GK7 443-1GX11-0XE0 or 6GK7 443-1EX41-0XE0 must continue to be ordered.

Note the other information in this section relating to the predecessor modules listed here.

Upgrading

The following predecessor products can be upgraded to the CP 443-1 Advanced (6GK7 443-1GX30-0XE0) described here:

- CP 443-1 (6GK7 443-1EX20-0XE0)
- CP 443-1 Advanced (6GK7 443-1EX40-0XE0)

Module replacement with a CP 443-1 Advanced (GX20 / EX40 / EX41)

Note the following procedure when replacing an older module (GX20, EX40 or EX41) with the new module (GX30):

Step 1: Replacing the CP

1. Remove the module to be replaced from the rack.
2. Take the C-PLUG from the removed module and insert it in the new module.
3. Insert the new module with the C-PLUG from the removed module in the rack.
4. Note the following points and, in the case of the EX40, continue at step 2 as described below.

Note

It is not necessary to turn the power supply off and on.

You should note the following restrictions:

- If OB83 is not loaded, the CPU changes to STOP.
- In PROFINET IO mode and when operating with a CPU < V6.0, you will need to cycle power.

Note

The C-PLUG removed from the old module has the internal identifier "GX20", "EX40" or "EX41"; this does not, however, affect the operation of the new CP (GX30).

If you do not, however, want to keep this identifier, you will either have to use the C-PLUG supplied with the new module or reformat the C-PLUG of the old module. You will then, however, have to provide the CP with its original IP address (node initialization).

Step 2: Adapting the configuration (upgrading an EX40)

1. In the STEP 7 configuration, replace the already configured CP with the new module; You will find this in the hardware catalog.
2. As soon as you drag the new module from the catalog onto the module you are replacing, the configured connections and data are adopted.
3. If necessary, modify the configuration according to your requirements, for example in the Properties dialog for the Ethernet subnet.
4. Save and compile the project.
5. Download the configuration data to the target system again.

Note

If you have been operating an EX40 with PROFINET communication, the EX40 can only be replaced with a GX30 if you are using a CPU as of firmware version 5.2 (see section System environment (Page 31)). In this case, you may need to adapt the configuration.

7.3.2 Replacing older modules: CPs with configurable data management

Other older modules (GX11) can be replaced in different ways depending on the type of data management:

Data management on the CPU: Replacing a device

Here, it is not necessary to adapt or download the configuration data; the new module behaves identically in every way to the replaced module.

This variant is only possible if the originally used CP was configured for data maintenance on the CPU (option "Module replacement without PG"). Follow the steps below:

1. Remove the module to be replaced from the rack.
2. Insert the new module in the rack.

Data management on the CP: Module replacement with download

The module must be supplied with the existing or adapted configuration data.

These variants are necessary when the originally used CP was configured without the option "Module replacement without PG", in other words, with data management on the CP.

- **Variant A:** Adapting the STEP 7 project (preferred solution)

  If you adopt the configuration data unchanged and therefore leave the data management on the CP, do not use the option of data storage protected from power down with the new CP. For this reason, we recommend that whenever possible you adapt the existing configuration to the new CP type:

1. Replace the old module with the new module in the rack.
2. In STEP 7, replace the already configured CP with the new module; You will find this in the hardware catalog.

   As soon as you take the new module from the catalog in HW Config and drag it to the module you are replacing, the configured connections and data are adopted.

   The mode is then automatically configured as "data management on the CPU".
3. Save and compile the project.
4. Download the configuration data to the target system again.

- **Variant B**: STEP 7 project unchanged

  If you do not want to use any of the new features, you can replace the module as follows without any further configuration:

1. Remove the module to be replaced from the rack.
2. Insert the new module in the rack.
3. Download the configuration data from the PG/PC to the new module.

Result

After downloading the configuration, the CP changes to RUN.

The following table shows you which of the options described above are available with the module types that were available up to now. Note the description of the possible procedures above.

Table 7- 1 Behavior of the module following module replacement

Module used up to now	Data management (configurable)		Characteristics / notes
	CP	CPU	
6GK7 443-1GX11-0XE0	X	X	Module replacement is possible; procedure depending on selected data management on the predecessor module. • Retentivity of data management on the CP: IP address retained after cycling power; this makes downloading and diagnostics possible using the existing IP address. • The IT functionality available on the new CP corresponds to the range of functions of the predecessor module. If you want to use the new IT functions of the GX30, you will need to change the configuration with the necessary STEP 7 version.

7.3.3 Replacing a module without a programming device

General procedure

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

Note

Configured MAC address is adopted

When setting the ISO protocol, remember that MAC address set previously during configuration is transferred by the CPU to the new CP module.

Note

Reloaded IP access control list

Entries entered later in the IP access control list by HTTP / HTTPS are not saved on the CPU. After a module has been replaced, previous entries that had been entered later must be reloaded in the IP access control list.

For information on replacing previous modules, refer to the information in section Diagnostics and upkeep (Page 81).

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

When configuring in the Properties dialog, you can specify the IP configuration of the CP. One option here is that the CP obtains the IP address from a DHCP server.

Note

Recommendation: Configuring a client ID

When replacing modules, 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 no IP address.

If, after replacing a module, you want to make sure that the CP always receives the same IP address from the DHCP server, follow the steps below when creating the IP configuration:

- Always configure a client ID for the CP in the DHCP configuration and configure your DHCP server accordingly.

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. In this case, the new CP also has the same IP address as the previous CP.

7.3.4 Loading new firmware

Options for a firmware update

You can use the following alternative methods to download a new firmware file to the CP:

- The firmware loader supplied with STEP 7 V5

  Requirement for downloading:

  – 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!

- The update center of the Web server

  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.

Note the descriptions of firmware downloads in the manual Part A /2/ (Page 103).

Note

Security functions enabled:

If the Security functions are enabled for modules, a protection level is automatically configured that prevents loading a new firmware file with 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 anyway, the CPU and the CP must be in STOP mode.

How to download new firmware

You can download the firmware via both interfaces of the CP.

Note

Operation with CPU version < V6.0

Remember that the CPU with version < V6.0 changes to STOP during downloading of the firmware if you are using PROFINET IO communication.

Follow the steps outlined below:

1. Connect the CP module to the PG/PC via a LAN cable.
2. Start the download on your PG/PC using one of the firmware download functions described above.

   You can find the corresponding LED displays in the section LEDs (Page 37). Downloading new firmware via the update center does not affect the LED display.

   The download involves two stages:

   – Section 1: Downloading firmware

   – Section 2: Activating firmware
3. After the firmware download, the CP goes through a warm restart.

If the download using the firmware loader is aborted, the RUN and STOP LEDs flash alternately.

What to do if a download is interrupted

Disturbances or collisions on the network can lead to packets 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. En entry is made in 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, you should turn off the entire rack and turn it on again. You can then restart the firmware download.

7.3.5 Memory reset / reset to factory defaults

The CP has a two-level function available for resetting:

- Memory reset
- Resetting to factory setting

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 obtain the configuration data that was previously on the CP (with parameters, connections, IP address).

Note

Memory reset - ACL (access control list) / firewall / VPN configuration

After a memory reset on the module, the following applies:

- ACL or firewall configurations remain active.
- The VPN configuration is deleted.

  Effect: After a memory reset, the module can no longer be reached via a VPN tunnel.

Note

Memory reset - PROFINET IO is being used

If you run a memory reset a CPU as of version 5.2, the CP memory is also reset if you are using PROFINET IO.

Note the restrictions when a protection level is configured for the CPU. See section Effects of protection levels (Page 57) for information on this.

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 -> 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 with "Online" > "Online & Diagnostics" > "Functions" > "Reset to Factory Settings"

Clear/reset module - effects

After resetting memory, the CP retains the configured MAC address, the IP address and the retentive parameters (for information on the retentive parameters, refer to section CPLUG (configuration plug) (Page 49)). The CP is therefore immediately ready for downloads using the IP address.

The configuration data is retained on the CPU.

The CPU in the S7 station does not recognize that the CP memory was reset. The CP changes to the "stopped with error" state (see section LEDs (Page 37)). The configuration data must then be reloaded. You can also initiate this loading by cycling power (OFF > ON).

This has the following overall effect:

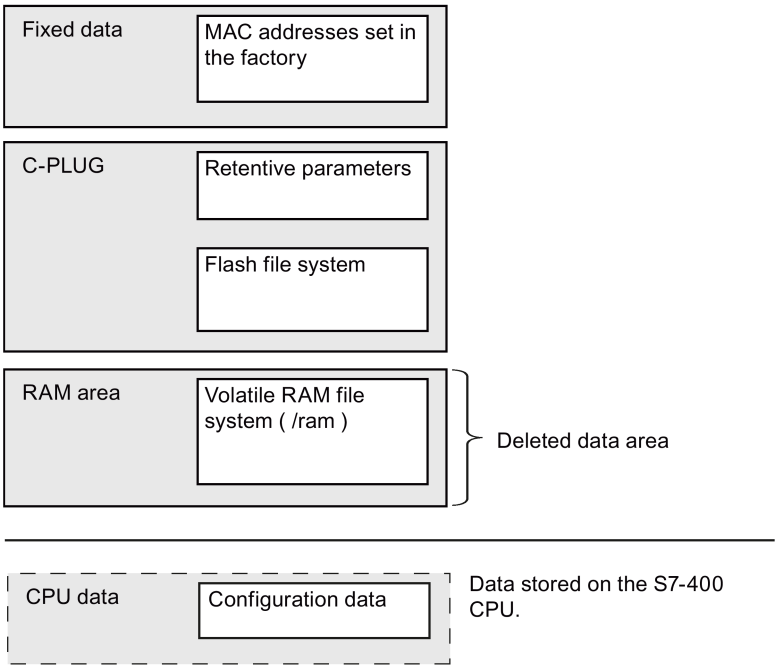


Figure 7-1 Memory following a memory reset

Reset to factory defaults - effects

After resetting to factory defaults, the CP always retains the factory set MAC address (as supplied).

The IP address and the configuration data in the CP RAM are deleted. The configuration data is retained on the CPU.

The data in the file system of the CPLUG (flash area) is retained, the retentive parameters are deleted.

This has the following overall effect:

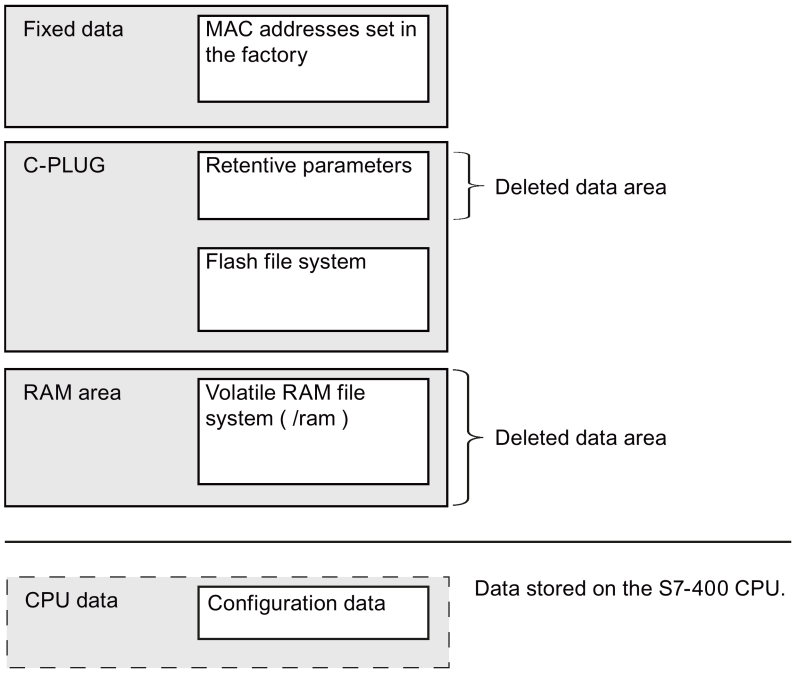


Figure 7-2 Memory after Reset to Factory Settings

Security configuration data when running a memory reset in STEP 7 V5.5

The behavior of the configuration data for the security functions when memory is reset depends on the STEP 7 version used for the reset.

- STEP 7 V5.5 SP2
  - Memory reset with STEP 7 special diagnostics:

    The security configuration is deleted during the memory reset.
  - Memory reset with the SIMATIC Manager:

    The security configuration is retained during the memory reset.
- STEP 7 V5.5 SP3

  The retentive security configuration is retained during the memory reset.

Technical specifications

8

Table 8- 1 Technical specifications of the CP 443-1 Advanced

Technical specifications		
Article number	6GK7443-1GX30-0XE0	
Connection to Industrial Ethernet		
Quantity	1 x gigabit interface 1 x PROFINET interface with 4port switch	
Design of gigabit interface	Connector	1 x RJ-45 jacks
	Transmission speed	10/100/1000 Mbps
Design of PROFINET interface (4port switch)	Connector	4 x RJ-45 jacks
	Transmission speed	10/100 Mbps
		When working with PROFINET IO and cyclic transmission, the transmission speed of 100 Mbps full duplex is mandatory.
	Aging time (4port switch)	5 minutes
	Special features of the X2P1R and X2P2R ports	Integration in ring topology / MRP possible
Permitted cable lengths (Ethernet)	**(Alternative combinations per length range) ***	
0 ... 55 m	• Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180 • Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet	
0 ... 85 m	• Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180 • Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet	
0 ... 100 m	• Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180 • Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet	
Electrical data		
Power supply	via S7 backplane bus	5 V
Current consumption	From backplane bus	1.8 A
	Power dissipation	7.25 W
Permissible ambient conditions		
Ambient temperature	During operation	0 °C to +60 °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	≤ 2,000 m above sea level	
Contaminant concentration	Acc. to ISA-S71.04 severity level G1, G2, G3	

Technical specifications	
Design, dimensions and weight	
Module format	Compact module for S7-400, single width
Degree of protection	IP20
Weight	Approx. 700 g
Dimensions (W x H x D)	25 x 290 x 210 mm
Installation options	Mounting in an S7-400 rack
Memory modules	
C-PLUG 32 (6GK1900-0AB00)	Ships with the CP
Memory capacity	• Total capacity: 32 MB • Free capacity available: 30 MB
Number of write cycles	Max. approx. 100 000
Product functions **	

***** For details, refer to the IK PI catalog, cabling technology.
****** You will find the product functions in the section Properties and services (Page 13).

For further data, refer to section Performance data (Page 21)

In addition to this, all the information in the S7400/M7400 reference manual "Module Data" /7/ (Page 104) 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

9

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.

Approval for CP and C-PLUG

The following approvals apply to the CP and the supplied C-PLUG.

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/15353/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

EU declaration of conformity

CE

The CP meets the requirements and safety objectives of the following EU 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

UK Declaration of Conformity

UK CA

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 CP according to the section Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 41).

The product meets the explosion protection requirements outlined below.

IECEx

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

The product meets the requirements of the standards:

- IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- IEC 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-Ex

Classification: Ex ec IIC T4 Gc

The product meets the requirements of the following standards:

- GB 3836.1

  Hazardous areas - Part 0: Equipment - General requirements
- GB 3836.3

  Explosive atmospheres - Part 3: Equipment protection by increased safety "e"

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

c(UL)us

Applied standards:

- Underwriters Laboratories, Inc.: UL 508 Listed (Industrial Control Equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

Applied standards:

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4
- Cl. 1, Zone 2, GP. IIC T4

Ta: Refer to the temperature class on the type plate of the CP.

Report / UL file: E223122 (NRAG, NRAG7)

Note the conditions for the safe deployment of the CP according to the section Notes on use in hazardous areas according to UL HazLoc / FM (Page 42).

FM

Factory Mutual Approval Standard Class Number 3600, 3611, 3810

Class I, Division 2, Group A, B, C, D, T4 or Class I, Zone 2, Group IIC, T4

Ta: Refer to the temperature class on the type plate of the CP.

Certificate of Compliance: 3030463

Australia - RCM

The CP meets the requirements of the AS/NZS 2064 standards (Class A).

Notice for Canada

This class A digital device meets the requirements of the Canadian standard ICES-003.

AVIS CANADIEN

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Marking for the customs union

EAC (Eurasian Conformity)

Customs union of Russia, Belarus and Kazakhstan

Declaration of the conformity according to the technical regulations of the customs union (TR CU)

MSIP 요구사항 - For Korea only

Certification Number: MSIP-REM-S49-S7400CP

A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Current approvals

SIMATIC NET products are regularly submitted to the relevant authorities and approval centers for approvals relating to specific markets and applications.

If you require a list of the current approvals for individual devices, consult your Siemens contact or check the Internet pages of Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15351/cert)

Documentation references

A

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").

- **Documentation on the data storage medium**

  You will find some of the documentation for the "SIMATIC NET PC Software" products directly on the data storage medium or, after installation, in the folder "%ProgramFiles%\Siemens\SIMATIC.NET\doc".

A.1 For configuring, installing, commissioning and using the CP

/1/

SIMATIC NET
CP 443-1 Advanced (GX30)
Manual Part B - device manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/59187252)

/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
Link: (https://support.industry.siemens.com/cs/ww/en/view/56699406)

/4/

SIMATIC
S7 F/FH Systems - Configuring and Programming
programming manual and user's guide
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/109773062)

/6/

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

/7/

SIMATIC S7
Automation System S7-400, M7-400
Siemens AG

- Installation: Installation manual
  Link: (https://support.industry.siemens.com/cs/ww/en/view/1117849)
- Module Data: Reference Manual
  Link: (https://support.industry.siemens.com/cs/ww/en/view/19539653)
- CPU data: Device Manual
  Link: (https://support.industry.siemens.com/cs/ww/en/view/53385241)

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

/8/

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)
Link: (https://support.industry.siemens.com/cs/ww/en/view/109751824)

/9/

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: (https://support.industry.siemens.com/cs/ww/en/view/18652056)

/10/

SIMATIC
System and Standard Functions for S7-300/400 - Volume 1/2
Reference manual
Siemens AG
(Part of the STEP 7 documentation package STEP 7 Basic Knowledge)
(Part of the online documentation in STEP 7)
Link: (https://support.industry.siemens.com/cs/ww/en/view/1214574)

/11/

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

/12/

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

/13/

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)

A.3 On program blocks

/14/

SIMATIC NET
Program blocks for SIMATIC NET S7 CPs
Programming Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/62543517)

/15/

SIMATIC NET
Version history of the SIMATIC NET program blocks for S7 CPs
Reference manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/109474421)

A.4 For application and configuration of PROFINET IO

/16/

SIMATIC
PROFINET system description
System manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/13715/man)

/17/

SIMATIC
From PROFIBUS DP to PROFINET IO
Programming manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/19289930)

A.5 On setting up and operating an Industrial Ethernet network

/20/

SIMATIC NET
Industrial Ethernet
System manual
Siemens AG

- Volume 1: Industrial Ethernet

  Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465)
- Volume 2: Passive network components

  Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

Index