SIEMENS

SIMATIC NET

S7-400 - Industrial Ethernet CP 443-1 EX31

Equipment Manual

Preface

Properties and services 1

Performance data 2

Requirements for use 3

LEDs, QR-Code 4

Installation, wiring, commissioning, removal 5

Configuration and operation 6

Diagnostics and upkeep 7

Technical specifications 8

Certification 9

Documentation references A

Manual Part B

05/2025
C79000-G8976-C755-01

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 Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

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

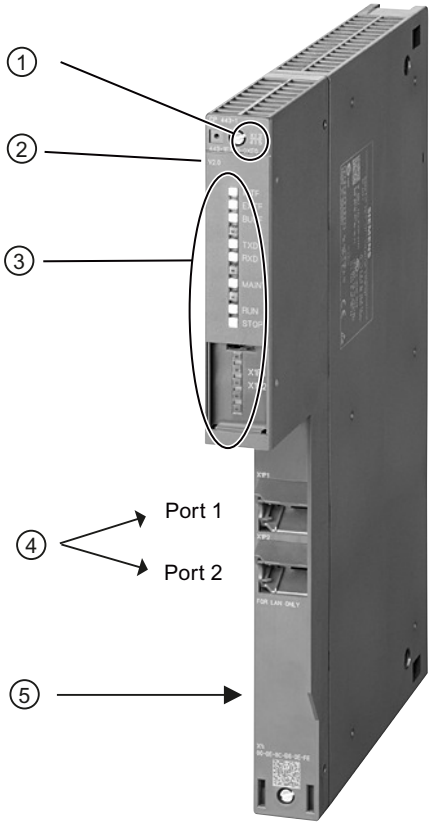
Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C755-01
Ⓟ 05/2025 Subject to change

Copyright © Siemens 2025.
All rights reserved

Preface

Product notes



Legend:

1 X = placeholder for hardware product version
2 Firmware version
3 LEDs
4 PROFINET interface: 2 x 8-pin RJ-45 jack
5 Label with MAC address

Figure 1 CP 443-1 EX31

Validity and product names

This description contains information on the following product:

- CP 443-1 EX31
  Article number 6GK7 443-1EX31-0XE0

Hardware product version 1

Firmware version V4.0

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

Structure of the documentation

The documentation for this device consists of the following parts:

- Manual Part A: Configuration manual "Configuring and Commissioning S7CPs for Industrial Ethernet", see references Documentation references (Page 81).
- Manual Part B: "CP 443-1 EX31" Equipment Manual (this document)
- Program blocks for SIMATIC NET S7 CPs - programming manual, see references Documentation references (Page 81)
  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

Current version of the manual and FAQs 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/15352)

Select the appropriate entry type in the filter settings.

CP/CM 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.

Compatibility with previous versions - service and maintenance

Note

Read the information regarding extended functions and restrictions in section Enhanced functions (Page 13) of this manual!

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.
- EX11 / EX30 / EX31 / EX41
  The abbreviations used in this manual for the modules (for example "EX30" 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>.

Address label: Unique MAC address preset for the CP

The CP is supplied with total of 3 default MAC addresses with the following assignment:

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

The MAC address of the PROFINET interface is printed on the housing.

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

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

Information can be accessed via QR code

There is a QR code on the device via which you can call up a web page relating to the device which provides a great deal of information. Refer to section QR code (Page 36) for more on this.

License conditions

Note

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

Cybersecurity information

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry (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 customer's exposure to cyber threats.

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

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.

Device defective

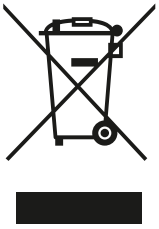
If a fault develops, please send the device to your Siemens representative for repair. Repairs on-site are not possible.

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 products are low in pollutants, can be recycled and meet the requirements of the WEEE directive 2012/19/EU for the disposal of electrical and electronic equipment.

Do not dispose of the products 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 (Product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Note the different national regulations.

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)

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:
Link: (https://support.industry.siemens.com/cs/de/en/)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option submitting a support query:
  Link: (https://support.industry.siemens.com/cs/my?lc=en-WW)
- Our service offer:
  Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:
Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (https://new.siemens.com/global/en/products/services/industry/sitrain/personal.html)

Industrial Networks Education

Training and certification for Industrial Networks

In our Industrial Networks Education courses you'll learn to design and implement wired and wireless data networks and connect them to a corporate network. You will also receive instruction on how to secure, diagnose and optimize communication networks. Certification can also be offered to supplement almost all training courses.

Link: (https://www.siemens.com/industrial-networks-education)

Table of contents

Preface ... **3**

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

1.1 Properties of the CP ... 13

1.2 Enhanced functions ... 13

1.3 Communication services ... 14

1.4 Further services and characteristics of the CP ... 15

2 Performance data ... **19**

2.1 General characteristic data ... 19

2.2 Characteristics of S7 communication ... 20

2.3 SEND/RECEIVE interface ... 21

2.3.1 Characteristic data ... 21

2.3.2 Number of simultaneous SEND/RECEIVE calls ... 22

2.4 Characteristics of open TCP/IP communication ... 23

2.5 Characteristic data for PROFINET IO ... 24

2.6 Characteristic data of TCP connections for HTTPS ... 24

2.7 Characteristic data of the integrated 2port switch ... 24

2.8 Encryption methods (Ciphers) used by the module ... 25

3 Requirements for use ... **27**

3.1 Configuration limits ... 27

3.2 System environment ... 27

3.3 Project engineering ... 29

3.4 Program blocks ... 30

4 LEDs, QR-Code ... **33**

4.1 Condition codes ... 33

4.2 QR code ... 36

5 Installation, wiring, commissioning, removal ... **39**

5.1 Important notes on using the device ... 39

5.1.1 Notices on use in hazardous areas ... 39

5.1.2 Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex ... 40

5.1.3 Notes on use in hazardous areas according to UL HazLoc and FM ... 40

5.2 Installation, removal and repairs in hazardous areas ... 41

5.3 Installing and connecting ... 43

5.4 Commissioning ... 46

5.4.1 Commissioning - procedure ... 46
5.4.2 Controlling the mode ... 47
5.5 Disassembly ... 47
6 Configuration and operation ... 49
6.1 Security recommendations ... 49
6.2 Controlling the mode ... 52
6.3 Recommendation for use with a high communications load ... 53
6.4 Effects of protection levels ... 54
6.5 Configuration in STEP 7 ... 55
6.6 Interface configuration ... 55
6.6.1 Fast Ethernet ... 55
6.6.2 IP configuration ... 57
6.6.2.1 Points to note about IP configuration ... 57
6.6.2.2 Restart after detection of a duplicate IP address in the network ... 57
6.6.3 Port configuration with redundant partners ... 58
6.7 PROFINET IO mode ... 58
6.7.1 How PROFINET IO devices start up in a large configuration ... 58
6.7.2 Reduce the communication allocation reserved for PROFINET IO when operating alongside other services ... 58
6.7.3 Prioritized startup in PROFINET IO ... 59
6.7.4 IRT communication: Types of synchronization ... 60
6.8 Media redundancy ... 60
6.9 Interface in the user program ... 60
6.9.1 Call interface for open communications services SEND/RECV ... 60
6.9.2 Programmed communication connections with IP_CONFIG ... 61
6.9.3 IP access protection with programmed communications connections ... 61
6.9.4 Programmed communications connections - assigning parameters to the ports ... 62
6.9.5 Open TCP/IP communication ... 62
6.10 Time-of-day synchronization ... 63
6.11 SNMP agent ... 63
6.12 Ping: Permitted length of ICMP packets ... 66
6.13 Use in the H system ... 66
7 Diagnostics and upkeep ... 67
7.1 Diagnostics options ... 67
7.2 The CP as Web server ... 68
7.3 Replacing older modules ... 69
7.4 Loading new firmware ... 70
7.5 Memory reset / reset to factory defaults ... 71
8 Technical specifications ... 73
8.1 Resistance to harmful gases according to ISA-71.04 ... 74

9 Certification 75
A Documentation references 81
Index 87

Properties and services

1

1.1 Properties of the CP

Application

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

The CP has the following interfaces:

- PROFINET interface (Ethernet interface)
  A 2-port switch with IRT capability and with autocrossing, autonegotiation and autosensing is integrated in the CP. The 2-port switch allows the integration of the CP in a bus or a ring with media redundancy.
  Each port 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 manually using STEP 7. The following options are possible:
  - Automatic
  - Disabled
  - 100 Mbps full duplex

1.2 Enhanced functions

Compatibility with predecessor modules

The CP 443–1 EX31 (6GK7 443–1EX31–0XE0) with firmware version V4.0 is compatible with the following predecessor modules apart from the unsupported transmission speed 10 Mbps and the IRT High flexibility function:

- 6GK7 443–1EX30–0XE0, Firmware version V3.0 / V3.1 / V3.2 / V3.3
- 6GK7 443–1EX20–0XE0, 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 (Page 69)

Note

The CP 443–1 EX31 (6GK7 443–1EX31–0XE0) has a coated circuit board and is suitable for ambient temperatures up to 70 °C. The CP 443–1 EX31 is the replacement for the following predecessor modules:

- CP 443–1 EX30 (6GK7 443-1EX30-0XE0)
- CP 443–1 EX30 with coated circuit board (6GK7 443-1EX30-0XE1)

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.
  - 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.
    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 Documentation references (Page 81) 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 S7400 with the CP is always the server (passive connection establishment) while the fetch or write access (client function with active connection establishment) is always initiated by a SIMATIC S5 or a device from another range / PC.
  - LOCK/UNLOCK with FETCH/WRITE services (CPU-dependent; see section Requirements for use (Page 27))
- **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 parameter assignment as well as four FBs for high-speed data exchange.
  The CP supports communication via ISO-on-TCP connections for this interface.

1.4 Further services and characteristics of the CP

- **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.

- **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.
- **Module access protection**
  To protect the module from accidental or unauthorized access, protection can be configured at various levels.
- **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, you can configure how and with which method the CP is assigned the IP address, the subnet mask and the address of a gateway.
  The IP configuration and the connection configuration can also be assigned to the CP by the user program (program block IP_CONFIG; see Documentation references (Page 81)).
  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
  - Special information on S7 connections

  If you do not require this function, you can disable it in the STEP 7 configuration and disable the port ("IP access protection").
- **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:
  - CP during startup
    The CP remains in STOP mode.
  - CP in RUN mode
    There is an LED indication (BUSF 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)

Performance data

2

Note

Measurements of transmission and reaction times in Ethernet, PROFIBUS and PROFINET networks for a series of configurations can be found on the Internet under entry ID:

25209605 (http://support.automation.siemens.com/WW/view/en/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

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
- 16 ISO transport connections

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	Maximum 4 Maximum 30

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 TCP, ISO-on-TCP, ISO transport and UDP connections. The following characteristics are important:

Characteristic	Explanation / values
Number of SEND/RECEIVE connections	• TCP connections: 1...64 [1)] • 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) • Max. number of connections in total: Max. 64 (ISO transport + ISO-on-TCP + TCP + UDP) Refer to the example in the section General characteristic data (Page 19). [1)] Note on TCP connections: Avoiding 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 permanently exceeded by the sender (approximately 150200 messages per second).
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
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: • ISO-on-TCP, TCP, ISO transport: 1 to 8192 bytes • UDP: 1 to 2048 bytes
Maximum data length for the 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	• For sending ISO transport, ISOonTCP, TCP: – 400 bytes / TPDU with AG_SEND / AG_LSEND – 1452 bytes / TPDU with AG_SSEND • For receiving – ISO transport: 512 bytes / TPDU – ISO-on-TCP: 1452 bytes / TPDU – TCP: 1452 bytes / TPDU

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 via a UDP connection. This gives you the option of registering the CP as a node in a multicast group.
- UDP packet 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 27).

The following CPU resources are required:

- Per SEND job short (AG_SEND) or long (AG_LSEND): 1 resource
- Per RECEIVE job short (AG_RECV): 1 resource
- Per RECEIVE job long (AG_LRECV): 2 resources
- 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) or long (AG_LSEND): max. 32*) / 12**) per CPU
- RECEIVE calls short (AG_RECV): max. 64*) / 24**) per CPU
- RECEIVE calls long (AG_LRECV): variable ***)
  *) The higher values apply to the CPU 416 and CPU 417.
  **) The lower values apply to the CPU 412 and CPU 414.
  ***) 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.

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 and parameter assignment 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 Characteristic data of TCP connections for HTTPS

Connections for Web browser

For HTTPS access, at least 4 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.

2.7 Characteristic data of the integrated 2port 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 X1P2R) is then turned off.

2.8 Encryption methods (Ciphers) used by the module

The following tables list the encryption methods (ciphers) used by the CP with firmware versions V4.0.

Meaning of the table columns

- **Category**
  - Cipher: Cipher suite (cryptographical method)
  - SEA: Signature and encryption algorithm
  - DSA: Signature algorithm
- **Name**
  Name of the category according to IANA
  You can find an overview of the TLS parameters and Cipher Suites on the following page:
  Link: (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4)
- **Value**
  Value (hexadecimal) of the suite according to IANA
- **TLS**
  TLS version with which the respective category is used.
- **Security**
  - ✓
    Method considered secure
  - Legacy
    Method no longer considered secure
- **Protocol**
  The numbers indicate the communication protocols that use the respective category.

TLS versions used by the CP

TLS version	Security
TLS Version 1.3	✓

Ciphers used by CP with firmware version V4.0

Category	Name	Value	TLS	Security	Protocol
Cipher	TLS_AES_128_GCM_SHA256	0x13,0x01	TLS 1.3	✓	HTTPS (TCP 443)
Cipher	TLS_AES_256_GCM_SHA384	0x13,0x02	TLS 1.3	✓	HTTPS (TCP 443)
Cipher	TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS 1.3	✓	HTTPS (TCP 443)
Cipher	TLS_AES_128_CCM_SHA256	0x13,0x04	TLS 1.3	✓	HTTPS (TCP 443)
DSA	DSA_SHA256	0x0402		✓	HTTPS (TCP 443)
DSA	DSA_SHA384	0x0502		✓	HTTPS (TCP 443)
DSA	DSA_SHA512	0x0602		✓	HTTPS (TCP 443)
DSA	ecdsa_secp256r1_sha256	0x0403		✓	HTTPS (TCP 443)
DSA	ecdsa_secp384r1_sha384	0x0503		✓	HTTPS (TCP 443)
DSA	ecdsa_secp521r1_sha512	0x0603		✓	HTTPS (TCP 443)
SEA	secp384r1	0x18		✓	HTTPS (TCP 443)
SEA	secp521r1	0x19		✓	HTTPS (TCP 443)
SEA	x448	0x1E		✓	HTTPS (TCP 443)

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.

Please 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 5.3.
  CPUs with firmware version 5.0 must be upgraded to V5.3.

For more information about the required version of the STEP 7 configuration tool, refer to section Project engineering (Page 29).

Table of compatible CPUs

The CP is supported by the S7400 CPUs with the order 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
- Which CPUs support the LOCK/UNLOCK function with the FETCH/WRITE services
- Which CPUs support operation of the CP as 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				
			a	b	c	d	e
CPU 412-1	..412-1XJ05-0AB0	V5.3.5	+ [2)]	14	24/24	+	+
CPU 412-1	..412-1XJ07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 412-2	..412-2XJ05-0AB0	V5.3.5	+ [2)]	14	24/24	+	+
CPU 412-2	..412-2XK07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 412-2PN	..412-2EK06-0AB0	V6.0.7	+ [2)]	14	24/24	+	+
CPU 412-2PN	..412-2EK07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 414-2	..414-2XK05-0AB0	V5.3.5	+ [2)]	14	24/24	+	+
CPU 414-2	..414-2XL07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 414-3	..414-3XM05-0AB0	V5.3.5	+ [2)]	14	24/24	+	+
CPU 414-3	..414-3XM07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 414-3 PN/DP	..414-3EM05-0AB0	V5.3.5	+ [2)]	14	24/24	+	+
CPU 414-3 PN/DP	..414-3EM06-0AB0	V6.0.7	+ [2)]	14	24/24	+	+
CPU 414-3 PN/DP	..414-3EM07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 414F-3 PN/DP	..414-3FM06-0AB0	V6.0.7	+ [2)]	14	24/24	+	+
CPU 414F-3 PN/DP	..414-3FM07-0AB0	V7.0.2	+ [2)]	14	24/24	+	+
CPU 416-2	..416-2XN05-0AB0	V5.3.5	+ [2)]	14	64/64	+	+
CPU 416-2	..416-2XP07-0AB0	V7.0.2	+ [2)]	14	64/64	+	+
CPU 416F-2	..416-2FP07-0AB0	V7.0.2	+ [2)]	14	64/64	+	+
CPU 416-3	..416-3XR05-0AB0	V5.3.5	+ [2)]	14	64/64	+	+
CPU 416-3	..416-3XS07-0AB0	V7.0.2	+ [2)]	14	64/64	+	+
CPU 416-3 PN/DP	..416-3ER05-0AB0	V5.3.5	+ [2)]	14	64/64	+	+
CPU 416-3 PN/DP	..416-3ES06-0AB0	V6.0.7	+ [2)]	14	64/64	+	+
CPU 416-3 PN/DP	..416-3ES07-0AB0	V7.0.2	+ [2)]	14	64/64	+	+
CPU 416-3F PN/DP	..416-3FR05-0AB0	V5.3.5	+ [2)]	14	64/64	+	+
CPU 416F-3 PN/DP	..416-3FS06-0AB0	V6.0.7	+ [2)]	14	64/64	+	+
CPU 416F-3 PN/DP	..416-3FS07-0AB0	V7.0.2	+ [2)]	14	64/64	+	+
CPU 417-4	..417-4XT05-0AB0	V5.3.5	+ [2)]	14	64/64	+	+
CPU 417-4	..417-4XT07-0AB0	V7.0.2	+ [2)]	14	64/64	+	+
CPU 412-5H	..412-5HK06-0AB0	V6.0.9	+ [2)]	14	64/64	+	-
CPU 414-5H	..414-5HM06-0AB0	V6.0.9	+ [2)]	14	64/64	+	-
CPU 416-5H PN/DP	..416-5HS06-0AB0	V6.0.9	+ [2)]	14	64/64	+	-
CPU 417-5H PN/DP [3)]	..417-5HT06-0AB0	V6.0.9	+ [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				
			a	b	c	d	e
CPU 410-5H [3]	..410-5HX08-0AB0	V8.2.0	+ [2]	14	64/64	+	-
CPU 410-5H [4]	..410-5HX08-4AB0	V10.1	+ [2]	14	64/64	+	-
CPU 410 SMART	..410-5HN08-0AB0	V8.2.0	+ [2]	14	64/64	+	-
CPU 410E	..410-5HM08-0AB0	V8.2.0	+ [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) Only for use with PCS 7

4) Only for use with PCS neo

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

Table 3-1 Required STEP 7 version

Either STEP 7 V5 or STEP 7 Professional		CP 443-1 functionality
STEP 7 V5		
	• STEP 7 V5.7 + Service Pack 2 and • HSP 1128 (Hardware Update) *	The functionality described in this document can be used.
STEP 7 Professional		
	STEP 7 Professional V20	The functionality described in this document can be used.

Note

In older versions of the configuration software, you can configure the device as CP443-1 EX30. Note the differences between the CP443-1 EX30 and the CP443-1 EX31 in the section Enhanced functions (Page 13)

***** You will find the HSP on the Internet pages of Siemens Industry Online Support at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/view/23183356))

3.4 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 Documentation references (Page 81).

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 53) for operation with a high communications load.

LEDs, QR-Code

4

4.1 Condition codes

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 (EX30)

The LEDs have the following meaning:

- INTF: Internal error
- EXTF: External error
- BUSF: 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
- P1 / P2: Link status / activity of Ethernet port 1 / port 2

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)	BUSF (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 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.
-	○	●	-	-	-	Double IP address detected during CP operation.
○	●	☼	●	○	-	RUN with external error; One or more IO devices are not obtainable.
○	●	○	●	○	-	• 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.
○	○	●	●	○	-	• 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
○	●	●	○	○	○	When the CP is used in an expansion rack and switched-off central rack.
☼	☼	☼	☼	☼	☼	Module fault / system error

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.
P1 / P2 (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.
		There is permanent data transfer via Ethernet at the port.

Module identification with flashing LED (PROFINET interface)

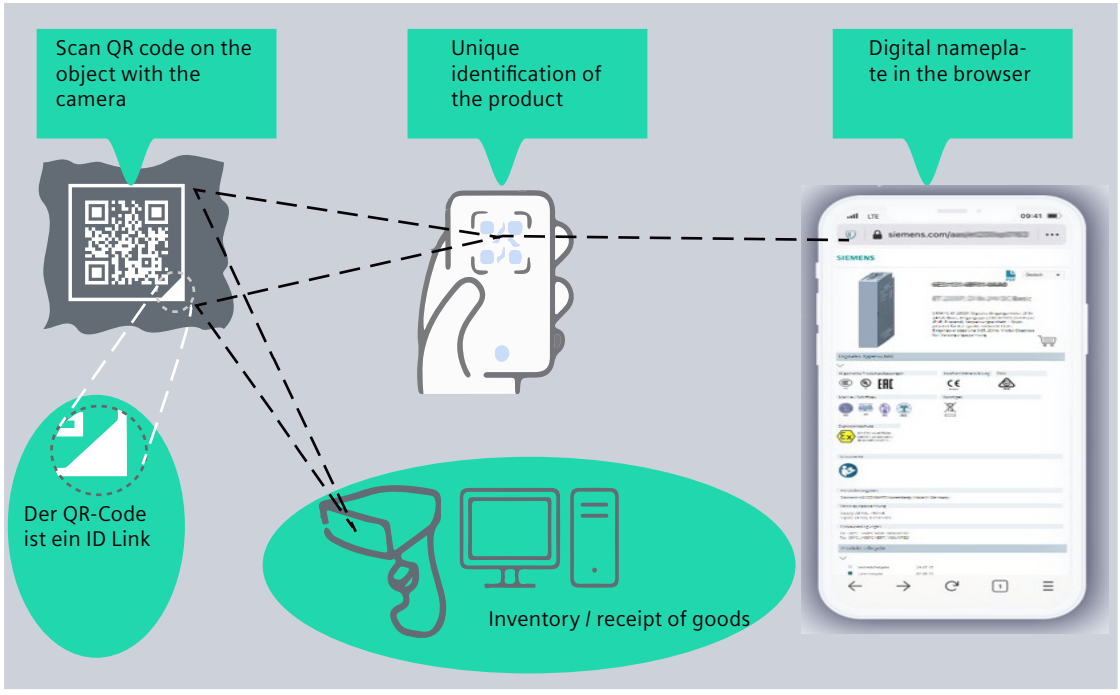
With the help of Web diagnostics or the online functions of STEP 7, you can search for and identify the module in the rack. The options for this are as follows:

- In Web diagnostics
  You click the "Flash" button in the update center.
- In STEP 7
  You click the "Flash" button in the "Browse network" dialog

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

4.2 QR code

Identification link - Easy to use



QR code

The QR code on the front of this product and on the packaging uniquely identifies the product.

The QR code is an Identification Link in accordance with IEC 61406-1.

When you scan the QR code, e.g. with a smartphone, you directly open the Siemens web page of the digital nameplate. The web page of the digital nameplate is structured in line with responsive web design.

For your plant documentation, you have the option to connect the link with your data.

Digital nameplate

The digital nameplate is:

- A contribution by Siemens towards reducing the CO_2 footprint and conserving resources.
- An efficient way to access the product information available on the Internet. This information is kept up to date over the entire product life.

You can retrieve the following information about the product on the web page of the digital nameplate:

- Product identification
- User documentation
- Technical specifications

- Certificates, Declaration of Conformity, manufacturer information
- Current software/firmware versions
- Product news and more information

Installation, wiring, commissioning, removal

5

Safety notices on the use of the device

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

5.1 Important notes on using the device

5.1.1 Notices on use in hazardous areas

⚠ WARNING

EXPLOSION HAZARD

Do not remove or replace while circuit is live when a flammable or combustible atmosphere is present.

⚠ WARNING

Explosion hazard

Do not disconnect equipment when a flammable or combustible atmosphere is present.

⚠ WARNING

Substitution of components may impair suitability of the equipment.

⚠ 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 surges of more than 40% of the rated voltage. Under no circumstances may transient surges exceed 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 and FM

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

EXPLOSION HAZARD

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

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

For operation the device is intended to be installed within an enclosure/control cabinet. The inner temperature of the enclosure/control cabinet corresponds to the ambient temperature of the device. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

⚠ CAUTION

Risk of injury

To prevent injury, read the manual before use.

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

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

5.2 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.
- For function checks, maintenance and servicing work, you need to observe the requirements on checking and maintaining plants in hazardous areas according to the standards EN / IEC 60079-17.

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.

NOTICE

Using the CP in shipbuilding

When the CP is used in shipbuilding, you need to install the modules in such a way that there are no free slots on the rack.

The steps for installing the CP are explained below.

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

Follow the steps outlined below:

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

NOTICE
CP as PROFINET IO controller when used with a CPU version < V6.0 When installing the CP for use as a PROFINET IO controller with a CPU version < V6.0, note the following points about 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. Depending on which CPU you use, there may be other limitations.

   Note

   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.
   You can find connection examples in the general Part A of this manual Documentation references (Page 81).
6. Where necessary, connect another component to the remaining free RJ45 jack.

Note

Autocrossing mechanism - effects on the connections

For small local area networks or for connecting several Ethernet devices, a 2port switch has been integrated in the CP 4431.

With the autocrossing mechanism integrated in the switch, it is possible to establish the connection from a laptop or from the PG/PC directly using standard cables. 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.
  You can find more information on this in section Interface configuration (Page 55)
- Connecting switches
  If you connect further switches, make sure that no ring is formed in the network.

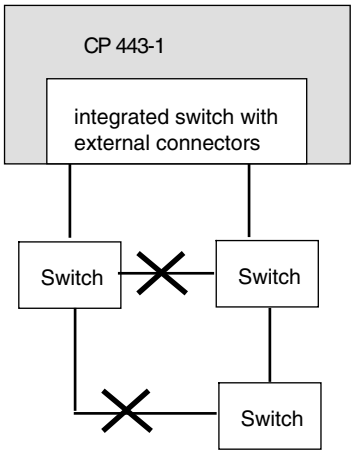


Figure 5-1 Connecting switches (a cross denotes an impermissible connection)

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 Documentation references (Page 81).

5.4 Commissioning

5.4.1 Commissioning - procedure

The steps for commissioning the CP are explained below. Commissioning involves the addressing 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 S7400 station.
   - Requirement:
     You have configured the CP in a STEP 7 project for the properties and services you want to use.

     Note

     You can connect the PG when configuring the CP as follows:
     - via MPI
     - via Industrial Ethernet
       For further details, refer to the general part Documentation references (Page 81) of this manual:
       - Initial addressing (node initialization);
       - Downloading the 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 have the following options available:
   - Hardware diagnostics and troubleshooting with STEP 7.
   - Communication diagnostics with special diagnostics.
   - Web diagnostics.

     Note

     Module replacement - adapting the cycle load with an older CPU

     If you use the CP as a replacement 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 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

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products.
- When the internal and external network are disconnected, an attacker cannot access internal data. Therefore operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Terminate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

Physical access

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Restrict physical access to the device to trusted personnel.
- Lock unused physical ports on the device. Unused ports can be used to access the system without authorization.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device.
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (e.g. for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it.

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 SC with firewall.

Security functions of the product

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

- Protection levels
  - Configure a protection level of the CPU.
  - The "Status-dependent" protection level is preset with a CP443-1 EX31.
- Security function of the communication
  - Enable the IP access protection of the CP (HW Config).
  - Disable access to the Web server of the CPU (CPU configuration) and on the CP.
- 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

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.

- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured, for example, or secure, higher layer protocols can be used.

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		
TCP Modbus	TCP/502	Closed	✓	--	No	No
S7 protocol	TCP/102	Open	--	--	No	No
SNMP	UDP/161	Closed	✓	--	No	No
HTTPS	TCP/443	Closed	✓	--	No	Yes
PROFINET CM	UDP/34964	Open	--	--	No	No
PROFINET UDP 2/x	UDP/49152-65535	Open	--	--	No	No

Also note the ports for configured and programmed connections. See section 5.6, item 5.7 in the configuration manual Documentation references (Page 81).

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)
- NTP / 123 (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.

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:
  - Configuration and diagnostics of the CP (relevant system connections for configuration, diagnostics, and PG channel routing are retained);
  - Web diagnostics
  - HTTP access
  - Routing function

6.3 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.

6.4 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.

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) 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.
- **Resetting / memory reset**
  It is not possible to reset or to reset the memory of the CP during operation of the station. To perform this action, perform a memory reset of the CPU.

6.5 Configuration in STEP 7

Configuration in STEP 7

You configure the CP alternatively with the following configuration tools:

- STEP 7 V5
- STEP 7 Professional

You will find the required versions in the section Project engineering (Page 29).

The following information on configuration applies to both configuration tools.

6.6 Interface configuration

6.6.1 Fast Ethernet

The configuration of the network settings "Transmission medium / Duplex" is made in the Properties dialog in the "Options" tab for both ports.

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.

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

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/ autocrossover" 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 order number 6GK7 443-1EX11-0XE0), you must not use a crossover cable.
- Connecting a switch
  To connect a switch, that does not support autocrossing, 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:

- Network components with 100 Mbps without "autonegotiation"
  If you use network components that do not support "autonegotiation" at 100 Mbps, 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 via 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 Ethernet port over which the PC is connected to the configuration PC is disabled in the loaded configuration.

6.6.2 IP configuration

6.6.2.1 Points to note about IP configuration

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.

6.6.2.2 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.

6.6.3 Port configuration with redundant partners

Using the same port number with redundant partners

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 considerable improvement in performance even in the following situations:

- Applications that generally require a fast start-up time for the IO devices following "Power on" 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 Documentation references (Page 81) Documentation references (Page 81).

Note

Reconfiguration - behavior on startup

After reconfiguring an IO device for prioritized startup, the first startup takes place in the normal time without being prioritized. 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.

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.

6.8 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 Documentation references (Page 81).

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 IP_CONFIG (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 Documentation references (Page 81)/.

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 passive unspecified connections are not entered in the IP-ACL because all required parameters are only known when the connection is established.

How to configure IP access protection is described in the general part of this manual, see "Documentation references (Page 81)".

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

Programming

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. There, you will also find examples of parameter assignment!

6.10 Time-of-day synchronization

General rules

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

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

Note

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

Note

Note the following about timeofday synchronization in NTP mode:

If an NTP frame is detected by the CP as "not exact" (example: NTP server is not synchronized externally), there is no forwarding via the backplane bus. If this problem occurs, none of the NTP servers is displayed as "NTP master" in the diagnostics; rather all NTP servers are displayed only as being accessible.

Project engineering

For more detailed information on configuration, refer to the online help of the "Time-of-day synchronization" parameter group and Part A of the manual Documentation references (Page 81).

6.11 SNMP agent

SNMP (Simple Network Management Protocol)

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

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

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

MIB file and SNMP profile file

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

Further information

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

You will find more information on the MIB in Documentation references (Page 81).

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
1-2	Port 1-2 (PROFINET interface)
3	Internal CP interface

Access permissions using community name

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

Table 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 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

6.12 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.

6.13 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, 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.

With an H-CPU with firmware as of V6.0, you can set the monitoring time in the properties parameters of the configured connection.

Diagnostics and upkeep

7

⚠ 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.



⚠ 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.

7.1 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, QR-Code (Page 33).
- **Web diagnostics**
  For information on Web diagnostics using HTTP, refer to the section The CP as Web server (Page 68).

- **STEP 7 V5.7**
  - 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.

7.2 The CP as Web server

Web diagnostics

The CP provides you with the functionality of a Web server for access using a Web browser. With the following address, you have access to Web diagnostics:
`https:\\<IP address of the CP>`

The CP uses a self-created certificate. The browser does not recognize this certificate and therefore issues a warning or denies access. In this case, adjust the configuration of the browser accordingly.

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.

The CP supports the following languages for interfaces and diagnostics buffer entries in the delivery state:

- German
- English
- French
- Italian
- Spanish

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 Documentation references (Page 81).

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.

By default, this function is disabled.

For detailed information on the Web server and Web diagnostics, refer to the general Part A of this manual Documentation references (Page 81)

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
- MS Edge

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

7.3 Replacing older modules

Replacing a device

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 Diagnostics and upkeep (Page 67) on plugging and pulling the module. This applies in particular if you operate the CP as a PROFINET IO controller.

The CP 443-1 EX31 described here with article number 6GK7 443-1EX31-0XE0 and the current firmware version can be used as a replacement for the following predecessor products. The prerequisite is that neither the transmission speed 10 Mbps nor the IRT flex function were configured.

- CP 443-1 (6GK7 443-1EX30-0XE0) firmware version V3
- CP 443-1 (6GK7 443-1EX20-0XE0) firmware version V1 / V2

When replacing modules with CPUs with a firmware version lower than V5.0, the 6GK7 443-1EX11-0XE0 or 6GK7 443-1EX41-0XE0 must continue to be used.

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

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 only for ISO connections

The configured MAC address is only used for ISO connections and S7 connections of the type "ISO". In all other cases, the MAC address assigned by the manufacturer is used.

For information on replacing previous modules, refer to the information in section Diagnostics and upkeep (Page 67).

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

During configuration of the CP you can specify the IP configuration in the properties dialog; one option is to obtain 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.

Ideally, you should therefore configure IP as follows:

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

7.4 Loading new firmware

Options for a firmware update

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

- Via the firmware loading mechanism integrated in STEP 7/TIA.
- Using the update center
  You can reach the update center using Web diagnostics.
  The CP supports the storage of several firmware versions. Using the firmware load function in the update center, you can activate the required firmware version.
  Requirement: The "Firmware download via Web" option is selected in the configuration and the user rights have been set.

Note the descriptions of firmware downloads in the manual Part A Documentation references (Page 81).

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.
   The download involves two stages:
   - Section 1: Downloading firmware
   - Section 2: Activating firmware

   You will find the LED displays in the section LEDs, QR-Code (Page 33)
   If the download is aborted, RUN and STOP flash alternately.
3. After the firmware download, the CP goes through a warm restart.

7.5 Memory reset / reset to factory defaults

The CP has a two level function available for resetting:

- Memory reset
- Resetting to factory settings

Note

Data on the CP is deleted - CPU data is retained

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

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

- ACL remains active.

Note

Memory reset - PROFINET IO is being used

If you use PROFINET IO, the following applies:

If you reset the memory of a CPU, there is also a memory reset on the CP.

Note the restrictions when a protection level is configured for the CPU. See section Effects of protection levels (Page 54) 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 V5.7 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 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

Following the memory reset, the CP retains the configured MAC address and the IP address. 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 (STOP) with error" state (see LEDs, QR-Code (Page 33)). The configuration data must then be reloaded. You can also initiate this loading from the CPU by cycling power (OFF > ON).

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.

Technical specifications

8

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

Technical specifications			
Article number	6GK7 443-1EX31-0XE0		
Attachment to Industrial Ethernet			
Amount	1 x PROFINET interface with 2port switch		
Design of PROFINET interface (2port switch)	Connector	2 x RJ-45 jacks	
	Transmission speed	100 Mbps	
	Aging time (2port switch)	5 minutes	
	Special features of the X1P1R and X1P2R 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	Typical	390 mA
		Maximum	540 mA
	Power dissipation	Typical	2 W
		Maximum	2.9 W
Permitted ambient conditions			
Ambient temperature	During operation with the rack installed horizontally	0 °C to +70 °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		
Corrosive gases as airborne contaminants Reactive species H_2S and SO_2	ISA-S71.04 Severity Level	G1, G2, G3 RH ≤ 75%, no condensation	
	Test according to	IEC 60068-2-42 (SO_2 10 ppm)	
		IEC 60068-2-43 (H_2S 1 ppm)	

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
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 19)

In addition to this, all the information in the S7-400 reference manual "Module Data" Documentation references (Page 81) 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

8.1 Resistance to harmful gases according to ISA-71.04

The devices listed in the scope of validity meet the following requirements regarding resistance to harmful gases:

Corrosive gases as airborne contaminants Reactive species H_2S and SO_2	ISA-71.04 severity level	G1, G2, G3 RH ≤ 75%, no condensation
	Test according to	IEC 60068-2-42 (SO_2 10ppm)
		IEC 60068-2-43 (H_2S 1ppm)

Certification

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.

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/15352/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



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



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 40)".

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)

Observe the conditions for safe usage of the CP according to the section "Notes on use in hazardous areas according to UL HazLoc and FM (Page 40)".

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

For information about the permissible ambient temperature used, refer to section 8 "Technical specifications (Page 73)".

Certificate of Compliance: FM 22US0030X

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.

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

Where to find Siemens documentation

- Article numbers
  You will find the article numbers for the Siemens products of relevance here in the following catalogs:
  - SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI
  - SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70

  You can request the catalogs and additional information from your Siemens representative. You will also find the product information in the Siemens Industry Mall at the following address:
  Link: (https://mall.industry.siemens.com)
- Manuals 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)
  Go to the required product in the product tree and make the following settings:
  Entry type “Manuals”
- Manuals on the data medium
  You will find manuals of SIMATIC NET products on the data medium that ships with many of the SIMATIC NET products.

On configuring, commissioning and using the CP

/1/

SIMATIC NET
CP 443-1
Manual Part B - device manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/109978340)

/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

See also

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/101509838)

/5/

SIMATIC NET
Diagnostics and configuration with SNMP
Diagnostics manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/103949062)

On installing and commissioning the CP

/6/

SIMATIC S7
Automation System S7-400
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/1117740)
- CPU data: Equipment Manual
  Link: (https://support.industry.siemens.com/cs/ww/en/view/53385241)

On configuration with STEP 7 / NCM S7

/7/

SIMATIC NET
Commissioning PC Stations - Manual and Quick Start
Configuration Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15362/man)

/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/45531110)

/9/

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

/10/

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)

On programming (blocks, OPC)

/11/

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

/12/

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)

/13/

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)

/14/

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)

/15/

SIMATIC NET
Industrial Communication with PG/PC
- Volume 1: Basics - System Manual
- Volume 2: Interfaces - programming manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15362/man)

On application and configuration of PROFINET IO

/16/

SIMATIC
PROFINET System Description
System Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/19292127)

/17/

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

On setting up and operating an Industrial Ethernet network

/18/

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

A

Abbreviations, 5

C

Change from RUN to STOP, 47
Change from STOP to RUN, 47
Connection and system diagnostics, 4
Controlling the mode, 47

F

Fault-tolerant system, 17
FETCH/WRITE
    Access coordination, 4
FTP services, 4

G

Glossary, 7

H

H system, 17

I

IP configuration, 4

K

KNOW_HOW_PROTECT, 50

O

Open communications services, 4

P

Programmed connections and IP configuration, 4

R

Redundancy, 58

S

Safety notices, 39
SIMATIC NET glossary, 7
STEP 7, 5