SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet SIMATIC CP 1543-1

Operating Instructions

Preface

Application, functions and requirements 1

LEDs, connections, QR code 2

Connection, mounting, commissioning, disassembly 3

Configuration, program blocks 4

Diagnostics and upkeep 5

Technical specifications 6

Approvals 7

Additional information A

CP 1543-1, firmware V3.0 (6GK7543-1AX00-0XE0)
CP 1543-1, firmware V4.0 (6GK7543-1AX10-0XE0)

07/2024
C79000-G8976-C289-09

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-C289-09
Ⓟ 07/2024 Subject to change

Copyright © Siemens 2013 - 2024.
All rights reserved

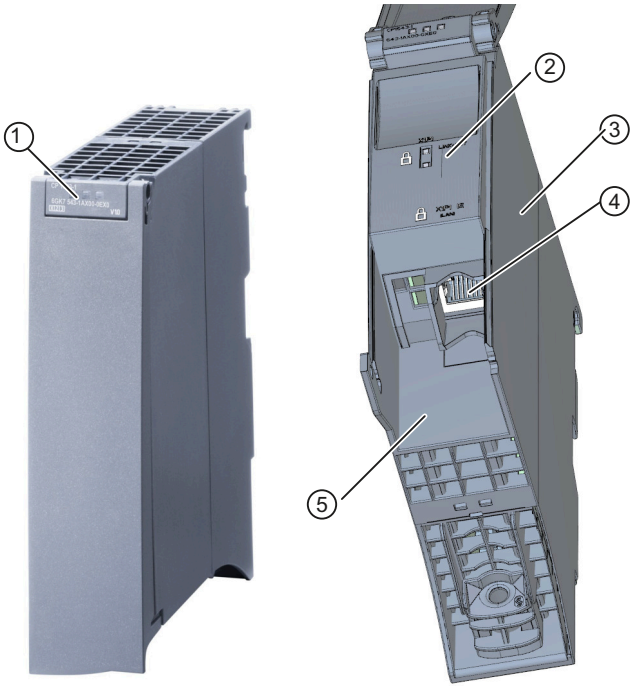
Preface

Validity

This description contains information on the following products:

- CP 1543-1
  Article number 6GK7 543-1AX00-0XE0
  Hardware product version 2
  Firmware version V3.0
  Communications processor for SIMATIC S7-1500
- CP 1543-1
  Article number 6GK7 543-1AX10-0XE0
  Hardware product version 1
  Firmware version V4.0
  Communications processor for SIMATIC S7-1500

View of the CP 1543-1



① LEDs for status and error displays
② LED displays of the Ethernet interface for connection status and activity
③ Type plate
④ Ethernet port: 1 x 8-pin RJ-45 jack
The padlock icon symbolizes the interface to the external, non-secure subnet.
⑤ Label with MAC address

Figure 1 View of the CP 1543-1 with closed (left) and open (right) front cover

Address label: Unique MAC address preset for the CP

The CP ships with a default MAC address. The MAC address is printed on the housing.

If you configure a MAC address (ISO transport connections), we recommend that you use the printed MAC address for the configuration! This ensures that you assign a unique MAC address in the subnet!

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 32) for more on this.

Purpose of the documentation

This manual supplements the S7-1500 system manual.

With the information in this manual and the system manual, you will be able to commission the communications processor. This manual is valid for:

- CP 1543-1, article number 6GK7 543-1AX00-0XE0
- CP 1543-1, article number 6GK7 543-1AX10-0XE0

New in this edition

- New module (6GK7 543-1AX10-0XE0) with hardware product version 1 and firmware version V4.0 with various small improvements, e.g. relating to the security functions.
- Editorial revision

Replaced edition

Edition 07/2021

Current manual edition on the Internet

You will find the current version of this manual on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15340/man)

Version history (only CP with article number 6GK7 543-1AX00-0XE0)

- Firmware version V3.0 with the following new functions:
  - Support of the redundant S7-1500 R/H system; see section Configuration in the redundant R/H system (Page 55).
  - Network authentication according to IEEE 802.1X, refer to section Network authentication (Page 86).
  - Connection to SINEMA Remote Connect, refer to section Communication via SINEMA RC (Page 17).
  - Improvements in the use of the virtual interface of the CPU, refer to section Virtual interface of the CPU (Page 51).
  - Configurable CP diagnostics during runtime, refer to section CP diagnostics (Page 57).
  - Configurable UDP buffering, refer to section Settings (Page 47).
- Firmware version V2.2 with the following new functions:
  - Support of the virtual interface of the CPU, see section Virtual interface of the CPU (Page 51).

- Firmware version V2.1 with the following new functions:
  - Extended security settings using IP routing via the backplane bus, see section IP routing (Page 51).
- Firmware version V2.0 with the following new functions:
  - Secure OUC (Open User Communication) via TCP/IP
  - Secure Mail: New system data types (SDTs) for transferring e-mails
    Alternative: Non secure transfer via port 25 or secure transfer via port 587
  - Operation as FTP server: Access to the SIMATIC memory card of the CPU
  - IP routing via the backplane bus

Sources of information and other documentation

See below, Documentation guide.

Notes on this document

Abbreviations and names

- CP / Module
  Used instead of the full product name CP 1543-1
  These terms are used in the following instead of the complete product designation. In this case, the information applies equally to both firmware versions or hardware product versions of the module.
  If the data of the two devices differs, the firmware version or the hardware product version of the respective device is explicitly stated.
- CP "AX00"
  CP 1543-1 with article number 6GK7 543-1AX00-0XE0
- CP "AX10"
  CP 1543-1 with article number 6GK7 543-1AX10-0XE0
- STEP 7
  Used for the configuration tool STEP 7 Professional

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 display all instances of a search term in a list, some PDF readers support the command <Ctrl>+<Shift>+<F>.

License conditions

Note

Open source software

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

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

- OSS_CP15431_99.pdf
- OSS_CP-15431_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.

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.

See also:
Industrial Ethernet Security (Page 20)
Security recommendations (Page 43)
Encryption methods (Ciphers) used by the module (Page 113)

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.

Documentation guide

The documentation of the SIMATIC products has a modular structure and covers topics relating to your automation system.

The complete documentation for the S7-1500 system consists of a system manual, function manuals, device manuals or operating instructions.

The STEP 7 information system (online help) also supports you in configuring and programming your automation system.

The following table shows additional documents that supplement this CP manual and are available on the Internet.

Table 1 Overview of the documentation for S7-1500

Topic	Documentation	Important contents
System description	System manual: S7-1500 Automation System (https://support.industry.siemens.com/cs/ww/en/view/59191792)	• Application planning • Installation • Connecting • Commissioning
System diagnostics	System diagnostics (https://support.industry.siemens.com/cs/ww/en/view/59192926) function manual	• Overview • Diagnostics evaluation for hardware/software
Communication	Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) function manual	• Overview
	Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) function manual	• Function • Operation
	SIMATIC NET - Industrial Ethernet / PROFINET - system manual • Industrial Ethernet Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465) • Passive network components Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)	• Ethernet networks • Network configuration • Network components

Topic	Documentation	Important contents
Interference-free installation of control systems	Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566) function manual	• Basics • Electromagnetic compatibility • Lightning protection • Housing selection
Cycle and response times	Function manual: Cycle and Response Times (https://support.industry.siemens.com/cs/ww/en/view/59193558)	• Basics • Calculations

CP documentation on DVD

You can find the documentation on the product and the configuration on the DVD supplied with the product. This DVD contains the product manuals valid at the time it is created.

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)

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

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

Keep to the local regulations.

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

Table of contents

Preface ... **3**

1 Application, functions and requirements ... **15**

1.1 Application ... 15

1.2 Intended operational environment ... 15

1.3 Communication services ... 16

1.4 Communication via SINEMA RC ... 17

1.5 Further functions ... 18

1.6 Industrial Ethernet Security ... 20

1.7 Configuration limits and performance data ... 21
1.7.1 Configuration limits of communications modules ... 21
1.7.2 General characteristic data ... 21
1.7.3 Characteristics of S7 communication ... 23
1.7.4 Characteristic data for FTP / FTPS mode ... 24
1.7.5 Characteristics security ... 24

1.8 Requirements for use ... 25
1.8.1 Usable CPUs ... 25
1.8.2 Project engineering ... 26
1.8.3 Program blocks - overview ... 26

2 LEDs, connections, QR code ... **29**

2.1 LEDs ... 29

2.2 Gigabit interface ... 31

2.3 QR code ... 32

3 Connection, mounting, commissioning, disassembly ... **35**

3.1 Disassembly ... 35

3.2 Important notes on using the device ... 35
3.2.1 Safety-extra low voltage + redundant power supply / without NEC ... 35
3.2.2 Notes on use in hazardous areas ... 36
3.2.3 Notes on use in hazardous areas according to ATEX / IECEx ... 36
3.2.4 Notes on use in hazardous areas according to UL HazLoc and FM ... 37

3.3 Installation, removal and repairs in hazardous areas ... 38

3.4 Installing and commissioning the CP 1543-1 ... 40

3.5 Operating mode of the CPU: Reaction of the CP ... 41

4 Configuration, program blocks ... **43**

4.1 Security recommendations ... 43

4.2 Settings ... 47

4.3 PUT/GET/FETCH/WRITE: Restrictions in the CPU ... 48
4.4 Network settings ... 49
4.5 IP configuration ... 49
4.5.1 Points to note about IP configuration ... 49
4.5.2 IPv6 addresses ... 50
4.5.3 Restart after detection of a duplicate IP address in the network ... 50
4.5.4 IP routing ... 51
4.5.5 Virtual interface of the CPU ... 51
4.5.6 Programmed connections: Restriction of firewall rules ... 54
4.6 Configuration in the redundant R/H system ... 55
4.7 Time-of-day synchronization ... 55
4.8 DNS configuration ... 56
4.9 Communication with the CPU ... 57
4.9.1 CP diagnostics ... 57
4.10 FTP communication ... 58
4.10.1 FTP server ... 58
4.10.1.1 Configuring the FTP server function ... 58
4.10.2 FTP client ... 61
4.10.2.1 The program block FTP_CMD (FTP client function) ... 61
4.10.2.2 Input parameter - FTP_CMD ... 63
4.10.2.3 Job blocks for FTP_CMD ... 65
4.10.2.4 Output parameters and status information FTP_CMD ... 70
4.10.2.5 Structure of the data block (file DB) for FTP client operation ... 73
4.11 Security ... 75
4.11.1 Security user ... 76
4.11.2 VPN ... 76
4.11.2.1 Creating VPN tunnel communication between S7-1500 stations ... 77
4.11.2.2 Establishment of VPN tunnel communication between the CP and SCALANCE M ... 79
4.11.2.3 VPN tunnel communication with SOFTNET Security Client ... 79
4.11.2.4 SINEMA Remote Connect ... 80
4.11.2.5 CP as passive subscriber of VPN connections ... 83
4.11.3 Firewall ... 83
4.11.3.1 Firewall sequence when checking incoming and outgoing frames ... 83
4.11.3.2 No counting of incorrect packages ... 84
4.11.3.3 Notation for the source IP address (advanced firewall mode) ... 84
4.11.3.4 HTTP and HTTPS not possible with IPv6 ... 84
4.11.3.5 Firewall settings for connections via a VPN tunnel ... 84
4.11.3.6 Settings for online security diagnostics and downloading to station with the firewall activated ... 85
4.11.4 Log settings - Filtering of the system events ... 85
4.11.5 Network authentication ... 86
4.12 Program blocks for OUC ... 88

5 Diagnostics and upkeep ... 91

5.1 Diagnostics options ... 91
5.2 Online functions ... 93
5.2.1 Online security diagnostics via port 8448 of the CP ... 93

5.2.2 Connect online ... 93
5.3 Diagnostics with SNMP ... 94
5.4 Update firmware ... 97
5.5 Replacing a module without a programming device ... 99
6 Technical specifications ... 101
6.1 Technical specifications of the CP (6GK7543-1AX00-0XE0) ... 101
6.2 Technical specifications of the CP (6GK7543-1AX10-0XE0) ... 102
6.3 Ambient temperature ... 103
6.4 Pinout of the Ethernet interface ... 104
6.5 Permitted cable lengths - Ethernet ... 104
6.6 Permitted cable lengths - Gigabit Ethernet ... 104
7 Approvals ... 105
A Additional information ... 111
A.1 Linking to other systems with FETCH/WRITE ... 111
A.2 Encryption methods (Ciphers) used by the module ... 113
A.3 Syslog messages ... 116
A.3.1 Structure of the Syslog messages ... 117
A.3.2 Tags in Syslog messages ... 118
A.3.3 Messages ... 119
Index ... 123

Application, functions and requirements

1

1.1 Application

The CP is intended for operation in a single or redundant (R/H) S7-1500 automation system. The CP enables the S7-1500 to be connected to Industrial Ethernet.

With a combination of different security measures such as firewall, VPN and protocols for data encryption, the CP protects the S7-1500 or even entire automation cells from unauthorized access. The CP also protects the communication between the S7 station and communications partners from spying and manipulation.

1.2 Intended operational environment

The following figure shows a sample system configuration as intended operating environment for the CP.

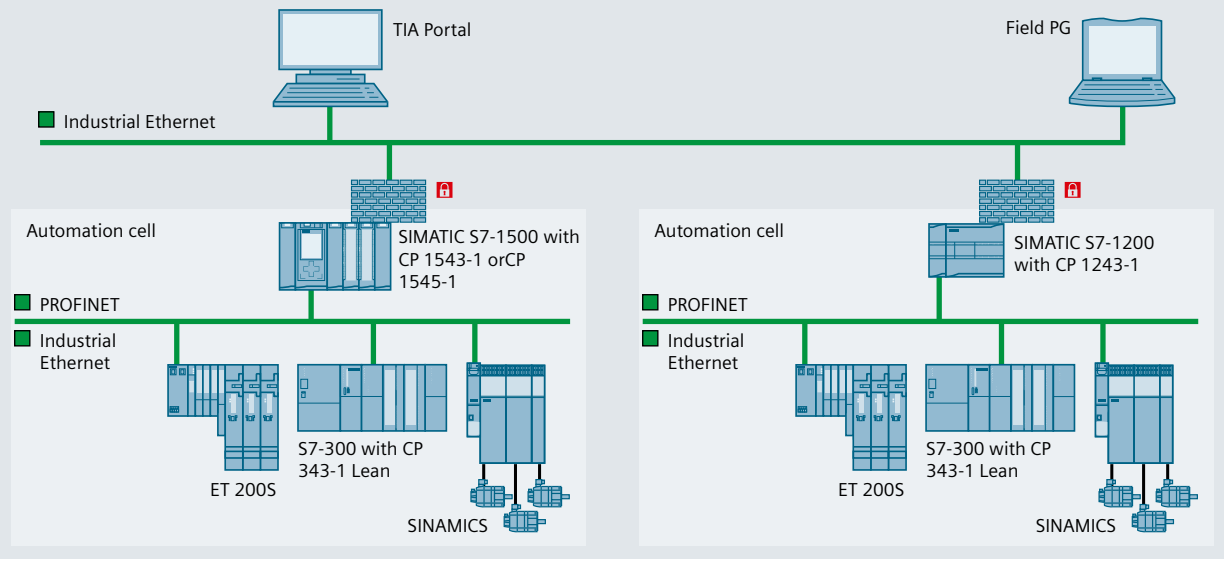


Figure 1-1 Example of a system configuration for the intended operating environment of the CP

For protection of the company and plant network, the following security components are recommended:

- External firewalls with Intrusion Detection System (IDS) protect the company network against external attacks.
- DMZ firewalls in the backbone level protect the plant network.
- Security modules protect each individual automation cell.

Note

Security information

To protect your system, refer to the information in the section Security recommendations (Page 43).

1.3 Communication services

The CP supports the following communication services:

- **Open User Communication (OUC)**
  Open User Communication supports the following communications services via the CP using programmed or configured communications connections:
  - ISO transport (complying with ISO/IEC 8073)
  - TCP (IPv4/IPv6) (acc. to RFC 793 and 8200)
    With the interface via TCPv4/v6 connections, the CP supports the socket interface to TCP/IP available on practically every end system.
  - ISO-on-TCP (acc. to RFC 1006)
  - UDP (acc. to RFC 768)
  - Multicast over UDP connection
    The multicast mode is made possible by selecting a suitable IP address when configuring connections.
  - Sending e-mail via SMTP (port 25) or SMTPS (port 587) with authentication on an e-mail server.
- **S7 communication**
  - PG communication
  - Operator control and monitoring functions (HMI communication)
  - Data exchange over S7 connections
    Note: In the R/H system, the CP only supports S7 connections as server.
  - PUT/GET
    See section PUT/GET/FETCH/WRITE: Restrictions in the CPU (Page 48) for more on this.

- **FTP/FTPS**
  FTP functions (File Transfer Protocol) for file management and access to data blocks in the CPU
  - FTP server
    Can be activated via the configuration
  - FTP client
    Configurable via program blocks.
- **FETCH/WRITE**
  - FETCH/WRITE services as server (corresponding to S5 protocol) via ISO transport, ISO-on-TCP and TCP connections
    The S7-1500 with the CP is always the server (passive connection establishment).
    The fetch or write access (client function with active connection establishment) is performed by a SIMATIC S5 or a third-party device / PC.

1.4 Communication via SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

The "SINEMA RC Server" application provides end-to-end connection management of distributed networks via the Internet. This also includes secure remote access to lower-level stations. Communication between SINEMA RC Server and the remote devices takes place via a VPN tunnel with consideration of the stored access rights.

SINEMA RC uses OpenVPN for encryption of the data. The center of the communication is SINEMA RC Server via which communication runs between the subscribers and that manages the configuration of the communications system.

SCALANCE M routers, which you can use for the connection, also support OpenVPN and connection to SINEMA Remote Connect.

Parameter groups

You configure communication via SINEMA RC in the following parameter group:

> "Security > VPN"

For information on the configuration, refer to section SINEMA Remote Connect (Page 80).

Application

If the function is enabled, you use the CP for remote maintenance via SINEMA RC.

1.5 Further functions

Time-of-day synchronization with NTP (Network Time Protocol)

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

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

Security function: The CP supports the NTP (secure) protocol with support of RFC5905 and RFC5906 with shared key for secure transfer during time-of-day synchronization.

For details, see section Time-of-day synchronization (Page 55).

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 and Automation System MIB.

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

IP configuration - IPv4 and IPv6

The essential features of IP configuration for the CP:

- The CP supports the use of IP addresses according to IPv4 and IPv6.
- 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 (IPv4) can also be assigned to the CP by the user program (for program blocks refer to the section Program blocks - overview (Page 26)).
  Note: Does not apply to S7 connections.

IP routing

The CP supports static IP routing (IPv4) to other CMs/CPs.

For details, see section IP routing (Page 51).

IPv6 addresses - area of use on the CP

An IP address according to IPv6 can be used for the following communications services:

- FETCH/WRITE access (CP is server)
- FTP server mode
- FTP client mode with addressing via program block
- E-mail transfer with addressing via program block
- TCP via OUC blocks with the following SDTs: TCON_QDN, TCON_QDN_SEC
- SNMP

When using IPv6 addresses, make sure to configure the DNS server accordingly. Observe also the information on address bands in section IPv6 addresses (Page 50).

Access to the Web server of the CPU

Via the LAN interface of the CP, you have access to the Web server of the CPU. With the aid of the Web server of the CPU, you can read out module data from a station.

Note the special description of the Web server; see Cybersecurity information (Page 7), Documentation guide.

Note

Web server access using the HTTPS protocol

The Web server of a SIMATIC S7-1500 station is located in the CPU. For this reason, when there is secure access (HTTPS) to the Web server of the station using the IP address of the CP 1543-1, the SSL certificate of the CPU is displayed.

S5/S7 addressing mode for FETCH/WRITE

The addressing mode can be configured for FETCH/WRITE access as S7 or S5 addressing mode. The addressing mode specifies how the position of the start address is identified during data access (S7 addressing mode applies only to data blocks / DBs).

Read the additional information in the online help of STEP 7.

1.6 Industrial Ethernet Security

All-round protection - the task of Industrial Ethernet Security

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. The data transfer from the external network connected to the CP can be protected by various security measures:

- Data espionage (FTPS, HTTPS)
- Data manipulation
- Unauthorized access

Secure underlying networks can be operated via additional Ethernet/PROFINET interfaces implemented by the CPU or additional CPs.

Security functions of the CP for the S7-1500 station

As result of using the CP, the following security functions are accessible to the S7-1500 station on the interface to the external network:

- Firewall
  - IP firewall with stateful packet inspection (Layer 3 and 4)
  - Firewall also for non-IP frames according to IEEE 802.3 (Layer 2)
  - Global and user-defined firewall rules

  The protective function of the firewall can be applied to the operation of single devices or several devices, as well as entire network segments.
- VPN
  The following alternatives can be used:
  - Secured communication via IPsec tunnels
    VPN communication allows the establishment of secure IPsec tunnels for communication with one or more security modules. The CP can be grouped together with other modules to form VPN groups during configuration. IPsec tunnels are created between all security modules of a VPN group.
    The CP "AX10" supports IKEv1 and IKEv2.
  - Remote maintenance via SINEMA Remote Connect
    It is not necessary and not possible to create a VPN group for communication via a SINEMA RC server. The SINEMA RC server manages the communication between the devices and the security mechanisms (OpenVPN).
- Logging
  To allow monitoring, events can be stored in log files that can be read out using STEP 7 or can be sent automatically to a Syslog server.
- FTPS (explicit mode)
  For encrypted transfer of files
- NTP (secure)
  NTP with support of RFC5905 and RFC5906 with shared key for secure transfer during time-of-day synchronization

- SMTPS
  Foe secure transfer of e-mails via port 587
- SNMPv3
  For secure transmission of network analysis information safe from eavesdropping

Observe the information in section Security recommendations (Page 43).

1.7 Configuration limits and performance data

1.7.1 Configuration limits of communications modules

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

- The number of communications modules that can be operated in a rack depends on the CPU type being used.
  By operating several CMs/CPs, you can increase the configuration limits listed below for the station as a whole. The CPU does, however, have set limits for the entire configuration. The size of the configuration made available by a CP can be increased by using more than one CP within the framework of the system limits.
  Note the information in the documentation of the CPU, see Preface (Page 3), Documentation guide.

  Note

  Power supply via the CPU adequate or additional power supply modules required

  You can operate a certain number of modules in the S7-1500 station without an additional power supply. Make sure that you keep to the specified power feed to the backplane bus for the particular CPU type. Depending on the configuration of the S7-1500 station you may need to provide additional power supply modules.

You can find information on pluggable CPs in the redundant R/H system in the "S7-1500R/H redundant system" system manual:
Link: (https://support.industry.siemens.com/cs/ww/en/view/109754833)

1.7.2 General characteristic data

Characteristic	Explanation / values
Total number of freely usable connections on Industrial Ethernet	118 The value applies to the total number of connections of the following types, including the connections via the virtual interface W1 of a redundant CPU: • S7 connections • Connections for open communications services • FTP (FTP client)

Note

Connection resources of the CPU

Depending on the CPU type, different numbers of connection resources are available. The number of connection resources is the decisive factor for the number of configurable connections. This means that the values that can actually be achieved may be lower than specified in this section describing the CP.

Open User Communication (OUC) provides access to communication over TCP, ISO-on-TCP, ISO transport and UDP connections.

The following characteristics are important (OUC + FETCH/WRITE):

Characteristic	Explanation / values
Number of connections	Number of configured and programmed connections (ISO transport + ISO-on-TCP + TCP + UDP + FETCH/WRITE + email): • Max. 118 in total Of which maximum: – TCP connections: 0...118 – ISO-on-TCP connections: 0...118 – ISO transport connections: 0...118 – UDP connections (specified and free) in total: 0...118 – Connection for e-mail: 0...1 – Connections for FETCH/WRITE: 0...16
Maximum data length for program blocks	Program blocks allow the transfer of user data in the following lengths: • ISO-on-TCP, TCP, ISO transport: 1 to 64 kB • UDP: 1 byte to 2 KB • E-mail – Job header + user data: 1 to 256 bytes – E-mail attachment: up to 64 kB
LAN interface max. data field length generated by CP per protocol data unit (TPDU = transport protocol data unit)	• sending ISO transport, ISOonTCP, TCP: 1452 bytes / TPDU • receiving – ISO transport: 512 bytes / TPDU – ISO-on-TCP: 1452 bytes / TPDU – TCP: 1452 bytes / TPDU

Note

Connection resources of the CPU

Depending on the CPU type, different numbers of connection resources are available. The number of connection resources is the decisive factor for the number of configurable connections. This means that the values that can actually be achieved may be lower than specified in this section describing the CP.

You will find detailed information on the topic of connection resources in the "Communication" function manual, see Cybersecurity information (Page 7), Documentation guide.

Restrictions for UDP

- UDP broadcast / multicast
  To avoid overloading the CP due to high broadcast/multicast frame traffic, the receipt of UDP broadcast/multicast on the CP can be limited; refer to section Settings (Page 47).
- UDP frame buffering
  Length of the frame buffer: At least 7360 bytes
  Following a buffer overflow, newly arriving frames that are not fetched by the user program are discarded.

1.7.3 Characteristics of S7 communication

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

Characteristic	Explanation / values
Total number of freely usable S7 connections on Industrial Ethernet	Max. 118
LAN interface - data field length generated by CP per protocol data unit (PDU = protocol data unit)	• For sending: 480 bytes / PDU • For receiving: 480 bytes / PDU
Number of reservable OP connections *	Max. 4
Number of reservable PG connections *	Max. 4
Number of HTTP connections for Web	Max. 4

***** The CPU reserves connection resources. Take the specified values into account for programmed connections also.

Note

Maximum values for an S7-1500 station

Depending on the CPU you are using, there are limit values for the S7-1500 station. Note the information in the relevant documentation.

1.7.4 Characteristic data for FTP / FTPS mode

TCP connections for FTP

FTP actions are transferred from the CP over TCP connections. The following characteristics apply:

- FTP client mode
  You can use a maximum of 32 FTP sessions.
  Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).
- FTP server mode
  You can operate a maximum of 16 FTP sessions at the same time.
  Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).

Program block FTP_CMD for FTP client mode

For communication, use the program block FTP_CMD.

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

1.7.5 Characteristics security

IPsec tunnel (VPN)

VPN tunnel communication allows the establishment of secure IPsec tunnel communication with one or more security modules.

Configuration limits	Value
Number of IPsec tunnels	16 maximum

Firewall rules (advanced firewall mode)

The maximum number of firewall rules in advanced firewall mode is limited to 256.

The firewall rules are divided up as follows:

- Maximum 226 rules with individual addresses
- Maximum 30 rules with address ranges or network addresses
  (e.g. 140.90.120.1-140.90.120.20 or 14.90.120.0/16)
- Maximum 128 rules with limitation of the transmission speed

No bandwidth limitation with CP "AX10"

Under DCP, the CP "AX10" does not support any limitation of the transmission speed (bandwidth limitation).

1.8 Requirements for use

1.8.1 Usable CPUs

- **Compatible CPUs**
  The following CPUs of the specified series that can be configured in STEP 7 can be used as local CPUs of the communications module:
  - Standard CPUs (CPU 15xx) as of firmware version V2.1
  - Compact CPUs (CPU 15xxC) as of firmware version V2.1
  - Technology CPUs (CPU 15xxT / TF) as of firmware version V2.1
  - Fail-safe CPUs (CPU 15xxF) as of firmware version V2.1
  - H-CPUs (CPU 1517H / HF) as of firmware version V3.1
  - R-CPUs (CPU 151xR) as of firmware version V3.1
- **Non-compatible CPUs**
  The following CPUs cannot be used together with the CP:
  - H-CPUs (CPU 151xH... / HF...) ≤ firmware version V3.0
  - R-CPUs (CPU 151xR...) ≤ firmware version V3.0

Note

Keep the firmware version of the CPUs and communications modules up to date

To avoid possible problems when using newer CPUs together with older communications modules, you should keep the firmware of both your communications modules and your CPUs up to date.

Check regularly for security updates for the firmware and use them.

Information regarding product news and new firmware versions of the communications module is available at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15340/dl)

1.8.2 Project engineering

Configuration and downloading the configuration data

When the configuration data is downloaded to the CPU, the CP is supplied with the relevant configuration data. The configuration data can be downloaded to the CPU via a memory card or any Ethernet/PROFINET interface of the S7-1500 station.

The following versions of STEP 7 are required:

STEP 7 version	CP "AX00"	CP "AX10"
STEP 7 Professional as of V14	The functionality of the CP with firmware version V2.0 can be configured.	The CP can be used, but only with the functions of firmware V2.0.
STEP 7 Professional as of V14.1	The functionality of the CP with firmware version V2.1 can be configured.	The CP can be used, but only with the functions of firmware V2.1.
STEP 7 Professional as of V16	The functionality of the CP with firmware version V2.2 can be configured.	The CP can be used, but only with the functions of firmware V2.2.
STEP 7 Professional as of V17	The functionality of the CP with firmware version V3.0 can be configured.	The CP can be used, but only with the functions of firmware V3.0.
STEP 7 Professional V19	The functionality of the CP with firmware version V3.0 can be configured.	The complete functionality of the CP "AX10" with firmware version V4.0 can be configured.

1.8.3 Program blocks - overview

Program blocks - overview

The following program blocks (instructions) are available for the CP.

Table 1-1 Blocks of the Open User Communication

Protocol	Program block (instruction)	System data type
TCP	• TSEND_C/TRCV_C or • TCON/TDISCON + TSEND/TRCV	• TCON_IP_v4 • TCON_QDN • TCON_QDN_SEC • TCON_Configured
ISO-on-TCP		• TCON_IP_RFC
ISO		• TCON_ISOnative

Protocol	Program block (instruction)	System data type
UDP	• TCON/TDISCON + TU-SEND/TURCV	• TCON_IP_v4 • TCON_QDN
E-mail	• TMAIL_C	• TMAIL_V4 • TMAIL_QDN • TMAIL_QDN_SEC • TMAIL_V6 • TMAIL_V6_SEC

Table 1-2 Block for communication services of the CP

Protocol	Program block (instruction)	System data type
FTP	• FTP_CMD	• FTP_CONNECT_IPV4 • FTP_CONNECT_IPV6 • FTP_CONNECT_NAME • FTP_FILENAME • FTP_FILENAME_PART

Table 1-3 Block for configuration of the Ethernet interface or an NTP/DNS server

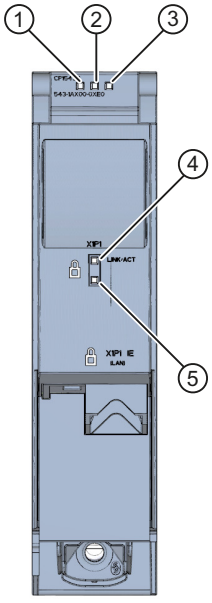
Function	Program block (instruction)	System data type
Configuration of the Ethernet interface	• T_CONFIG	• IF_CONF_V4 • IF_CONF_V6 • IF_CONF_NTP • IF_CONF_DNS • IF_CONF_MAC

LEDs, connections, QR code

2

2.1 LEDs

LEDs



① RUN LED
② ERROR LED
③ MAINT LED
④ LINK/ACT LED
⑤ Reserve LED

Figure 2-1 LED display of the CP 1543-1 (without front cover)

Meaning of the LED displays of the CP

The CP has the following 3 LEDs to display the current operating status and the diagnostics status:

- RUN (one-color LED: green)
- ERROR (one-color LED: red)
- MAINT (one-color LED: yellow)

The following table shows the meaning of the various combinations of colors of the RUN, ERROR and MAINT LEDs.

Table 2-1 Meaning of the LEDs "RUN", "ERROR", "MAINT"

RUN	ERROR	MAINT	Meaning
LED off	LED off	LED off	No supply voltage on the CP or supply voltage too low.
LED lit green	LED lit red	LED lit yellow	LED test during startup
LED lit green	LED lit red	LED off	Startup (booting the CP)
LED lit green	LED off	LED off	CP is in RUN mode. No disruptions
LED lit green	LED flashing red	LED off	A diagnostics event has occurred.
LED lit green	LED off	LED lit yellow	Maintenance, maintenance is demanded.
LED lit green	LED off	LED flashing yellow	Maintenance is required. Downloading the user program
LED flashing green	LED off	LED off	No CP configuration exists Loading firmware
LED flashing green	LED flashing red	LED flashing yellow	Module fault (LEDs flashing synchronized)

Meaning of the LED displays of the Ethernet interface: X1 P1

The LED LINK/ACT (two color green/yellow) is assigned to the port of the Ethernet interface. The table below shows the LED patterns.

Table 2-2 Meaning of the "LINK/ACT" LED

LINK/ACT		Meaning
green off	yellow off	No connection to Ethernet There is no Ethernet connection between the Ethernet interface of the CP and the communications partner. At the current time, there is no data being received/sent via the Ethernet interface.
flashing green	yellow off	The "node flash test" is being performed.

LINK/ACT		Meaning
■ green on	□ yellow off	Connection to Ethernet exists. There is an Ethernet connection between the Ethernet interface of your CP and a communications partner.
■ green on	■ yellow flickers	At the current time, data is being received/sent via the Ethernet interface of the Ethernet device of a communications partner on Ethernet.

2.2 Gigabit interface

Ethernet interface with gigabit specification and security access

The CP has an Ethernet interface according to the gigabit standards IEEE 802.3. The Ethernet interface supports autocrossing, autonegotiation and autosensing.

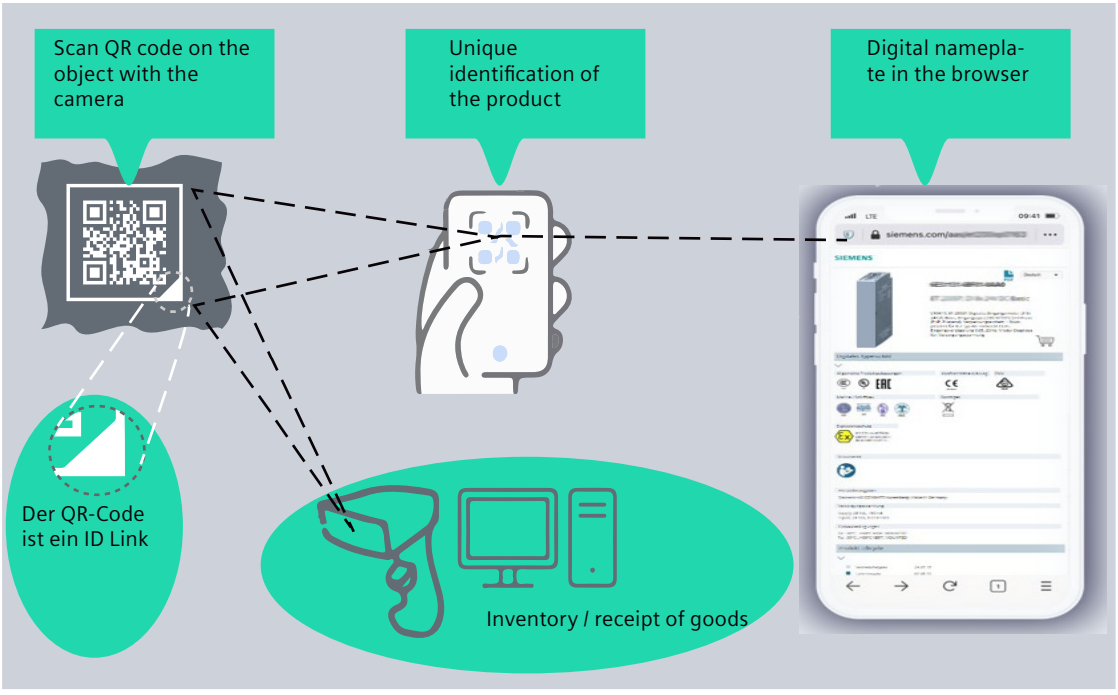
The Ethernet interface allows a secure connection to external networks via a firewall. The CP provides the following protective function:

- Protection of the S7-1500 station in which the CP is operated;
- Protection of the underlying company networks connected to the other interfaces of the S7-1500 station.

You will find the pin assignment of the sub RJ-45 jack in section Installing and commissioning the CP 1543-1 (Page 40).

2.3 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

Connection, mounting, commissioning, disassembly

3

3.1 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.

3.2 Important notes on using the device

Safety notices on the use of the device

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

3.2.1 Safety-extra low voltage + redundant power supply / without NEC

⚠ 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.

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

NOTICE

LAN attachment

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

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

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

3.2.2 Notes on use in hazardous areas

⚠ WARNING

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

⚠ WARNING

EXPLOSION HAZARD

Do not connect or disconnect cables to or from the device when a flammable or combustible atmosphere is present.

3.2.3 Notes on use in hazardous areas according to ATEX / IECEx

⚠ 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

At an ambient temperature of ≥ 60 °C, use heat-resistant cables designed for an ambient temperature at least 20 °C higher. The cable entries used on the housing must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB/T 3836.1.

WARNING

Transient overvoltages

Take measures to prevent transient overvoltages of more than 40% of the rated voltage (or more than 119 V). This is the case if you only operate devices with SELV (safety extra-low voltage).

3.2.4 Notes on use in hazardous areas according to UL HazLoc and FM

WARNING

The IP rating marking is not associated with the FM approvals certification.

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

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

WARNING

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

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

WARNING

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

⚠ WARNING

Wall mounting outside of the control cabinet or housing does not fulfill the requirements of the FM approval.

⚠ WARNING

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

⚠ WARNING

EXPLOSION HAZARD

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

3.3 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.

3.4 Installing and commissioning the CP 1543-1

Installation and commissioning

⚠ WARNING

Read the system manual "S7-1500 Automation System"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System" (for references to documentation, refer to Cybersecurity information (Page 7), Documentation guide.

Make sure that the power supply is turned off when installing/uninstalling the devices.

Configuration

Commissioning the CP fully is only possible if the STEP 7 project data is complete.

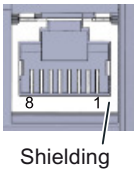
Procedure for installation and commissioning

Step	Execution	Notes and explanations
1	When installing and connecting up, keep to the procedures described for installing I/O modules in the system manual "S7-1500 Automation System".	
2	Connect the CP to Industrial Ethernet via the RJ45 jack.	Underside of the CP
3	Turn on the power supply.	
4	Close the front covers of the module and keep them closed during operation.	
5	The remaining steps in commissioning involve downloading the STEP 7 project data.	The STEP 7 project data of the CP is transferred when you download to the station. To load the station, connect the engineering station on which the project data is located to the Ethernet interface of the CPU. You will find more detailed information on loading in the following sections of the STEP 7 online help: • "Compiling and loading project data" • "Using online and diagnostics functions"

Ethernet interface

The table below shows the pin assignment of the Ethernet interface (RJ-45 jack). The assignment corresponds to the Ethernet standard IEEE 802.3.

Table 3-1 Pin assignment of the Ethernet interface

View	Pin	10/100 Mbps operation		10/100 Mbps or gigabit operation	
		Signal name	Pin assignment	Signal name	Pin assignment
	1	TD	Transmit Data +	D1+	D1 bidirectional +
	2	TD_N	Transmit Data -	D1-	D1 bidirectional -
	3	RD	Receive Data +	D2+	D2 bidirectional +
	4	GND	Ground	D3+	D3 bidirectional +
	5	GND	Ground	D3-	D3 bidirectional -
	6	RD_N	Receive Data -	D2-	D2 bidirectional -
	7	GND	Ground	D4+	D4 bidirectional +
	8	GND	Ground	D4-	D4 bidirectional -

You will find additional information on the topics of "Connecting up" and "Accessories (RJ-45 plug)" in the system manual:
Link: (https://support.industry.siemens.com/cs/ww/en/view/59191792)

3.5 Operating mode of the CPU: Reaction of the CP

Switching the CPU: RUN → STOP

You can switch the operating mode of the CPU between RUN and STOP via STEP 7.

Note

RUN/STOP LED of the CP

The green RUN/STOP LED of the CP continues to be lit green regardless of the STOP mode of the CPU.

In the STOP state of the CPU, the CP remains in RUN.

The following behavior applies to the CP:

- This applies to established connections (S7, ISO Transport, ISO-on-TCP, TCP, UDP):
  - Programmed connections are terminated.
  - Configured connections are retained.
- The following functions remain enabled:
  - Configuration and diagnostics of the CP
    System connections for configuration, diagnostics and PG channel routing are retained.
  - Web diagnostics
  - S7 routing function
  - Time-of-day synchronization

Configuration, program blocks

4

4.1 Security recommendations

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

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area. For more information, refer to section Intended operational environment (Page 15).
  Connections over unsecured network areas must be secured by security mechanisms such as VPN.
- Check regularly for new features on the Siemens Internet pages.
  - You can find information on Industrial Security here:
    Link: (http://www.siemens.com/industrialsecurity)
  - You can find information on security in industrial communication here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)
- Keep the firmware up to date. Check regularly for security updates for the firmware and use them.
  Information regarding product news and new firmware versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15340/dl)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the PC directly to the Internet. If a connection from the CP to the Internet is required, enable the security functions or arrange for suitable protection before the CP, for example a SCALANCE S / 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 access to the CPU under "Protection & Security".
- Security function of the communication
  - Enable the security functions of the CP and set up the firewall.
    If you connect to public networks, you should use the firewall. Think about the services you want to allow access to the station via public networks. By limiting the transmission speed in the firewall rules, you can restrict the possibility of flooding and DoS attacks. The FETCH/WRITE functionality allows you to access any data of the CPU. The FETCH/WRITE functionality should not be used in conjunction with public networks.
  - Use the secure protocol variants HTTPS, FTPS, NTP (secure) and SNMPv3.
  - Use the program blocks for secure OUC communication (Secure OUC).
  - Leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CP disabled.
- Protection of the passwords for access to program blocks
  Protect the passwords stored in data blocks for the program blocks from being viewed. You will find information on the procedure in the STEP 7 information system under the keyword "Know-how protection".
- Logging function
  Enable the function in the security configuration and check the logged events regularly for unauthorized access.

You can find the ciphers used by the CP in the appendix Encryption methods (Ciphers) used by the module (Page 113).

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel. See also the preceding section for information on this.
- Do not use one password for different users and systems.

Protocols

Secure and non-secure protocols

- Only activate protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.
- Deactivate DHCP at interfaces to public networks such as the Internet, for example, to prevent IP spoofing.

Note that, for example, the e-mail function uses a non-secure protocol via the "TMAIL_C" program block.

Table: Meaning of the column titles and entries

The following table provides you with an overview of the open ports on this device.

- **Protocol / function**
  Protocols that the device supports.
- **Port number (protocol)**
  Port number assigned to the protocol.
- **Default of the port**
  - Open
    The port is open at the start of the configuration.
  - Closed
    The port is closed at the start of the configuration.
- **Port status**
  - Open
    The port is always open and cannot be closed.
  - Open after configuration
    The port is open if it has been configured.
  - Open (login, when configured)
    As default the port is open. After this port is configured, the communications partner needs to log in.
  - Open with block call
    The port is only opened when a suitable program block is called.
- **Authentication**
  Specifies whether or not the protocol authenticates the communications partner during access.

Table 4-1 Server ports

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
S7 and online connections	102 (TCP)	Open	Open *	No
Online security diagnostics	8448 (TCP)	Closed	Open after configuration	No
HTTP	80 (TCP)	Closed	Open after configuration	No
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
FTP	20 (TCP) 21 (TCP)	Closed	Open after configuration	No
FTPS	20 (TCP) 21 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)
IPsec	500 (TCP) 4500 (UDP)	Closed	Open after configuration	Yes
Communication via SINEMA RC	443 (TCP), 5243 (UDP)	Closed	Open after configuration	Yes
Modbus	502 (TCP)	Closed	Open after configuration	No

***** For information on avoiding opening port 102 during diagnostics, see section Online security diagnostics via port 8448 of the CP (Page 93).

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 security modules.

These can be:

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- FTPS / 20, 21 (TCP)
- SMTP / 25 (TCP) - Open in CP on block call (outgoing only)
- SMTPS / 587 (TCP) - Open in CP on block call (outgoing only)
- SNMP / 161, 162 (UDP)
- IPSec / 500 (TCP) / 4500 (UDP)
- SINEMA RC Autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC
- Syslog / 514 (UDP)

4.2 Settings

FETCH/WRITE

You can use the FETCH/WRITE services to access system memory areas of the S7-CPU.

- FETCH: Read data directly
- WRITE: Write data directly

Access is possible from the following devices:

- SIMATIC S5
- SIMATIC PC stations
- Non-SIMATIC devices

The S7-1500 CP is the server for FETCH/WRITE services.

The FETCH/WRITE services are supported by the following protocols:

- TCP
- ISO-on-TCP
- ISO transport

A configured connection is not required for using the FETCH/WRITE services.

Requirements in the CPU configuration

You need to enable the FETCH/WRITE communication service in the CPU configuration, refer to section PUT/GET/FETCH/WRITE: Restrictions in the CPU (Page 48).

System memory

You can access the following operand areas in the system memory of the S7-1500 CPU using FETCH or WRITE:

- Data blocks (DB)
  Note the following:
  - With access to DBs, the highest DB no. is 255.
  - Activate the "S7 addressing" parameter in the TSAP table of the CP for access of S5 or S7 partners.
- Bit memory (M)

Link to non-SIMATIC systems

The FETCH/WRITE services can be used from non-Siemens devices to access S7 system memory areas.

To be able to use this type of access also for PC applications, for example, you need to know the PDU structure of the jobs. Refer to the appendix Linking to other systems with FETCH/WRITE (Page 111).

UDP frame buffering

Disables the buffering of UDP datagrams in order to protect the module from possible overload.

When buffering is disabled, all received UDP datagrams that are not fetched by the user program within one cycle are discarded.

4.3 PUT/GET/FETCH/WRITE: Restrictions in the CPU

Communications services without connections

The CPU can be a server for a series of communications services without connections being configured for the CPU. Other communications partners can access CPU data. This means that it is no longer possible for the local CPU to control communication with the clients.

You need to grant permission for these communications services at the following location in the CPU configuration:

- Parameter group "Protection & Security > Connection mechanisms"
  Enable the option "Permit access with PUT/GET communication from remote partner".

A prerequisite for enabling this option is enabling an access option in the "Access control > Access level" parameter group. Set the option "Read access" or "Full access".
Note: This setting is connected with security restrictions.

When the "No access (complete protection)" option is enabled, PUT/GET communication cannot be enabled.

"Permit access with PUT/GET communication from remote partner"

Parameter group "Protection & Security > Connection mechanisms" > option "Permit access with PUT/GET communication from remote partner"

The activation of communication services described below applies to the use of the communications module together with a CPU V2.x to V3.0.

- Option enabled
  - Access to CPU data from the client side via the communications module using PUT/GET or FETCH/WRITE is possible.
- Option disabled
  - Access to CPU data from the client side via the communications module using PUT/GET or FETCH/WRITE is not possible.
  - FTP access via the CP is possible.

  Read and write access to CPU data is only possible with communication connections that require configuration or programming both for the local CPU and for the communications partner.
  Connections for which the local CPU is only a server (no configuration/programming of communication with the partner) are not possible.

Configuring PUT/GET

You can find additional information on the following Siemens Industry Customer Support page and in the documentation specified in the "Download" section:
Link: (https://support.industry.siemens.com/cs/ww/en/view/82212115)

4.4 Network settings

Automatic setting

The Ethernet interface of the CPU is set permanently to autosensing.

Note

In normal situations, the basic setting ensures troublefree communication.

Autocrossing mechanism

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

Note

Connecting a switch

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

4.5 IP configuration

4.5.1 Points to note about IP configuration

Configured S7 and OUC connections cannot be operated if the IP address is assigned using DHCP

Note

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

IP address band 169.254.0.0/16 not permissible

Note

If you configure an IP address from the 169.254.0.0/16 band for the CP or this is assigned by a DHCP server, the CP is not reachable.

DHCP: Aborting ISO transport connections

Note

When the IP address is obtained via DHCP, the CP aborts all ISO transport connections if the IP address of the CP is not renewed by the DHCP server, for example in the event of a temporary server failure.

4.5.2 IPv6 addresses

No Link-Local addresses

For communication via IPv6, the CP needs an IPv6 address that you configure yourself or that is obtained via DHCP.

Do not use a Link-Local address (fe80::/16) for the CP interface or for the communication partner. Frames from and to Link-Local addresses are not forwarded by routers.

This applies to all protocols and services supported by the CP.

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

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

Behavior when the CP starts up

If double addressing is detected when the CP starts up, the CP changes to RUN and cannot be reached via the Ethernet interface. The ERROR LED flashes.

4.5.4 IP routing

IP routing via the backplane bus

The function enables static IPv4 routing between communications modules in a rack via the backplane bus. This means that routing between two subnets that are connected via two communications modules of the station is operated via the backplane bus of the station.

The function is supported by the following modules:

- CP 1545-1
- CM 1542-1
  As of firmware version V2.0
- CP 1543-1
  - As of firmware version V2.0 with disabled security functions
  - As of firmware version V2.1 with enabled security functions

You can use IP routing, for example, for Web server access by lower-level modules.

With IP routing, the data throughput is limited to 1 Mbps. Remember this in terms of the number of modules involved and the expected data traffic via the backplane bus.

Restrictions

IPv4 routing via the communications module into the CPU of the station is not possible.

Configuration

You reach the function in STEP 7 via:
"Ethernet interface > Ethernet addresses > IP routing between communication modules"

IP routing must be activated in at least 2 modules of a station.

Please note:
If you wish to use IP routing, you can only configure a router for one communications module in the station.

When the security function is activated, additional IP firewall rules are created, which you can modify in advanced firewall mode of the Global Security settings.

4.5.5 Virtual interface of the CPU

The CP 1543-1 supports the virtual interface of the CPU.

Requirement

The following requirements must be met to use the virtual interface of the CPU:

- S7-1500 CPU firmware V2.8 or higher
  R/H CPUs support the function as of firmware version V3.1.
- CP 1543-1
  - As of CP firmware version V2.2 with disabled security functions of the CP
  - As of CP firmware version V3.0 also with enabled security functions of the CP
- Configurability
  - As of STEP 7 V16 with CP firmware V2.2
  - As of STEP 7 V17 with CP firmware V3.0

Virtual interface of the CPU

As of firmware version V2.8, the S7-1500 CPU offers the option of reaching its IP-based applications, such as OPC UA client and server, not only via its local PROFINET interfaces, but also via the interface of a CP 1543-1 in the same station.

The virtual interface is called W1.

Features of the virtual interface

The virtual interface is not a fully diagnosable interface with the familiar properties of conventional interfaces. The virtual interface is not displayed in the graphical views, because the internal connection via the backplane bus does not represent an S7 subnet and does not have any ports. A physical connection by means of a network cable therefore cannot be established.

The following IP-based services can also be reached via the virtual interface:

- OPC UA (client and server)
- Programmed OUC connections
- S7 communication: ES/HMI access and instructions for S7 communication such as PUT/GET

The IP address of the virtual interface is displayed in STEP 7 and in the display of the CPU.

The activated interface can be used in the configuration of the communication partners.

For information on the restrictions of the virtual interface as compared to physical interfaces, see the STEP 7 information system.

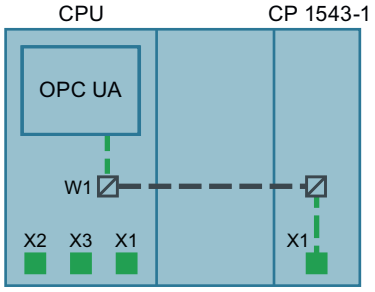


Figure 4-1 Principle of the virtual interface

Configuration of the virtual interface W1

The virtual interface of the CPU is configured in STEP 7 in the parameter group "Advanced configuration > Access to PLC via communication module".

Here, the virtual interface is assigned to a CP of the station, via which external access to the CPU can take place. The configured CPs of the station can be selected in the drop-down list.

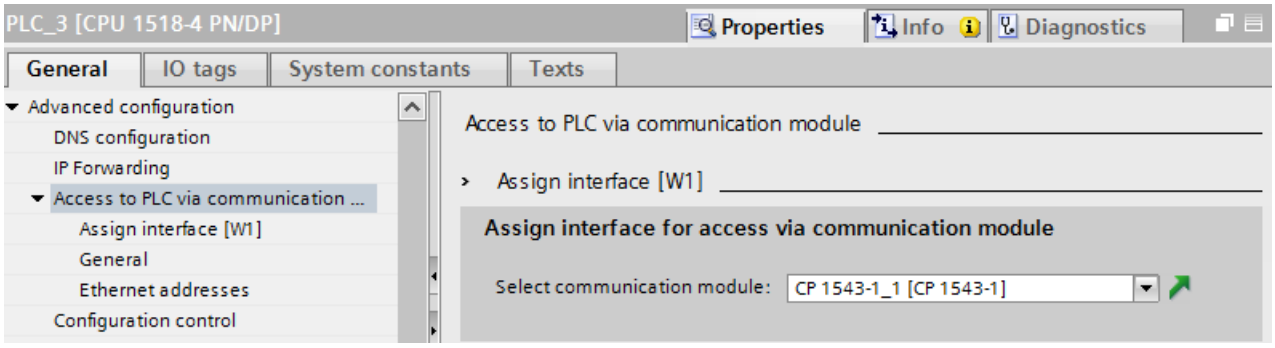


Figure 4-2 Selecting the CP in the CPU properties

After selecting the CP, configure the IP and PROFINET parameters of the virtual interface.

Observe the following rules:

- The IP address of the virtual interface and the IP addresses of the PROFINET interfaces of the CPU must be in different, disjointed address bands.
- The IP address of the virtual interface must be in the subnet of the Ethernet interface so that the services of the CP can be reached from the CPU and vice versa.

After loading the configuration data, the CPU services such as the OPC UA server can be reached via the CP and the virtual interface.

The IP address of the virtual interface is shown in the list of server addresses in the properties dialog of the OPC UA server of the CPU. Created connections and S7 communication (e.g. HMI and BSEND, BRCV) run over this interface.

The IP address of the virtual interface W1 is not listed under the currently displayed local interfaces (Xn) in the device display, but under "Addresses" in the "Settings" section. The virtual interface is also visible when no CP is plugged or when the virtual interface is deactivated. If there is no IP configuration, the IP address and subnet mask are shown with 0.0.0.0.

The virtual interface W1 is displayed in the diagnostics view under "Online & Diagnostics".

The hardware ID of the virtual interface is displayed in the system constants in the CPU properties.

Note

Address change during runtime and restart

When the IP parameters of the virtual interface are loaded, you can then change them via the display of the CPU, via T_CONFIG or online.

However, note that the originally loaded configuration will be active again after a restart of the CPU.

Configuration changes

A change of the assigned CP may have an effect on the configuration of the virtual interface:

- Changes in the configuration
  - Assignment of a different CP
    The configuration is used for the new CP.
  - Deselect the assigned CP
    The virtual interface W1 is deactivated and the configuration is lost.
    When a CP is assigned again, you need to configure the virtual interface again.
- Changes to the station configuration
  - Move the CP
    If the CP is only moved to another slot of the device, the configuration remains valid.
  - Removing the CP
    If the CP is removed from the station, the configuration is retained in the CPU.
    In the drop-down list of the parameter group of the CPU, the CP is displayed as missing and compiling the configuration indicates an error. The missing CP can be deselected or assigned to another CP.

Security settings of the CP

Via the CP-internal firewall, you can protect data traffic via the virtual interface of the CPU for the following services:

- HTTPS
- OPC UA client/server

For connections via the W1 virtual interface, you can use the Layer 2 firewall of the CP. The CP "AX10" also supports the Layer 3 firewall for the W1 virtual interface of the CPU.

Access to the W1 virtual interface cannot be secured with a VPN tunnel.

You will find the options in the parameter group "Security > Firewall".

4.5.6 Programmed connections: Restriction of firewall rules

Restrictions with programmed connections and configured security functions

In principle, it is possible to set up communications connections program-controlled using the program block TCON and at the same time by configuring the firewall.

Note

Partner IP addresses not in firewall rules

When configuring specified connections (active endpoints) in STEP 7, the IP addresses of the partners are not entered automatically in the firewall configuration.

4.6 Configuration in the redundant R/H system

The CP in the redundant R/H system

The CP as of firmware version V3.0 supports use in the redundant S7-1500 R/H system.

Configuration

To integrate the CP fully in the redundancy functionality of the system, you need to observe the following configuration steps, among others:

- Assign the W1 virtual interface to the respective CP for the CPU:
  ("Advanced configuration > Access to PLC via communications module")
- Activate and configure the system IP address for switched communication and the virtual MAC address on the CPU.
  The CPs then communicate via the W1 virtual interface and the system IP address.
  The W1 virtual interface is specified as destination address on the communications partners of the CPs.

These are only two important points from the complete scope of required configuration steps for integrating the CP in the redundant system.

Further information

You can find more detailed information on requirements, configurations, design (e.g. U-connector or active backplane bus) and engineering in the following manuals:

- SIMATIC
  S7-1500
  S7-1500R/H redundant system
  System manual
  Link: (https://support.industry.siemens.com/cs/ww/en/view/109754833)
- SIMATIC
  S7-1500 / S7-1500H / ET 200MP
  Active backplane bus
  Equipment manual
  Link: (https://support.industry.siemens.com/cs/ww/en/view/109778694)

4.7 Time-of-day synchronization

Note

Recommendation for setting the time

Synchronization with a external clock at intervals of approximately 10 seconds is recommended. This achieves as small a deviation as possible between the internal time and the absolute time.

Note

Ensuring a valid time of day

If you use security functions, a valid time of day is required. If you do not obtain the time-of-day from the station (CPU), we therefore recommend that you use the NTP (secure) method.

Synchronization method

If the security functions are disabled, the CP supports the NTP synchronization method (Network Time Protocol).

If the security functions are enabled, the CP supports the following methods:

- NTP
  NTP with support of RFC5905
- NTP (secure)
  NTP with support of RFC5905 and RFC5906 with shared key
  In the extended NTP configuration, you can create and manage additional NTP servers.

For more information on configuration, refer to the STEP 7 online help.

If you use the program block "T_CONFIG" together with the "SDT CONF_DATA" for assigning the parameters of NTP servers, you can use four additional NTP servers.

Diagnostics

You can query the current time of the module and the time source with the "Online & Diagnostics" TIA functions.

4.8 DNS configuration

DNS server

A DNS server may be required when the module itself, a communications partner, or for example an FTP server should be reachable via the host name (FQDN). If you specify the address of a device as FQDN, you need to configure a DNS server. In this case, the IP address of the device is determined via the configured DNS server.

Max. 3 DNS servers can be configured for the CP. The 4th configured DNS server is not evaluated.

4.9 Communication with the CPU

4.9.1 CP diagnostics

CP diagnostics

Using the CP diagnostics, you can save the states of some functions of the CPU and the CP in variables for the CPU and use them for other evaluations and diagnostic purposes.

The smallest cycle for updating the diagnostics data is 1 second.

- Enable advanced CP diagnostics
  Enabling the option allows use of the following diagnostic functions.
  If the option is enabled, the "Diagnostics trigger tag" must be configured.
- Diagnostics trigger tag
  If the user program of the CPU sets the "Diagnostics trigger tag" (BOOL) to 1, the CP updates the values of the configured variables for advanced diagnostics.
  After writing the current values to the variables for advanced diagnostics, the CP sets the "Diagnostics trigger tag" to 0, signaling to the CPU that the updated values can be read from the variables.

General

- CPU load
  The variable (Byte) specifies the CPU processor load as a percentage.
- Memory Resources
  The variable (Byte) specifies the utilization of the CP work memory (RAM) as a percentage.
- Current IP address
  Variable (data type String) for the current IP address of the CP.
  The string for the IP address must have a length of 254 bytes. Configure the data type in the data block as follows: String[254]

Security

The meaningful use of the options depends on the utilized security functions of the CP.

- VPN IPsec status
  The variable (data type Bool) is set to 1 when a VPN tunnel is established.
  Value = 0 if no VPN tunnel is established.
- Connection to SINEMA Remote Connect
  The variable (data type Bool) is set to 1 when a connection to SINEMA Remote Connect Server is established.
  Value = 0 if no connection is established.

4.10 FTP communication

FTPS access only with security functions enabled

FTPS access to the S7-1500 station as an FTP server is only possible if a user with suitable rights has been created in the STEP 7 project. This means that the security functions must be enabled on the CP. For this, security settings are available in the global user administration.

4.10.1 FTP server

4.10.1.1 Configuring the FTP server function

CP configuration

Configure the FTP server function of the CP in the following parameter group.

- With security functions disabled: "FTP server configuration"
- With security functions enabled: "Security > FTP server configuration"

Requirements in the CPU configuration and programming

Use the following settings to allow FTP access:

- In the CPU configuration in "Protection & Security > Connection mechanisms": Disable the option "Access via PUT/GET communication...".
- As file DBs create data blocks of the type "Array of byte".

Only for CP 1543-1 with firmware version ≤ V2.0:

- For all data blocks being used as file DBs, disable the "Optimized block access" attribute.

S7-1500 CP as FTP server

The functionality described here allows you to transfer data in the form of files to or from an S7-1500 station using FTP commands. At the same time, the conventional FTP commands for reading, writing and managing files can also be used.

Access to the following data of the S7-1500 is possible:

- **RAM of the CP**
  Name of the directory:
  /ram
- **Data blocks of the CPU**
  Name of the directory:
  /cpu1 / DBx
  "DBx" is the name of the relevant data block e.g. DB10.
- **SIMATIC memory card of the CPU**
  The function is supported as of the following firmware versions:
  - CPU: V2.0
  - CP 1543-1: V2.0
  - CP 1545-1: V1.0

  Name of the directory:
  /mmc_cpu1
  Access to the following folders of the SIMATIC memory card is possible:
  - /DATALOGS
    Directory for log files
  - /RECIPES
    Directory for recipe files

Note

FTP access to the SIMATIC memory card of the CPU: CPU STOP possible

Note that the cards have a limited capacity. If the memory space of the SIMATIC memory card is completely occupied due to storage of large amounts of data, the CPU changes to STOP.

- Use a card with adequate storage capacity.
- Avoid writing large amounts of data often to the SIMATIC memory card using FTP.

Reading/writing via DBs of the CPU

To transfer data with FTP via data blocks, create the required DBs in the CPU. Due to their special structure, these are known as file DBs.

When it receives an FTP command, the CP acting as FTP server queries its assignment table to find out how the data blocks used for file transfer in the CPU will be mapped to files. You make the data block assignment in the STEP 7 configuration of the CP (FTP configuration).

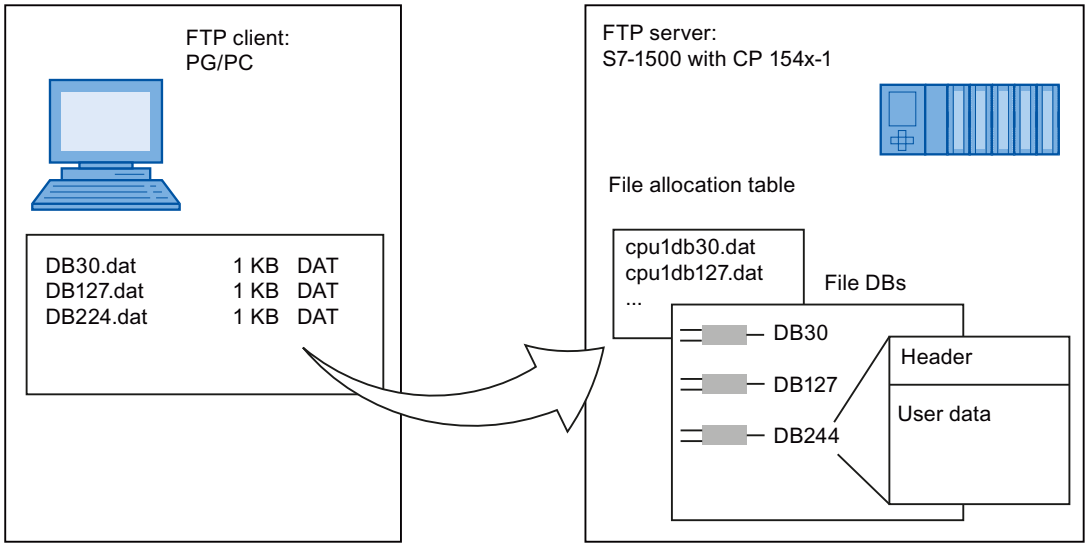


Figure 4-3 S7-CPU with CP 154x-1 as FTP server for the S7 CPU data

DB assignment in STEP 7

The fields of the table in the data block assignment in STEP 7 have the following meaning and syntax:

Column title	CPU	DB	File name	Comment
Meaning	Assignment of the CPU Selectable from drop-down list	No. of the data block (file DB) Selectable from drop-down list	The file name assigned to the file DB Automatic name proposal; entry can editable.	Informal comment
Example	cpu1 [PLC_1]	20	cpu1_db20.dat	Measured values plant 1

Notes on the syntax

The following applies to the file name of a file DB:

- The file name begins with "cpuX" (where X=1 for S7-1500).

  Note

  Keep to the notation (lower case for "cpu" and no leading spaces at the start of the row). Otherwise, the files will not be recognized.

- Length: maximum 64 characters (including "cpuX")

4.10.2 FTP client

4.10.2.1 The program block FTP_CMD (FTP client function)

FTP_CMD

Using the FTP_CMD instruction, you can establish FTP connections and transfer files from and to an FTP server.

Data transfer is possible using FTP or FTPS (secure SSL connections).

You will find the block in STEP 7 in the "Instructions" task card under "Communication > Communications processor > SIMATIC NET CP" when the Main [OB1] is open.

Note

Block versions

You can use the version V2.x of FTP_CMD in a station only in conjunction with a CPU and a CP V2.x V2.x.

As soon as the station obtains a CPU V1.x or CP V1.x, you must use FTP_CMD in the older version V1.x (e.g. V1.4). To do this, change the version of the "SIMATIC NET CP" library to V3.4. You can then select an older version of the block.

The table below shows the compatibility.

Table 4-2 Compatibility of the block FTP_CMD with versions of the CPU and CP

FTP_CMD	CPU	CP 1543-1
V1.5	V1.x	Any
V1.5	Any	V1.x
V2.0	V2.x	V2.x

Data transfer is possible using FTP or FTPS (secure SSL connections).

Note

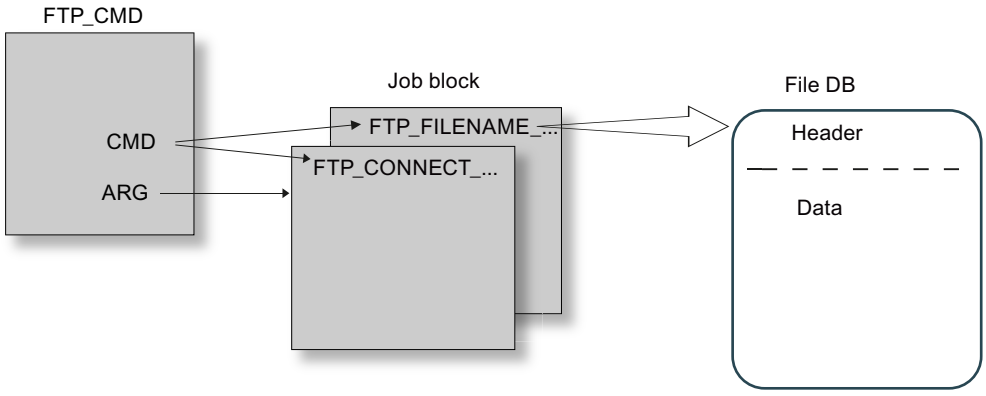
FTPS: Comparing certificates

FTPS requires a comparison of the certificates between FTP server and FTP client. If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server. Import the certificate of the FTP server as a trusted certificate in the certificate manager.

How it works

The FTP_CMD instruction references a job block (ARG) in which the FTP command is specified. Depending on the type of FTP command (CMD), this job block uses different data structures for parameter assignment. Suitable data types (UDTs) are available for these various structures.

The following diagram shows the call structure:



Job blocks (UDTs)

The following data structures are used for the job blocks:

- Connection establishment
  Various data structures are available for the connection establishment using the following types of access:
  - FTP_CONNECT_IPV4: Connection establishment with IP addresses according to IPv4
  - FTP_CONNECT_IPV6: Connection establishment with IP addresses according to IPv6
  - FTP_CONNECT_NAME: Connection establishment with server name (DNS)
- Data transfer
  For the data transfer, two different data structures are available:
  - FTP_FILENAME: Data structure for access to a complete file
  - FTP_FILENAME_PART: Data structure for read access to a data area

Data transfer in the File_DB

The data transfer is achieved using data blocks containing a header for job data and the area for the user data. The data block is specified in the job buffer.

You will find the description of an example file DB in the STEP 7 information system.

Requirements in the CPU configuration

Use the following settings to allow FTP access:

- For all data blocks being used as file DBs, disable the "Optimized block access" attribute.
- Only when using a CPU V1.x and a CP V1.1.x:
  Enable the "Access via PUT/GET communication..." option in the configuration data of the CPU under "Protection & Security" (PUT/GET must be released).

4.10.2.2 Input parameter - FTP_CMD

Explanation of the input parameters

You supply the FTP_CMD instruction with the following input parameters:

Table 4-3 Formal parameters of the FTP_CMD instruction - input parameters

Parameter	Declaration	Data type	Memory area	Meaning / remarks
REQ	Input	BOOL	E, A, M, DB, L	Starts the send job on a rising edge.
ID *	INPUT	INT	1, 2 ... 64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
CMD *	INPUT	BYTE	See following table "Commands".	FTP command to be executed when the instruction is called. You will find value ranges for the FTP command types after the table. The FTP command specified here must be specified identically in the job block (ARG parameter). If a command is not supported by the CP firmware, an error message with STATUS = $8F6B_H$ is output.
ARG *	INPUT	VARIANT	See following table "Commands".	Job block References the data area with the execution parameters suitable for the FTP command. Specific data types (UDT) are used depending on the FTP command. The UDTs are shown below. The ANY data type is not permitted for the pointer to be specified here!

***** The values of the input parameters "ID" and "CMD" overwrite the value of the input parameter "ARG".

FTP commands in the "CMD" parameter

The following table shows you the significance of the commands of the "CMD" parameter and which UDTs you use to supply the job blocks.

Table 4-4 Command types

CMD (command type)	Relevant job blocks / UDT	Meaning / handling
0 (NOOP)	*	The called FB does not execute any actions. The status codes are set as follows when these parameters are supplied: DONE=1; ERROR=0; STATUS=0
1 (CONNECT)	FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME	FTP connection establishment With this command, the FTP client establishes an FTP connection to an FTP server (port 21). The connection is available under the connection ID specified here for all further FTP commands. Data is then exchanged with the FTP server specified for this user.
2 (STORE)	FTP_FILENAME	This function call transfers a data block (file DB) from the FTP client (S7-CPU) to the FTP server. Caution: If the file (file DB) already exists on the FTP server, it will be overwritten.
3 (RETRIEVE)	FTP_FILENAME	This function call transfers a file from the FTP server to the FTP client (S7-CPU). Caution: If the data block (file DB) on the FTP client already contains a file, it will be overwritten.
4 (DELETE)	FTP_FILENAME	With this function call, you delete a file on the FTP server.
5 (QUIT)	*	With this function call, you close the FTP connection specified in "ID".
6 (APPEND)	FTP_FILENAME	Similar to "STORE", the "APPEND" command saves a file on the FTP server. With "APPEND", the file on the FTP server is, however, not overwritten. The new content is appended to the existing file. If the file (file DB) does not exist on the FTP server, it will be created.
7 (RETR_PART)	FTP_FILENAME_PART	Using the "RETR_PART" command (retrieve part) , you can request a section of a file from the FTP server. If very large files are involved, this allows you to restrict the read to the part you currently require. To do this, you need to know the structure of the file. Enter the required part of the file using the two parameters "OFFSET" and "LEN" in FB40.

***** With the command types 0 (NOOP) and 5 (QUIT) a freely selectable job block (UDT) must be specified. This is not evaluated.

4.10.2.3 Job blocks for FTP_CMD

Meaning

You supply the FTP_CMD instruction with a job block using the ARG parameter. The structure depends on the FTP command type. By using the default data types (UDT), the instruction recognizes the type of the job block. Below, you will find the relevant data types (UDTs) for the following job blocks:

- FTP connection establishment with IP address according to IPv4
- FTP connection establishment with IP address according to IPv6
- FTP connection establishment with server name
- Write and read access and other FTP commands
- FTP command RETR_PART

Job block for FTP connection establishment with IP address according to IPv4

For FTP connection establishment with IP address according to IPv4, the following data structure is used.

Table 4-5 FTP_CONNECT_IPV4

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPCmd	BYTE	1	FTP command "CONNECT" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 63). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.
UserName	STRING[32]	'benutzer'	User name for the login on the FTP server

Parameter	Type	Range of values	Meaning / remarks
Password	STRING[32]	'passwort'	Password for the login on the FTP server
FTPserverIPaddr	IP_V4	ADDR(1) ... ADDR(4)	IP address of the FTP server as Array[1..4] of Byte, where 1 byte specifies one block of the address. Example: ADDR(1) specifies the first address block (the first byte of the address).

Job block for FTP connection establishment with IP address according to IPv6

For FTP connection establishment with IP address according to IPv6, the following data structure is used.

Table 4-6 FTP_CONNECT_IPV6

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPCmd	BYTE	1	FTP command "CONNECT" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 63). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.
UserName	STRING[32]	'user'	User name for the login on the FTP server
Password	STRING[32]	'password'	Password for the login on the FTP server
FTPserverIPaddr	IP_V6	ADDR(1) ... ADDR(16)	IP address of the FTP server as Array[1..16] of Byte, where 2 bytes specify one block of the address. Example: ADDR(1) + ADDR(2) specify the first address block.

Job block for FTP connection establishment with server name

For FTP connection establishment specifying the server name, the following data structure is used. The server name is assigned to an IP address using DNS.

Table 4-7 FTP_CONNECT_NAME

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPcmd	BYTE	1	FTP command "CONNECT" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 63). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.
UserName	STRING[32]	'benutzer'	User name for the login on the FTP server
Password	STRING[32]	'passwort'	Password for the login on the FTP server
FTPserverName	STRING[254]		IP address of the FTP server

Job block for write and read access and other FTP commands

The following data structure is used for the FTP commands store, retrieve, delete and append.

Table 4-8 FTP_FILENAME

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment

Parameter	Type	Range of values	Meaning / remarks
FTPcmd	BYTE	2, 3, 4, 6	FTP command "STORE / RETRIEVE / DELETE / APPEND" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 63). Note: The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.
DataBlockNumber	UINT		The data block specified here contains the file DB to be read / written.
LenFilename	UINT	0...1000	The "LenFilename" parameter for specifying the total length of the file name is not evaluated. Instead, the length information in the string of the "Filename" parameter is evaluated.
Filename	ARRAY[0..3] OF STRING[254]		File name of the destination or source file. The four strings for the file name are concatenated and transferred to the server as a complete string.

Job block for the RETR_PART FTP command

The following data structure is used for the RETR_PART FTP command.

Table 4-9 FTP_FILENAME_PART

Parameter	Type	Range of values	Meaning / remarks
InterfaceID	HW_ANY		Module start address When you call an instruction, you transfer the module start address of the CP in the LADDR parameter. You will find the module start address of the CP in the configuration of the CP under: "Properties>Addresses>Inputs"
ID	CONN_OUC	1, 2...64	The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.
ConnectionType	BYTE	0	Connection type "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = active connection establishment
FTPcmd	BYTE	7	FTP command "RETR_PART" FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 63). The FTP command specified here must be specified identically in the CMD input parameter.
CertIndex	BYTE	0 = FTP 1 = FTPS	Here, choose between the protocol types FTP or FTPS. Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.

Parameter	Type	Range of values	Meaning / remarks
Offset	DWORD		Offset in bytes starting at which the file will be read.
Length	DWORD		Sublength in bytes that is read starting at the value specified in "OFFSET". Special features: • If "DW#16#FFFFFFFF" is specified, the available rest of the file will be read. Result OK (DONE = 1, STATUS = 0) if no other error occurred. • When OFFSET > length of the original file: Length of the destination file (ACT_LENGTH in file DB): 0 bytes on the CPU. Result OK (DONE = 1, STATUS = 0) if no other error occurred. • When OFFSET + LEN > length of the original file (and LEN ≠ 0xFFFFFFFF): Length of the destination file (ACT_LENGTH in file DB): Available bytes starting at "OFFSET". Result OK (DONE = 1, STATUS = 0) if no other error occurred.
DataBlockNumber	UINT		The data block specified here contains the file DB to be read / written.
LenFilename	UINT	0...1000	The "LenFilename" parameter for specifying the total length of the file name is not evaluated. Instead, the length information in the string of the "Filename" parameter is evaluated.
Filename	ARRAY[0..3] OF STRING[254]		File name of the destination or source file. The four strings for the file name are concatenated and transferred to the server as a complete string.

Parameter supply for command types NOOP and QUIT

Supply the FTP_CMD with a reference to a job block with the following command types as well:

CMD = 0 (NOOP)

CMD = 5 (QUIT)

The content of the job block is not evaluated when these command types execute, the type (UDT) of the specified job block is therefore unimportant.

Note

Response if the reference to the FTP job block is missing

If this reference is not supplied, the command is not executed. The instruction remains blocked in an apparent execution status without any feedback to the user program on the interface.

4.10.2.4 Output parameters and status information FTP_CMD

Parameters BUSY, DONE and ERROR

You control the execution status with the parameters BUSY, DONE, ERROR and STATUS. The BUSY parameter indicates the processing status. With the DONE parameter, you check whether or not a job was correctly executed. The ERROR parameter is set if errors occur during execution of "FTP_CMD". Error information is output in the STATUS parameter.

The following table shows the relationship between the parameters BUSY, DONE and ERROR:

BUSY	DONE	ERROR	Description
1	-	-	The job is being processed.
0	1	0	The job was completed successfully.
0	0	1	The job was terminated with an error. The cause of the error is specified in the STATUS parameter.
0	0	0	No new job was assigned.

Evaluating status codes

Note

Evaluation

- Evaluation for BUSY = 0
  Do not evaluate the status displays until BUSY = 0.
- Status $8Fxx_H$
  For entries coded with status $8Fxx_H$, refer to the information in the STEP 7 Standard and System Functions reference manual. The chapter describing error evaluation with the RET_VAL output parameter contains detailed information.

Table 4-10 FTP_CMD: Meaning of the STATUS parameter in conjunction with DONE and ERROR

DONE	ERROR	STATUS	Meaning
0	0	0000_H	No job is being executed.
1	0	0000_H	the job was completed without error.
0	0	7001_H	The job was initiated for the first time.
0	0	7002_H	Job still running.
0	1	$80C4_H$	Communication error (occurs temporarily, it is usually best to repeat the job in the user program).
0	1	8183_H	The configuration does not match the job parameters.
0	1	8401_H	Unknown error Possible causes: • A timeout was detected on the connection. • The FTP server has aborted the connection. Remedy: Send the QUIT and CONNECT commands again to re-establish the connection.

DONE	ERROR	STATUS	Meaning
0	1	8402_H	The connection has an error status. The timeout of the connection may have been exceeded or the FTP server may have terminated the connection. Remedy: Send the QUIT and CONNECT commands to re-establish the connection.
0	1	8403_H	Login has failed.
0	1	8404_H	FTP server is not obtainable.
0	1	8405_H	Transfer has failed.
0	1	8406_H	Timeout for current action
0	1	8407_H	File was not found on the FTP server.
0	1	8408_H	Transfer not possible.
0	1	8409_H	File could not be fetched.
0	1	8410_H	Setting the TCP port for the data connection has failed.
0	1	8411_H	Offset information does not match.
0	1	8412_H	Error changing the specified directory
0	1	8413_H	Error receiving data
0	1	8414_H	Error sending data
0	1	8415_H	Specified CMD (command type) was rejected by the client.
0	1	8416_H	Connection was closed by the FTP server.
0	1	8418_H	Error in the user data. Possible causes: • File name is empty. • Data length is "0". • etc.
0	1	8419_H	There is no socket resource available to open a data connection.
0	1	8420_H	There is no socket resource available to open a control connection.
0	1	8421_H	Error opening the file DB to be read
0	1	8422_H	Error opening the file DB to be written
0	1	8423_H	Connection establishment to the FTP server has failed.
0	1	8424_H	Internal error
0	1	8425_H	Format error in the domain name
0	1	8426_H	There are too many DNS queries pending.
0	1	8427_H	The specified DNS server could not assign the specified domain name.
0	1	8428_H	There is no connection resource available.
0	1	8429_H	Unknown channel ID
0	1	8430_H	The file DB is too short.
0	1	8431_H	Error when writing to the file DB.
0	1	8432_H	Error when reading from the file DB.
0	1	8433_H	Error when accessing the file DB.
0	1	8434_H	Action was aborted.
0	1	8435_H	Channel will be reset.
0	1	8436_H	Unexpected server reply
0	1	8437_H	Certificate could not be verified.
0	1	8438_H	Unknown error occurred.

DONE	ERROR	STATUS	Meaning
0	1	8439_H	The FTP command causes an error. The cause must be looked for on the FTP server (REST command).
0	1	8440_H	The FTP server does not support the requested SSL protocol.
0	1	8446_H	After the FTP password was sent to the FTP server, an unexpected code was returned by the FTP server.
0	1	8451_H	An error was signaled when attempting to change the transmission mode from binary to ASCII.
0	1	8455_H	A memory request has failed on the CM/CP.
0	1	8460_H	A problem has occurred handling SSL/TLS.
0	1	8469_H	Interface error The specified output interface could not be used. Remedy: Set the interface to be used for outgoing connections.
0	1	8475_H	The SSL certificate or the SSH md5 fingerprint was not considered trusted.
0	1	8476_H	Nothing was received from the FTP server. In the current status, an incorrect response must be assumed.
0	1	8477_H	The specified "Crypto engine" (cryptographic module) was not found.
0	1	8478_H	The attempt to set the selected SSL "Crypto engine" as the default failed.
0	1	8480_H	A problem has occurred with the certificate of the FTP client.
0	1	8481_H	The specified number could not be used.
0	1	8482_H	The FTP server uses encoding that is not supported.
0	1	8484_H	The maximum file size was exceeded.
0	1	8485_H	The file DB was modified while being processed to be sent or the file DB is incorrectly structured.
0	1	8489_H	Data could not be sent. There is not enough memory available for the action on the FTP server.
0	1	8492_H	The file already exists. The file will not be overwritten.
0	1	8496_H	A problem occurred reading the SSL CA certificate.
0	1	8497_H	An unexpected error occurred in the SSH session.
0	1	8498_H	It was not possible to terminate the SSL connection.
0	1	8499_H	The socket is not ready for sending/receiving. Wait until it is ready and try again.
0	1	8501_H	The SSL certificate check of the FTP server failed.
0	1	8507_H	A timeout has occurred establishing the connection during the active FTP session while waiting for the FTP server.
0	1	$8F54_H$	The "EXIST" bit in the file DB header is not set.
0	1	$8F55_H$	Header status bit: Locked
0	1	$8F56_H$	The NEW bit in the file DB header was not reset

DONE	ERROR	STATUS	Meaning
0	1	$8F6B_H$	Possible causes: • Bad value for the CMD parameter Values from 0 to 15 are permitted. • An FB40 command is not supported. Possible cause: Incorrect firmware of the CP Remedy: Firmware update (with older CPs, use the functions FC 40...FC 44 instead of FB 40.)
0	1	$8F7F_H$	Internal error, for example, illegal ANY reference.

4.10.2.5 Structure of the data block (file DB) for FTP client operation

How it works

To transfer data with FTP, create data blocks (file DBs) on the CPU of your S7 station. These data blocks must have certain structure to allow them to be handled as transferable files by the FTP services. They consist of the following sections:

- Section 1: File DB header (has a fixed length of 20 bytes)
- Section 2: User data as "Array [..] of Byte" or "Array [..] of Char" (has a variable length and structure)

Data consistency

Make sure that you do not access the same file DB more than once at the same time.

Creating a file DB

1. Create a new data block in STEP 7.
2. Open the block editor.
3. In the block editor of the DB, select the line you want to use as the start line for the file DB.
4. In the "Data type" column, enter the type "FILE_DB_HEADER" using the keyboard.
   A data structure with the header structure required for the file DB is created.
5. Set the "WRITEACCESS" parameter to "true" to enable access.
6. Enter a value for the length of the user data at the "MAX_LENGTH" parameter.
7. Below this, create a data field of the type "Array [..] of Byte" or "Array [..] of Char" for the user data to be sent.
   The size of the field must match the specification of "MAX_LENGTH" in the header.

File DB header for FTP client mode

The file DB header described here is identical to the file DB header described for server mode.

Parameter	Type	Value / meaning	Supply
EXIST	BOOL	The EXIST bit indicates whether the user data area contains valid data. The retrieve FTP command executes the job only when EXIST=1. • 0: The file DB does not contain valid user data (file does not exist). • 1: The file DB contains valid user data (file exists).	The DELETE FTP command sets EXIST=0. The STORE FTP command sets EXIST=1.
LOCKED	BOOL	The LOCKED bit is used to restrict access to the file DB. • 0: The file DB can be accessed. • 1: The file DB is locked.	The "STORE" and "RETRIEVE" FTP commands set LOCKED=1 when they are executed if the bit was previously at 0. The user program on the S7 CPU can also set or reset LOCKED during write access to achieve data consistency. This results in mutual locking between the user program and FTP handling to ensure consistency. Recommended sequence in the user program: 1. Check LOCKED bit (if = 0) 2. Set WRITEACCESS bit = 0 3. Check LOCKED bit (if = 0) 4. Set LOCKED bit = 1 5. Write data 6. Set LOCKED bit = 0
NEW	BOOL	The NEW bit indicates whether data has been modified since the last read access. • 0: The content of the file DB is unchanged since the last write access. The user program of the S7 CPU has registered the last modification. • 1: The user program of the S7 CPU has not yet registered the last write access.	After execution, the "RETRIEVE" FTP command sets NEW=1. After reading the data, the user program in the S7 CPU must set NEW=0 to allow a new "RETRIEVE" command.
WRITEACCESS	BOOL	• 0: The user program has write access rights for the file DBs on the S7 CPU. • 1: The user program has no write access rights for the file DBs on the S7 CPU.	During the configuration of the DB, the bit is set to an initialization value. Recommendation: Whenever possible, the bit should remain unchanged! In special situations, adaptation during operation is possible.

Parameter	Type	Value / meaning	Supply
ACT_LENGTH	DINT	Current length of the user data area. The content of this field is only valid when EXIST = 1.	The current length is updated following write access.
MAX_LENGTH	DINT	Maximum length of the user data area (length of the entire DB less 20 bytes header).	The maximum length should be specified during configuration of the DB. The value can also be modified by the user program during operation.
FTP_REPLY_CODE	INT	Unsigned integer (16-bit) containing the last reply code from FTP as a binary value. The content of this field is only valid when EXIST = 1.	Updated by the FTP protocol handler with the FTP command processing of the server.
DATE_TIME	DATE_AND_TIME	Date and time of the last modification to the file. The content of this field is only valid when EXIST = 1.	The current date is updated following a write access. If the function for forwarding the time of day is used, the entry corresponds to the time that was passed on. If the function for forwarding the time of day is not used, a relative time is entered. The reference is the startup time of the CP (initialization value: 01.01.1994 00:00h).

Evaluating the "LOCKED" and "NEW" status bits from the FTP_CMD program block

- In version 1.2 of the "FTP_CMD" program block, the status bits "LOCKED" and "NEW" of the FILE_DB_HEADER are not evaluated.
  With the functions of the FTP server or when using the same file DB, the possibility of multiple simultaneous access to the same data area cannot be excluded. This can lead to data inconsistency.
- As of version 1.5 of the "FTP_CMD" program block, the status bits "LOCKED" and "NEW" of the FILE_DB_HEADER are set correctly. The two status bits are evaluated. Version 1.5 is available as of STEP 7 Professional V12 SP1.

Note

Avoiding data inconsistency

Make sure that you do not access the same file DB more than once at the same time.

4.11 Security

You will find an overview of the range and use of the security functions in section Industrial Ethernet Security (Page 20).

For the configuration limits of the security functions refer to the section Characteristics security (Page 24).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 76).

4.11.1 Security user

Creating a security user

You need the relevant configuration rights to be able to configure security functions. For this purpose, you need to create at least one security user with the corresponding rights.

Navigate to the global security settings > "User and roles" > "Users" tab.

1. Create a user and configure the parameters.
2. Assign this user the role "NET Administrator" in the "Assigned roles" area below.

After logging on, this user can make the necessary settings in the STEP 7 project.

In the future, continue to log on as this user when working on security parameters.

4.11.2 VPN

The "VPN" parameter group of the module is only displayed when you assign the module to a VPN group in the global security functions.

What is VPN?

Virtual Private Network (VPN) is a technology for secure transportation of confidential data in public IP networks, for example the Internet. With VPN, a secure connection (= tunnel) is set up and operated between two secure IT systems or networks via a non-secure network.

One of the main characteristics of the VPN tunnel is that it forwards all network packets regardless of higher protocols (HTTP, FTP).

The data traffic between two network components is transported practically unrestricted through another network. This allows entire networks to be connected together via a neighboring network.

Properties

- VPN forms a logical subnet that is embedded in a neighboring (assigned) network. VPN uses the usual addressing mechanisms of the assigned network, however in terms of the data, it transports its own network packets and therefore operates independent of the rest of this network.
- VPN allows communication of the VPN partners with the assigned network.

- VPN is based on tunnel technology, can be individually configured, is customer-specific and is self-contained.
- Communication between the VPN partners is protected from eavesdropping or manipulation by using passwords, public keys or a digital certificate (= authentication).

Areas of application

- Local area networks can be connected together securely via the Internet ("site-to-site" connection).
- Secure access to a company network ("end-to-site" connection).
- Secure access to a server ("end-to-end" connection).
- Communication between two servers is possible without being accessible to third parties ("end-to-end" or "host-to-host" connection).
- Ensuring information security in networked automation systems.
- Securing the computer systems including the associated data communication within an automation network or secure remote access via the Internet.
- Secure remote access from a PC/programming device to automation devices or networks protected by security modules is possible via public networks.

Cell protection concept

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected:

- The access to individual devices or even to entire automation cells protected by security modules is allowed.
- Secure connections via non-secure network structures becomes possible.

Due to the combination of different security measures such as firewall, NAT/NAPT routers and VPN via IPsec tunnels, security modules protect against the following:

- Data espionage
- Data manipulation
- Unwanted access

4.11.2.1 Creating VPN tunnel communication between S7-1500 stations

Requirements

To create a VPN tunnel between two S7-1500 stations, the following requirements must be met:

- Two S7-1500 stations have been configured.
- Participating CP 1543-1 are configured with a firmware version ≥ V1.1.
- The Ethernet interfaces of the two stations are located in the same subnet.

Note

Communication also possible via an IP router

Communication between the two S7-1500 stations is also possible via an IP router. To use this communications path, however, you need to make further settings.

Procedure

To create a VPN tunnel, you need to work through the following steps:

1. Create a security user.
   If the security user has already been created: Log on as a user.
2. Select the "Activate security features" check box.
3. Create the VPN group and assign security modules.
4. Configure properties of the VPN group.
   Configure local VPN properties of the two CPs.

You will find a detailed description of the individual steps in the following paragraphs of this section.

Creating a security user

To create a VPN tunnel, you require appropriate configuration rights. To activate the security functions, you need to create at least one security user.

1. In the local security settings of the CP, click the "User logon" button.
   Result: A new window opens.
2. Enter the user name, password and confirmation of the password.
3. Click the "User login" button.
   You have created a new security user. The security functions are now available to you.

With all further logons, log on as user.

"Activate security features" option enabled

- After logging on, you must enable the "Activate security features" option for both CPs.
  The security functions are now available to you for both CPs.

Creating the VPN group and assigning security modules

Note

Current date and current time of day on the security modules

When using secure communication (for example HTTPS, VPN...), make sure that the security modules involved have the current time of day and the current date. Otherwise the certificates used will not be evaluated as valid and the secure communication will not work.

1. In the global security settings, select the entry "Firewall" > "VPN groups" > "Add new VPN group".
2. Double-click on the entry "Add new VPN group", to create a VPN group.
   Result: A new VPN group is displayed below the selected entry.
3. In the global security settings, double-click on the entry "VPN groups" > "Assign module to a VPN group".
4. Assign the security modules between which VPN tunnels will be established to the VPN group.

Configuring properties of the VPN group

1. Double-click on the newly created VPN group.
   Result: The properties of the VPN group are displayed under "Authentication".
2. Enter a name for the VPN group. Configure the settings of the VPN group in the properties. In this way, you define the basic properties of the VPN group.

Note

Specifying the VPN properties of the CP

You specify the VPN properties of the required CP in the local properties of the module ("Security" > "Firewall" > "VPN")

Result

You have created a VPN tunnel. The firewalls of the CPs are activated automatically: The "Activate firewall" option is enabled by default when you create a VPN group. You cannot disable the option.

- Download the configuration to all modules that belong to the VPN group.

4.11.2.2 Establishment of VPN tunnel communication between the CP and SCALANCE M

Setting up VPN tunnel communication between the CP and SCALANCE M is essentially the same as described in Procedure for S7-1500 stations (Page 77).

VPN tunnel communication will only be established if you have enabled the "Perfect Forward Secrecy" option in the global security settings of the created VPN group ("VPN group > Authentication").

If the option is disabled, the CP rejects establishment of the connection.

4.11.2.3 VPN tunnel communication with SOFTNET Security Client

Setting up VPN tunnel communication between the SOFTNET Security Client and the CP is essentially the same as described in Procedure for S7-1500 stations (Page 77).

VPN tunnel communication works only if the internal node is disabled

Under certain circumstances, the establishment of VPN tunnel communication between SOFTNET Security Client and the CP fails.

SOFTNET Security Client also attempts to establish VPN tunnel communication to a lower-level internal node. This communication establishment to a non-existing node prevents the required communication being established to the CP.

To establish successful VPN tunnel communication to the CP, you need to disable the internal node.

Use the procedure for disabling the node as explained below only if the described problem occurs.

Disable the node in the SOFTNET Security Client tunnel overview:

1. Remove the checkmark in the "Enable active learning" check box.
   The lower-level node initially disappears from the tunnel list.
2. In the tunnel list, select the required connection to the CP.
3. With the right mouse button, select "Enable all members" in the shortcut menu.
   The lower-level node appears again temporarily in the tunnel list.
4. Select the lower-level node in the tunnel list.
5. With the right mouse button, select "Delete entry" in the shortcut menu.

Result: The lower-level node is now fully disabled. VPN tunnel communication to the CP is established successfully.

4.11.2.4 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

The application "SINEMA Remote Connect" (SINEMA RC) is available for remote maintenance purposes.

SINEMA RC uses OpenVPN for encryption of the data. The center of the communication is SINEMA RC Server via which communication runs between the subscribers and that manages the configuration of the communications system.

Preparatory steps

Execute the following steps before start configuring the SINEMA RC connection of the module in STEP 7. They are the prerequisite for a consistent STEP 7 project.

- Configuration of SINEMA Remote Connect Server
  Configure SINEMA RC Server as necessary (not in STEP 7). The communications module and its communications partners must be configured in the SINEMA RC Server.
- Exporting the CA certificate (optional)
  If you want to use the server certificate as authentication method of the communications module during connection establishment, export the CA certificate from SINEMA RC Server. Then import the CA certificate from SINEMA RC Server to the engineering station.
  Alternatively, you can use the fingerprint of the server certificate as authentication method of the communications module. The fingerprint's duration of validity may be shorter than that of the certificate.
  Please note that you need to repeat the import of a certificate in the event of a module replacement.

Configuration of SINEMA Remote Connect

Importing your own certificate

1. On the CP, navigate to the parameter group "Security > Certificate manager > Certificates of the partner devices".
2. Open the certificate selection dialog with a double-click on the first free table row.
3. Select the CA certificate of SINEMA RC Server.

Then navigate to the parameter group "Security > VPN".

VPN > General

1. Activate VPN
2. As "VPN connection type", select the option "Automatic OpenVPN configuration via SINEMA Remote Connect Server" if you wish to use communication via SINEMA Remote Connect.

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

Here you select the authentication method of the communications module during connection establishment.

- CA Certificate
  Under "CA certificate", select the CA certificate from SINEMA RC Server that was previously imported and assigned in the local certificate manager.
  The module generally checks the CA certificate of the server and its validity period. The two options cannot be changed.
- Fingerprint
  When you select this authentication method, you enter the fingerprint of the server certificate of SINEMA RC Server.

Authentication

- Device ID
  Enter the device ID generated for the module in SINEMA RC.
- Device password
  Enter the device password of the module configured in SINEMA RC.
  Max. number of characters: 127

Optional settings

The connection establishment is configured in the "Security > VPN > Optional settings" parameter group with the parameter "Connection type".

- **Update interval**
  With this parameter you set the interval at which the CP queries the configuration on the SINEMA RC Server.
  Note that with the setting 0 (zero) changes to the configuration of the SINEMA RC Server may result in the CP no longer being capable of establishing a connection to the SINEMA RC Server.
- **"Connection type"**
  The two options of the parameter have the following effect on the connection establishment:
  - Auto
    The module establishes a connection to the SINEMA RCServer. The OpenVPN connection is retained until the connection parameters are changed by the SINEMA Remote Connect Server. If the connection is interrupted, the CP automatically re-establishes the connection.
    If the connection parameters are changed by the SINEMA Remote Connect Server, the CP requests the new connection data after the update interval configured above has elapsed.
  - PLC trigger
    The option is intended for sporadic communication of the module via the SINEMA RC Server.
    You can use this option when you want to establish temporary connections between the module and a PC. The temporary connections are established via a PLC tag and can be used in servicing situations, for example.

Note

Connection abort

With a STOP of the CPU, for example due to a firmware update or "Download to device", the OpenVPN connection is aborted.

These functions can only be used when the "Auto" option is enabled.

- **PLC tag for connection establishment**
  If the option "PLC trigger" is selected, the module establishes a connection when the PLC tag (Bool) changes to the value 1. During operation the PLC tag can be set when necessary, for example using an HMI panel.
  When the PLC tag is reset to 0, the connection is terminated again.

Manual setting the time of day during commissioning

Note

Time-of-day synchronization when using Security / SINEMA RC

When using security functions, such as SINEMA Remote Connect, the CP needs the current time for authentication on the partner or on the SINEMA RC Server.

The CP receives the time from an NTP server before the connection is established for the first time.

4.11.2.5 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

If the CP is connected to another VPN subscriber via a gateway, you need to set the permission for VPN connection establishment to "Responder".

This is the case in the following typical configuration:

VPN subscriber (active) ⇔ gateway (dyn. IP address) ⇔ Internet ⇔ gateway (fixed IP address) ⇔ CP (passive)

Configure the permission for VPN connection establishment for the CP as a passive subscriber as follows:

1. In STEP 7, go to the devices and network view.
2. Select the CP.
3. Open the parameter group "VPN" in the local security settings.
4. For each VPN connection with the CP as a passive VPN subscriber, change the default setting "Initiator/Responder" to the setting "Responder".

4.11.3 Firewall

4.11.3.1 Firewall sequence when checking incoming and outgoing frames

Each incoming or outgoing frame initially runs through the MAC firewall (layer 2). If the frame is discarded at this level, it is not checked by the IP firewall (layer 3). This means that with suitable MAC firewall rules, IP communication can be restricted or blocked.

See also

Programmed connections: Restriction of firewall rules (Page 54)

Virtual interface of the CPU (Page 51)

4.11.3.2 No counting of incorrect packages

Incoming incorrect packages are filtered with an enabled firewall, but do not increase the counter for filtered packages ("drop").

Validity: CP "AX00"

4.11.3.3 Notation for the source IP address (advanced firewall mode)

If you specify an address range for the source IP address in the advanced firewall settings of the CP, make sure that the notation is correct:

- Separate the two IP addresses only using a hyphen.
  Correct: 192.168.10.0-192.168.10.255
- Do not enter any other characters between the two IP addresses.
  Incorrect: 192.168.10.0 - 192.168.10.255

If you enter the range incorrectly, the firewall rule will not be used.

4.11.3.4 HTTP and HTTPS not possible with IPv6

It is not possible to use HTTP and HTTPS communication on the Web server of the station using the IPv6 protocol.

If the firewall is enabled in the local security settings in the entry "Firewall > Predefined IPv6 rules": The selected check boxes "Allow HTTP" and "Allow HTTPS" have no function.

4.11.3.5 Firewall settings for connections via a VPN tunnel

IP rules in advanced firewall mode

If you have configured connections between CPs, note the following setting if you operate the CPs in advanced firewall mode.

In the parameter group "Security > Firewall > IP rules" select the setting "Accept" for tunnel connections for both CPs.

If you do not enable the option, the VPN connection is terminated and re-established.

This applies to connections between a CP 154x-1 and, for example, a CP 343-1 Advanced, CP 443-1 Advanced, CP 1628 or CP 1243-1.

See also

Settings for online security diagnostics and downloading to station with the firewall activated (Page 85)

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

Note

Additional services for online security diagnostics and download

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

Setting the firewall for online functions

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

Global security functions:

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

Local security functions of the CP:

Now select the CP in the S7 station.

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

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

4.11.4 Log settings - Filtering of the system events

Communications problems if the value for system events is set too high

If the value for filtering the system events is set too high, you may not be able to achieve the maximum performance for the communication. The high number of output error messages can delay or prevent the processing of the communications connections.

In "Security > Log settings > Configure system events", set the "Level:" parameter to the value "3 (Error)" to ensure the reliable establishment of the communications connections.

4.11.5 Network authentication

Network authentication and EAP methods

The CP supports network authentication according to IEEE 802.1X.

Network authentication is used for configurations in which the CP can access a network via a switch that also supports IEEE 802.1X. The CP must first authenticate itself before access to the network is enabled.

Authentication of the CP is handled either by a switch, which checks the identity of the CP itself, or an authentication server or configured RADIUS server.

The communication for authentication runs via the Extensible Authentication Protocol (EAP). It is used to authenticate the CP to the network and for key exchange to protect communication.

Configuration

1. Select the CP.
2. Select the "Network authentication" entry in the local security settings and enable the option.
3. Select an EAP method:
4. Make the respective settings for the selected EAP method.

The following authentication methods are supported.

EAP methods

- **MD5**
  MD5 is not secure against man-in-the-middle attacks and dictionary attacks.
  Use of a method with higher security is recommended.
- **TLS**
  TLS establishes an encrypted TLS connection and provides certificate-based mutual authentication of client and network.
- **PEAP**
  PEAP is a two-stage procedure. A secure tunnel is established in the first stage, in which another authentication procedure takes place subsequently.
  Unlike the TLS method, PEAP does not necessarily have to verify the identity of the client in the first stage. This is why the configuration of the client certificate is options.
- **TTLS**
  TTLS is an extension of TLS and is also a two-stage procedure. Provides certificate-based mutual authentication of the client and the network through an encrypted channel or tunnel. In contrast to TLS, it only requires server-side certificates.

- **MSCHAPv2**
  The method was originally used for logging into Microsoft networks, but is now also used by some other applications. It is used only within a secured tunnel.
- **PWD**
  PWD works without encryption. It can be used in a tunnel (e.g. TTLS) or alone.
  Use of a method with higher security is recommended.

Settings for the authentication method

Make the following settings for the EAP method used:

EAP methods	Identity	Internal EAP method *	Authentication settings	Verification settings	Server list
MD5	User name (1 to 256 characters)	-	Password (1 to 256 characters)	-	-
TLS	User name (1 to 256 characters) Can also be left blank depending on the configuration of the RADIUS server.	-	-	The CA certificate must be assigned to the CP. Client certificate with private key must be assigned to the CP.	Optional input of one or more servers Placeholders are possible. ** If no entry is made, any certificate signed by the certificate authority is allowed.
PEAPv0	User name (1 to 256 characters)	MD5 MSCHAPv2 PWD	Password (1 to 256 characters)	The CA certificate must be assigned to the CP. Client certificate (optional), depending on the configuration of the RADIUS server. Client certificates with private key	Optional input of one or more servers Placeholders are possible. ** If no entry is made, any certificate signed by the certificate authority is allowed.
TTLS	User name (1 to 256 characters)	MD5 MSCHAPv2 PWD	-	The CA certificate must be assigned to the CP. Client certificate (optional), depending on the configuration of the RADIUS server. Client certificates with private key	Optional input of one or more servers Placeholders are possible. ** If no entry is made, any certificate signed by the certificate authority is allowed.

EAP methods	Identity	Internal EAP method *	Authentication settings	Verification settings	Server list
MSCHAPv2	User name (1 to 256 characters)	-	Password (1 to 256 characters) or Hash value (MD4 hash of the password; 1 to 32 characters).	-	-
PWD	User name (1 to 256 characters)	-	Password (1 to 256 characters)	-	-

* The internal method is used in the two-stage procedure within the established tunnel.

** When placeholders are used (server domain masks), the distinguished name or SAN of the server certificate must match at least one mask.

4.12 Program blocks for OUC

Programming Open User Communication (OUC)

The instructions (program blocks) listed below are required for the following communication services via Ethernet:

- ISO transport
- TCP (IPv4 / IPv6)
- ISO-on-TCP
- UDP (Multicast)
- E-mail

For this, create suitable program blocks. The program block can be found in STEP 7 in the "Instructions > Communication > Open user communication" window.

You will find details on the program blocks in the information system of STEP 7.

Note

Different program block versions

Note that in STEP 7 you cannot use different versions of a program block in a station.

Supported program blocks for OUC

The following instructions in the specified minimum version are available for programming Open User Communication:

- **TSEND_C V3.1 / TRCV_C V3.1**
  Compact blocks for connection establishment/termination and for sending and receiving data
  or
- **TCON V4.0 / TDISCON V2.1**
  Connection establishment / connection termination
- **TUSEND V4.0 / TURCV V4.0**
  Sending and receiving data via UDP
- **TSEND V4.0 / TRCV V4.0**
  Sending and receiving data via TCP or ISOonTCP
- **TMAIL_C V4.0**
  Sending e-mails
  Note the description of TMAIL_C as of version V4.0 in the STEP 7 information system.

Note

Personal data unencrypted in TMAIL_C

Note that TMAIL_C uses personal data, such as user name and password, in its parameters. This data is stored unencrypted in a data block.

Connection establishment and termination

Connections are established using the program block TCON. Note that a separate program block TCON must be called for each connection.

A separate connection must be established for each communications partner even if identical blocks of data are being sent.

After a successful transfer of the data, a connection can be terminated. A connection is also terminated by calling TDISCON.

Note

Connection abort

If an existing connection is aborted by the communications partner or due to disturbances on the network, the connection must also be terminated by calling TDISCON. Make sure that you take this into account in your programming.

Connection descriptions in system data types (SDTs)

For the connection description, the blocks listed above use the parameter CONNECT (or MAIL_ADDR_PARAM with TMAIL_C). The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

You create the SDT required for every connection description as a data block. You generate the SDT type in STEP 7 by entering the name (e.g. "TCON_IP_V4") in the "Data type" box manually in the declaration table of block instead of selecting an entry from the "Data type" drop-down list. The corresponding SDT is then created with its parameters.

The following SDTs can be used.

- **TCON_Configured**
  For transferring frames via TCP
- **TCON_IP_V4**
  For transferring frames via TCP or UDP
- **TCON_IP_V4_SEC**
  For the secure transfer of frames via TCP
- **TCON_QDN**
  As of SDT version V2.2
  For transferring frames via TCP or UDP (IPv4 / IPv6)
- **TCON_QDN_SEC**
  As of SDT version V2.2
  For the secure transfer of frames via TCP (IPv4 / IPv6)
- **TCON_IP_RFC**
  For transferring frames via ISO-on-TCP
- **TCON_ISOnative**
  For transferring frames via ISO transport
- **TMail_V4**
  For transferring e-mails addressing the e-mail server using an IPv4 address
- **TMail_V6**
  For transferring e-mails addressing the e-mail server using an IPv6 address
- **TMail_FQDN**
  For transferring e-mails addressing the e-mail server using the host name
- **TMail_V4_SEC**
  For secure transfer of e-mails addressing the e-mail server using an IPv4 address
- **TMail_V6_SEC**
  For secure transfer of e-mails addressing the e-mail server using an IPv6 address
- **TMail_QDN_SEC**
  For secure transfer of e-mails addressing the e-mail server using the host name

You will find the description of the SDTs with their parameters in the STEP 7 information system under the relevant name of the SDT.

You can find a description of the parameters of SDTs TMail_V4_SEC, TMail_V6_SEC and TMail_QDN_SEC in the online help section on TCON_IP_V4_SEC.

Diagnostics and upkeep

5



⚠ CAUTION

Hot surfaces

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

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

⚠ WARNING

Cleaning the housing

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

Do not use any liquids or solvents.

⚠ WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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

5.1 Diagnostics options

You have the following diagnostics options available for the module:

LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 29).

CP diagnostics during runtime

Via the configuration, you can enable writing of diagnostics information into variables of the CPU; refer to section CP diagnostics (Page 57).

STEP 7: The "Diagnostics" tab in the Inspector window

If your engineering station is connected to the module via Ethernet, information on the connection status of the ES with the module can be found here.

STEP 7: Diagnostic functions via the "Online & Diagnostics" shortcut menu

Using the online functions, you can read various diagnostics information of the module from an engineering station on which the STEP 7 project is stored and perform maintenance functions.

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

Diagnostics

Here, you can obtain the following static information on the selected module:

- General
  General information on the module
- Diagnostics status
  Information on the diagnostics status
- Ethernet interface
  Address and statistical information
- Time
  Specification of the current time in the module and the time source
- Security
  Status information and log entries

Functions

You can run the following functions here:

- Firmware update
  For a description, see section Update firmware (Page 97).
- Assign IP address
- Assign PROFINET device name
- Save service data

STEP 7: Online connection

Establish the online connection to the module via the "Connect online" shortcut menu.

For the procedure, refer to the section Connect online (Page 93).

Web server

On a PC, you can access the Web pages of the CPU via HTTP/HTTPS. These pages provide various information.

For access to the content, see Cybersecurity information (Page 7), Documentation guide.

SNMP

You will find detailed information about the supported functions in the section Diagnostics with SNMP (Page 94).

5.2 Online functions

5.2.1 Online security diagnostics via port 8448 of the CP

Security diagnostics via port 8448

Requirements:

- With an activated firewall, access must be enabled.

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

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

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

For more information, refer to section Settings for online security diagnostics and downloading to station with the firewall activated (Page 85).

5.2.2 Connect online

Online functions

Together with STEP 7, the CP offers various diagnostic and maintenance functions at the engineering station (ES). The ES and the CP must be in the same subnet for this.

Establishing an online connection via Ethernet

Procedure:

1. Connect the ES to the network.
2. Open the relevant STEP 7 project on the ES.
3. Select the CP.
4. Enable the online functions using the "Connect online" icon.
5. In the "Connect online" dialog, select the entry "PN/IE" from the "Type of PG/PC interface" drop-down list.

6. In the "PG/PC interface" drop-down list, select the interface of the ES.
   You can use the  icon to the right of the drop-down list to check the settings of the interface.
7. In the "Connect with interface/subnet" drop-down list, select the interface of the station
8. Click "Start search".
   If a connection is possible, the station is displayed.
9. Select the station in the table of target devices.
   The path is possible both via the CP or the CPU.
10. Click "Connect".

Terminate online connection

On completion of the online session, terminate the online connection again using the "Disconnect" button.

5.3 Diagnostics with SNMP

Requirement

The requirement for using SNMP is the enabling of the function in the configuration.

SNMP (Simple Network Management Protocol)

SNMP is a protocol for diagnostics and managing networks and nodes in the network. To transmit data, SNMP uses the connectionless UDP protocol.

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

You will find detailed information on SNMP and the Siemens Automation MIB in the manual "Diagnostics and Configuration with SNMP" that you will find on the Internet:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15392/man)

Performance range of the CP

The CP supports the following SNMP versions:

- SNMPv1
- SNMPv3 (with activated Security functions)

Traps are not supported by the CP.

Supported MIBs in SNMPv1

The CP supports the following MIBs:

- **MIB II (acc. to RFC1213)**
  The CP supports the following groups of MIB objects:
  - System
  - Interfaces
  - IP
  - ICMP
  - TCP
  - UDP
  - SNMP
- **LLDP MIB**
- **Siemens Automation MIB**
  Note the rights for writing to the MIB objects, see the next section (SNMPv3).

Supported MIB objects in SNMPv3

If SNMPv3 is enabled, the CP returns the contents of the following MIB objects:

- **MIB II (acc. to RFC1213)**
  The CP supports the following groups of MIB objects:
  - System
  - Interfaces
    The "Interfaces" MIB object provides status information about the CP interfaces.
  - IP (IPv4/IPv6)
  - ICMP
  - TCP
  - UDP
  - SNMP

  The following groups of the standard MIB II are not supported:
  - Adress Translation (AT)
  - EGP
  - Transmission
- **LLDP MIB**
- **Siemens Automation MIB**
  Note that 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 and groups, only read access is possible for security reasons.

Access rights using community names (SNMPv1)

TCP uses the following community strings to control the permissions for access to the SNMP agent:

Table 5-1 Access rights in the SNMP agent

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

*) Note the use of lowercase letters!

Note

Security of the access

For security reasons, change the generally known strings "public" and "private".

5.4 Update firmware

New firmware versions of the module

If a new firmware version is available for the module, you will find this on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15340/dl)

Firmware files have the file format *.upd.

Save the firmware file on your PC.

There are different ways of loading a new firmware file into the module:

- Online functions of STEP 7 via Ethernet
- Loading the firmware file into the CPU from an SD card

Note

SD card only for firmware file

For the firmware file, you need a SIMATIC SD memory card, for example (article numbers):

- 6AV6671-8XB10-0AX1
- 6AV2181-8XP00-0AX0
- 6AV2181-8AQ10-0AX0

The firmware update card may not contain any other files. An SD card with configuration data cannot be used.

Note

Duration of the firmware update

Downloading a new firmware file can take several minutes.

Always wait until the completion of the firmware update can be recognized from the LEDs (see below).

Loading the firmware with the online functions of STEP 7 via Ethernet

Requirements:

- The CPU of the station is accessible via Ethernet.
- The engineering station and the CPU are located in the same subnet.

- The new firmware file is stored on your engineering station.
- The engineering station is connected to the network.
- The relevant STEP 7 project is open on the engineering station.

Procedure:

1. Select the station that you want to update with a new firmware.
2. Enable the online functions using the "Connect online" icon.
3. In the "Connect online" dialog, select the Ethernet interface in the "Type of PG/PC interface" list box.
4. Select the CPU of the station.
5. Click on "Start search" to search for the module in the network and to specify the connection path.
   When the module is found it is displayed in the table.
6. Connect using the "Connect" button.
   The "Connect online" wizard guides you through the remaining steps in installation.
7. Select the CPU in the network view and select the "Online & Diagnostics" shortcut menu (right-click).
8. In the navigation panel of the Online & Diagnostics view, select the entry "Functions > Firmware update".
9. Using the "Browse" button (parameter group "Firmware loader") search for the new firmware file in the file system of the engineering station.
10. Start to download the firmware with the "Start update" button when the correct version of the signed firmware is displayed in the "Status" output box.

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

Loading the firmware via the SD card

You can find detailed information on using an SD card in the S7-1500 System Manual, see Cybersecurity information (Page 7), Documentation guide.

Requirements:

- You have copied the new firmware file from your PC to the SD card using a suitable card reader.
- Optional: You have saved a backup file of the currently used firmware file.

Procedure:

1. Set the operating mode switch of the CPU to STOP.
   Ensure that no write functions (e.g. online or test functions) are active in the STOP state.
2. Remove the SIMATIC Memory Card with the configuration data from the slot of the CPU.

3. Insert the SD card with the firmware file in the card slot of the CPU.
   The firmware update starts shortly after the card has been inserted. The display shows the following: "STOP - FW UPDATE"
   If errors occur, appropriate messages are displayed.
   After completing the firmware update, the display shows a result page.
   A successful firmware update can be recognized by the following LED pattern from the CPU:
   - RUN lights up yellow.
   - MAINT flashing yellow.
4. Remove the SD card and insert the SIMATIC Memory Card again.
5. Set the operating mode switch of the CPU to RUN.
   The module uses the new firmware during startup.

For the LED pattern of the module during startup, refer to section LEDs (Page 29).

5.5 Replacing a module without a programming device

Configuration data when swapping modules

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

Note

Configured MAC address is adopted

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

Note

No SHA1 with CP "AX10"

The CP (6GK7 543-1AX10-0XE0) with firmware version V4.x no longer supports SHA1.

If you insert a new CP (6GK7 543-1AX10-0XE0), but do not configure this as CP (6GK7 543-1AX00-0XE0) in STEP 7, the CP still supports SHA1.

Module replacement: SHA1 support when replacing a CP "AX00" with a CP "AX10" *

When you replace a CP "AX00" with a CP "AX10" and operate the CP in a VPN group with SHA1, the CP "AX10" still supports SHA1 if you renew its certificate in STEP 7 and manually set the "Hash algorithm" option to "sha1".

* For information on the compatibility of the CP "AX10" with different firmware versions of the CP "AX00", see section Project engineering (Page 26).

Swapping modules for address reference via DHCP (IPv4)

One option in the IP configuration of the CP 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 factory default MAC address of the new module is sent to the DHCP server, the DHCP server returns 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. This ensures that the CP always receives the same IP address from the DHCP server after swapping a module.

If you have configured a new MAC address instead of the MAC address set in the factory, the configured MAC address will always be transferred to the DHCP server. In this case, the new CP also has the same IP address as the previous module.

Technical specifications

6

6.1 Technical specifications of the CP (6GK7543-1AX00-0XE0)

Note the information in the System description of SIMATIC S7-1500, see Cybersecurity information (Page 7).

In addition to the information in the system description, the following technical specifications apply to the module.

Technical specifications - CP 1543-1		
Product name	CP 1543-1	
Article number	6GK7 543-1AX00-0XE0	
Attachment to Industrial Ethernet		
• Quantity	1 x Ethernet (gigabit) interface	
• Design	RJ-45 jack	
• Transmission speed	10 / 100/ 1000 Mbps	
Electrical data		
Power supply		
• via S7-1500 backplane bus	15 V	
Current consumption		
• From backplane bus	350 mA	
• Power dissipation	5.3 W	
Insulation	Tested to:	DC 780 V (type test)
Permitted ambient conditions		
Ambient temperature *	During operation with the rack installed horizontally	0 °C ... +60 °C
	During operation with the rack installed vertically	0 °C ... +40 °C
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3	
Design, dimensions and weight		
Module format	Compact module S7-1500, single width	
Degree of protection	IP20	
Weight	Approx. 350 g	
Dimensions (W x H x D)	35 x 142 x 129 mm	
Installation options	Mounting in an S7-1500 rack	
Product functions **		

***** Also read the information in the Ambient temperature (Page 103) section.

****** You will find the product functions in the section Application, functions and requirements (Page 15).

6.2 Technical specifications of the CP (6GK7543-1AX10-0XE0)

Note the information in the System description of SIMATIC S7-1500, see Cybersecurity information (Page 7).

In addition to the information in the system description, the following technical specifications apply to the module.

Technical specifications - CP 1543-1		
Product name	CP 1543-1	
Article number	6GK7 543-1AX10-0XE0	
Attachment to Industrial Ethernet		
• Quantity	1 x Ethernet (gigabit) interface	
• Design	RJ-45 jack	
• Transmission speed	10 / 100/ 1000 Mbps	
Electrical data		
Power supply		
• via S7-1500 backplane bus	15 V	
Current consumption		
• From backplane bus (typical)	250 mA	
• Effective power loss (typical)	3.75 W	
Insulation	Tested to:	DC 780 V (type test)
Permitted ambient conditions		
Ambient temperature *****	During operation with the rack installed horizontally	-30 °C ... +60 °C
	During operation with the rack installed vertically	-30 °C ... +40 °C
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3	
Design, dimensions and weight		
Module format	Compact module S7-1500, single width	
Degree of protection	IP20	
Weight	260 g	
Dimensions (W x H x D)	35 x 142 x 129 mm	
Installation options	Mounting in an S7-1500 rack	
Product functions **		

***** Also read the information in the Ambient temperature (Page 103) section.

** You will find the product functions in the section Application, functions and requirements (Page 15).

6.3 Ambient temperature

Restrictions of the maximum specified ambient temperature

The maximum permissible temperatures of the module for altitudes up to 2000 m can be found above in the technical specifications.

When using the module at higher altitudes, the decrease in the cooling effect due to convection as a result of the lower air pressure must be taken into account. According to IEC 61010-2-201 CD2 2015, the temperature at altitudes > 2000 m must be reduced.

The following derating factors and maximum ambient temperatures apply.

Table 6-1 Restrictions of the maximum permissible ambient temperature in relation to the installation altitude

Installation altitude (Height above mean sea level)	Derating factor [1]	Maximum ambient temperature when the rack is mounted horizontally
-1000 m to 2000 m	1.00	60 °C
2000 m to 3000 m	0.93	56 °C
3000 m to 4000 m	0.86	52 °C
4000 m to 5000 m	0.78	47 °C

[1] Basic value for applying the derating factor is the maximum permissible ambient temperature in °C for 2000 m.

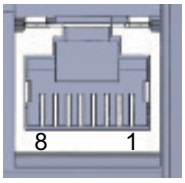
Note

- The derating factors compensate for the decreasing cooling effect of air at higher altitudes due to lower density.
- Linear interpolation between altitudes is permissible.

6.4 Pinout of the Ethernet interface

Pinout of the gigabit Ethernet interfaces

The table below shows the pin assignment of the Ethernet interface X1.

View of the RJ-45 jack	Pin	Signal name	Assignment
	1	D1+	D1+ bidirectional
	2	D1-	D1- bidirectional
	3	D2+	D2+ bidirectional
	4	D3+	D3+ bidirectional
	5	D3-	D3- bidirectional
	6	D2-	D2- bidirectional
	7	D4+	D4+ bidirectional
	8	D4-	D4- bidirectional

6.5 Permitted cable lengths - Ethernet

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

See also Siemens Mall: (https://mall.industry.siemens.com)

6.6 Permitted cable lengths - Gigabit Ethernet

Permitted cable lengths - Gigabit Ethernet	Alternative combinations
0 ... 60 m	• Max. 60 m IE FC TP Flexible Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE
0 ... 100 m	• Max. 90 m IE FC TP Standard Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE

See also Siemens Mall: (https://mall.industry.siemens.com)

Approvals

7

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals - with the exception of the certificates for shipbuilding - have only been obtained when there is a corresponding mark on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate. The approvals for shipbuilding are an exception to this.

Certificates for shipbuilding and national approvals

The device certificates for shipbuilding and special national approvals can be found in Siemens Industry Online Support on the Internet:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15340/cert)

Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15340/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 device meets the requirements and safety objectives of the following EC directives and it complies with the harmonized European standards (EN) for programmable logic controllers which are published in the official documentation of the European Union.

- **2014/34/EU (ATEX explosion protection directive)**
  Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356
- **2014/30/EU (EMC)**
  EMC directive of the European Parliament and of the Council of 26 February 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, p. 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 directives:

- 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, and related amendments.
- RoHS Regulations
  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX / IECEx / UKEX / CCC-Ex

Observe the information in the "Use of subassemblies/modules in a Zone 2 Hazardous Area" document, which you will find here:

- On the documentation DVD supplied with the product, under:
  "All documents" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- On the Internet at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013)

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 36).

The product meets the explosion protection requirements outlined below.

IECEx

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

The product meets the requirements of the standards:

- 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 3 G 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: II 3 G 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 device meets the requirements of the following guidelines:

- EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive)
- EMC Regulations SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

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 device meets the requirements of the following guidelines:

- 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, and related amendments.

Applied standard: EN IEC 63000

c(UL)us



Applied standards:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E 85972 (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 T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta: Refer to the temperature class on the type plate of the module

Report / UL file: E223122 (NRAG, NRAG7)

Note the conditions for the safe deployment of the product according to the section Notes on use in hazardous areas according to UL HazLoc and FM (Page 37).

Note

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

CSA

CSA Certification Mark Canadian Standard Association (CSA) nach Standard C 22.2 No. 142:

- Certification Record 063533–C-000

FM

Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

You will find the temperature class on the type plate on the module.

Australia - RCM

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

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

A급 기기(업무용 방송통신기자재)

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

Note that in terms of the emission of interference, this device corresponds to limit class A. This device can be used in all areas except for residential environments.

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/15340/cert)

Additional information

A

A.1 Linking to other systems with FETCH/WRITE

The FETCH/WRITE mode supported with ISO transport connections, TCP, and ISOonTCP connections can be used from non-Siemens devices to access the S7 system memory areas.

To be able to use this type of access, for example for PC applications, you need to know the PDU structure of the jobs. The required S7-specific or S5-specific headers for request and response frames are 16 bytes long. You will find your structure below.

Structure of WRITE frame

The meaning and values of parameters shown without fixed values in the following table can be found in the section "Parameter values".

WRITE request frame			**WRITE acknowledgment frame**		
0	System ID	="S"	0	System ID	="S"
1		="5"	1		="5"
2	Length of header in bytes	=16d.	2	Length of header	=16d.
3	ID OP code	=01	3	ID OP code	=01
4	Length OP code	=03	4	Length OP code	=03
5	OP code	=03	5	OP code	=04
6	ORG field	=03	6	Ack field	=0Fh
7	Length ORG field	=08	7	Length ack field	=03
8	**ORG ID**		**8**	**Error field**	**=No**
9	**DBNR**		**9**	**Empty field**	**=FFh**
A	**Start address**	**High byte**	**A**	**Length empty field**	**=07**
B		**Low byte**	**B**		
C	**Length**	**High byte**	**C**		
D		**Low byte**	**D**	**free**	
I	**Empty field**	**=FFh.**	**I**		
F	**Length empty field**	**=02**	**F**		
	Data field up to 64 K				

Structure of FETCH frame

The meaning and values of parameters shown without fixed values in the following table can be found in the section "Parameter values".

FETCH request frame			**FETCH response frame**		
0	System ID	="S"	0	System ID	="S"
1		="5"	1		="5"
2	Length of header	=0x10	2	Length of header	=0x10

3	ID OP code	=0x01	3	ID OP code	=0x01
4	Length OP code	=0x03	4	Length OP code	=0x03
5	OP code	=0x05	5	OP code	=0x06
6	ORG field	=0x03	6	Ack field	=0x0F
7	Length ORG field	=0x08	7	Length ack field	=0x03
8	ORG ID		8	Error field	=No
9	DBNR		9	Empty field	=0xFF
A	Start address	High byte	A	Length empty field	=0x07
B		Low byte	B	free	
C	Length	High byte	C		
D		Low byte	D		
I	Empty field	=0xFF	I		
F	Length empty field	=0x02	F		
				Data up to 64 K, but only if Error no. = 0	

Parameter values

S7 operand area	**DB**	**M**	**I**	**A**
ORG ID	01_H	02_H	03_H	04_H
	Source/dest. data from/to data block in main memory	Source/dest. data from/to bit memory area	Source/dest. data from/to process image of the inputs (PII)	Source/dest. data from/to process image of the outputs (PIQ)
DBNR	DB, from which the source data is taken or to which the dest data is transferred	irrelevant	irrelevant	irrelevant
Permitted range	1...255			
Start address	DW number from which the data is read or written.	Memory byte no. from which the data is read or written.	Input byte no. from which the data is read or written.	Output byte no. from which the data is read or written.
Permitted range	0...2047	All memory bytes made available by a CPU.	0...127	0...127
Length	Length of the source/destination data block in words	Length of the source/destination data block in bytes	Length of the source/destination data block in bytes	Length of the source/destination data block in bytes
Permitted range	Up to 8192 bytes	Up to 8192 bytes	1...128	1...128

S7 operand area	**PI/PQ**	**C**	**T**
ORG ID	05_H	06_H	07_H

	Source/destination data from/to I/O modules With source data input modules, with destination data output modules	Source/dest data from/to counter cells	Source/dest data from/to timer cells
DBNR	irrelevant	irrelevant	irrelevant
Start address	I/O byte no. from which the data is read or written.	Number of the counter cell from which the data is read or written.	Number of the timer cell from which the data is read or written.
Permitted range	0...127 digital I/O 128...255 anal. I/O	0...255	0...255
Quantity	Length of the source/destination data block in bytes	Length of the source/destination data block in words (counter cell = 1 word)	Length of the source/destination data block in words (counter cell = 1 word)
Permitted range	1...256	1	1

A.2 Encryption methods (Ciphers) used by the module

The following tables list the encryption methods (ciphers) used by the CP with firmware versions V4.x and V3.x.

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.
  - 1:
    Secure OUC client (TCP 2001), Secure OUC server (TCP 2000)
    SMTP client (TCP 587)
    FTPS client/server (TCP 989, 990)
    IPsec client/server (UDP 500), HTTPS (TCP 443), SNMPv3 server (UDP 161), openVPN client (UDP 1194) / SINEMA RC client (TCP 4443), STEP 7 security diagnostics (TCP 8448)
  - 2: IEEE 802.1X (Port-Based Network Access Control)
    Can be set under firewall MAC rules when network authentication is enabled.

TLS versions used by the CP

TLS version	Security
TLS Version 1.0	Legacy
TLS Version 1.2	✓
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	✓	1
Cipher	TLS_AES_256_GCM_SHA384	0x13,0x02	TLS 1.3	✓	1
Cipher	TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS 1.3	✓	1
Cipher	TLS_AES_128_CCM_SHA256	0x13,0x04	TLS 1.3	✓	1
Cipher	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00,0xA2	TLS 1.2	✓	1
Cipher	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00,0xA3	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x9E	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9E	TLS 1.2	✓	1, 2
Cipher	TLS_DHE_RSA_WITH_AES_256_CCM	0xC0,0x9F	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9F	TLS 1.2	✓	1, 2
Cipher	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAA	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0,0xAC	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0,0x2B	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0,0xAD	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC0,0x2C	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA9	TLS 1.2	✓	1
Cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC0,0x2F	TLS 1.2	✓	1, 2

Category	Name	Value	TLS	Security	Protocol
Cipher	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x30	TLS 1.2	✓	1, 2
Cipher	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA8	TLS 1.2	✓	1
DSA	DSA_SHA256	0x0402		✓	1
DSA	DSA_SHA384	0x0502		✓	1
DSA	DSA_SHA512	0x0602		✓	1
DSA	ecdsa_secp256r1_sha256	0x0403		✓	1
DSA	ecdsa_secp384r1_sha384	0x0503		✓	1
DSA	ecdsa_secp521r1_sha512	0x0603		✓	1
SEA	ed25519	0x0807		✓	1
SEA	ed448	0x0808		✓	1
SEA	rsa_pss_pss_sha256	0x0804		✓	1
SEA	rsa_pss_pss_sha384	0x0805		✓	1
SEA	rsa_pss_pss_sha512	0x0806		✓	1
SEA	rsa_pss_rsae_sha256	0x0809		✓	1
SEA	rsa_pss_rsae_sha384	0x080A		✓	1
SEA	rsa_pss_rsae_sha512	0x080B		✓	1
DSA	rsa_pkcs1_sha256	0x0401		✓	1, 2
DSA	rsa_pkcs1_sha384	0x0501		✓	1, 2
DSA	rsa_pkcs1_sha512	0x0601		✓	1

Ciphers used by CP with firmware version V3.0

Category	Name	Value	TLS	Security	Protocol
Cipher	TLS_AES_128_GCM_SHA256	0x13,0x01	TLS 1.3	✓	1
Cipher	TLS_AES_256_GCM_SHA384	0x13,0x02	TLS 1.3	✓	1
Cipher	TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS 1.3	✓	1
Cipher	TLS_AES_128_CCM_SHA256	0x13,0x04	TLS 1.3	✓	1
Cipher	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00,0xA2	TLS 1.2	✓	1
Cipher	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00,0xA3	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x9E	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9E	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_256_CCM	0xC0,0x9F	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9F	TLS 1.2	✓	1
Cipher	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAA	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0,0xAC	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0,0x2B	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0,0xAD	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC0,0x2C	TLS 1.2	✓	1
Cipher	TLS_ECDHE_ECDSA_WITH_CHACHA20_ POLY1305_SHA256	0xCC,0xA9	TLS 1.2	✓	1
Cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC0,0x2F	TLS 1.2	✓	1
Cipher	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x30	TLS 1.2	✓	1

Category	Name	Value	TLS	Security	Protocol
Cipher	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA8	TLS 1.2	✓	1
Cipher	TLS_RSA_WITH_3DES_EDE_CBC_SHA	0x00,0x0A	TLS 1.0	Legacy	2
Cipher	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	0x00, 0x16	TLS 1.0	Legacy	2
Cipher	TLS_RSA_WITH_AES_128_CBC_SHA	0x00, 0x2F	TLS 1.0	Legacy	2
Cipher	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x00,0x33	TLS 1.0	Legacy	2
Cipher	TLS_RSA_WITH_AES_256_CBC_SHA	0x00, 0x35	TLS 1.0	Legacy	2
Cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x00,0x39	TLS 1.0	Legacy	2
Cipher	TLS_RSA_WITH_AES_128_CBC_SHA256	0x00, 0x3C	TLS 1.0	Legacy	2
Cipher	TLS_RSA_WITH_AES_256_CBC_SHA256	0x00, 0x3D	TLS 1.0	Legacy	2
Cipher	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x00,0x67	TLS 1.0	Legacy	2
Cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x00,0x6B	TLS 1.0	Legacy	2
Cipher	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	0xC0,0x12	TLS 1.0	Legacy	2
Cipher	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0xC0,0x13	TLS 1.0	Legacy	2
Cipher	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xC0,0x14	TLS 1.0	Legacy	2
Cipher	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xC0,0x27	TLS 1.0	Legacy	2
Cipher	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xC0,0x28	TLS 1.0	Legacy	2
DSA	DSA_SHA256	0x0402		✓	1
DSA	DSA_SHA384	0x0502		✓	1
DSA	DSA_SHA512	0x0602		✓	1
DSA	ecdsa_secp256r1_sha256	0x0403		✓	1
DSA	ecdsa_secp384r1_sha384	0x0503		✓	1
DSA	ecdsa_secp521r1_sha512	0x0603		✓	1
SEA	ed25519	0x0807		✓	1
SEA	ed448	0x0808		✓	1
SEA	rsa_pss_pss_sha256	0x0804		✓	1
SEA	rsa_pss_pss_sha384	0x0805		✓	1
SEA	rsa_pss_pss_sha512	0x0806		✓	1
SEA	rsa_pss_rsae_sha256	0x0809		✓	1
SEA	rsa_pss_rsae_sha384	0x080A		✓	1
SEA	rsa_pss_rsae_sha512	0x080B		✓	1
DSA	rsa_pkcs1_sha256	0x0401		✓	1, 2
DSA	rsa_pkcs1_sha384	0x0501		✓	1, 2
DSA	rsa_pkcs1_sha512	0x0601		✓	1
DSA	rsa_pkcs1_sha1	0x0201		Legacy	2
DSA	MD5_rsa	0x0101		Legacy	2

A.3 Syslog messages

The product outputs Syslog messages according to RFC 5424. The messages are based on IEC 62443-3-3.

You can find a more detailed description of the individual messages below.

A.3.1 Structure of the Syslog messages

Syslog messages record changes in device states as status information. Syslog messages according to RFC 5424 or RFC 5426 are output by devices and transferred to a server via the set UDP port (standard: 514). The Syslog server collects the information of the devices and informs you about these events.

The Syslog protocol prescribes a fixed sequence and structure of the possible parameters. Syslog messages according to RFC5424 have the following structure:

Part / Parameter	Explanation
HEADER	
PRI	Priority of the Syslog message, divided into: • Severity (Severity) Possible values: – 0 Emergency – 1 Alert – 2 Critical – 3 Error – 4 Warning – 5 Notice – 6 Information – 7 Debug • Facility (Origin) Possible values, e.g.: Sub-system, service, user
VERSION	Version number of the Syslog specification
TIMESTAMP	Time stamp of the device as UTC Format: YYYY-MM-DDThh:mm:ss.msmsmsmmsZ Example: 2020-01-01T00:03:15.29.255Z
HOSTNAME	Identifies the source device by either: • FQDN • IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX • IPv6 address according to RFC4291 Section 2.2 • Host name "-" is output if information is missing. In the product: The configured IPv4 or IPv6 address of the interface [X1]
APP-NAME	Device or application from which the message originates. "-" is output if information is missing. In the product: "-"
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing. In the product: "-"
MSGID	ID to identify the message. "-" is output if information is missing. In the product: "-"
STRUCTURED-DATA	

Part / Parameter	Explanation
timeQuality	The structured data element "timeQuality" provides information on system time with the two parameters "tzKnown" and "isSynced". Example: [timeQuality tzKnown="0" isSynced="0"] • tzKnown This parameter specifies whether the time zone is known in the source device. – 1 = known – 0 = unknown • isSynced This parameter specifies whether the source device is synchronized with a reliable external time source, e.g. via NTP. In the product: "-"
MSG	
MESSAGE	Message text as ASCII string (English)

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in the RFCs:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

A.3.2 Tags in Syslog messages

The variables are displayed in the section "Syslog messages" in the field "Message text" within curly brackets {variable}.

The output messages can contain the following variables:

Variable	Description	Format	Possible values or example
{IP address}	IPv4 address according to RFC1035 IPv6 address according to RFC4291 Section 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{Src port} {Dest port}	Source port number (decimal) Destination port number (decimal)	%d	0 ... 65535
{Src mac} {Dest mac}	Source MAC address Destination MAC address	%02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	Protocol or service used that generated the event.	%s	UDP | TCP | HTTPS | WBM | Telnet | SSH | Console | PNIO | PB | OPC | TFTP | SFTP
{User name}	String (without spaces) that identifies the authenticated user by his or her name.	%s	User name, e.g. "admin"
{Time seconds}	Number of seconds	%d	44
{Failed login count}	Number of failed login attempts	%d	10
{Config detail}	String (with spaces) for the identification of a part of the configuration	%s	OpenVPN

Variable	Description	Format	Possible values or example
{Reason}	Reason for message	%s	TCP_STORM_4
{ether-type_name}	Service or protocol	%s	ARP
{Version}	Firmware version	%s	V4.0.8
{Old Version}	Previous firmware version	%s	V4.0.6

A.3.3 Messages

The product outputs the following SYSLOG messages, sorted by classes.

User identification and authentication

Message text	{Protocol}: User {User name} logged in from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.0.1.
Explanation	Valid login information that was specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} failed to log in from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or password specified during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} logged out from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
Explanation	Session ended with user logout.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Unsuccessful login attempts

Message text	{Protocol}: User {User name} login from {IP address} rejected because of too many unsuccessful login attempts.
Example	HTTPS: User admin login from 192.168.0.1 rejected because of too many unsuccessful login attempts.

Explanation	In the example, the BFA prevention blocked the "admin" user after too many failed attempts, even though the user name and password were correct. Possible cause: System still in locked state
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	{Protocol}: {IP address} is locked for {Time seconds} seconds after {Failed login count} unsuccessful login attempts.
Example	HTTPS: 192.168.1.105 is locked for 600 seconds after 11 unsuccessful login tempts.
Explanation	The BFA prevention has blocked an IP address for a specific period after too many failed login attempts. In the example, the BFA prevention has blocked the IP address "192.168.1.105" for 600 seconds after 11 failed login attempts.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Access via untrusted networks

Message text	{Protocol}: Connection from {IP address} established.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 established.
Explanation	VPN connection is established.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	{Protocol}: Connection from {IP address} closed.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 closed.
Explanation	VPN connection is closed.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R1)

Message text	{Protocol}: Connection from {IP address} failed. Reason: {Reason}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 failed. Reason: unsuccessful authentication.
Explanation	VPN connection could not be established due to invalid authentication.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 005-R3)

Non-repudiation

Message text	{Protocol}: User {User name} has changed the {Config detail} configuration.
Example	Backplane: User MGT Subsystem has changed or reloaded configuration.
Explanation	In the example, the user "MGT Subsystem" has changed and/or loaded the configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{Protocol}: User {User name} has initiated a reset to factory defaults.
Example	SSH: User admin has initiated a reset to factory defaults.
Explanation	A user has initiated a reset to default settings. In the example, the user "admin" has initiated a reset to default settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Software and information integrity

Message text	{Protocol}: Software integrity check failed.
Example	WBM: Software integrity check failed.
Explanation	An error was detected while the software integrity was being checked.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Message text	Configdata integrity check failed.
Explanation	An error was detected while the configuration integrity was being checked.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Protection against DoS events

Message text (IP) Message text (MAC)	DOS attack detected! src={remote_addr} spt={remote_port} dst={local_addr} dpt={local_port} proto={protocol} reason={reason} DOS attack detected! src={remote_addr_mac} dst={local_addr_mac} proto={ethertype_name} reason={reason}
Example (IP) Example (MAC)	DOS attack detected! src=192.168.100.20 spt=48961 dst=192.168.100.12 dpt=8448 proto=TCP reason=TCP_STORM_4 DOS attack detected! src=ac-86-21-2b-aa-1a dst=ff-ff-ff-ff-ff-ff proto=ARP reason=BCAST_LIMIT
Explanation	A Denial of Service (DoS) attack was detected. Information on address, protocol and reason depending on address type (IPv4/IPv6 or MAC)
Severity	Alert

Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

Restoration of the automation system

Message text	{Protocol}: Firmware Version {Version} loaded.
Example	ASinternalComm: Firmware Version V4.0.36 loaded.
Explanation	In the example, the firmware version "V4.0.36" was successfully loaded via the "ASinternalComm" protocol.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{Protocol}: Firmware Version {Current Version} was activated. Prior version was {Old Version}.
Example	PowerOn: Firmware Version V4.0.36 was activated. Prior version was V4.0.35.
Explanation	In the example, the firmware version "V4.0.36" was activated. The previous firmware version was "V4.0.35".
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Index

A

Autocrossing mechanism, 49
Autosensing, 49

C

Cell protection concept
    VPN, 77
Commissioning
    Completeness of the STEP 7 project data, 40
Configuration, 40
Configuration limits
    Communications modules, 21
Connecting a switch, 49
Connection resources of the CPU, 22
Connections for Web
    Quantity, 23
Crossover cable, 49

D

Data management - Configuration data, 99
DHCP, 100
Disposal, 9
Double addressing in the network, 50
Downloading project data, 40
Downloading the configuration data, 26

E

E-mail, 16
E-mail connection, 22
Ethernet interface, 4, 31
    Configuration via T_CONFIG, 27
    Pin assignment, 41

F

FETCH/WRITE
    Communication service, 17
    Enable in CPU, 48
    Functions, 47
    S5/S7 addressing mode, 19
FETCH/WRITE connections, 22
Firewall, 20
Firmware version, 3
FTP
    Response if the reference to the FTP job block is missing, 69
FTP (FTP client), 21
FTP client
    Configuration limits, 24
FTP server
    Configuration limits, 24
FTP_CMD, 61
    Block execution time, 24
FTPS, 20
FTPS - Security, 58

G

Gateway (VPN), 83
Gigabit specification, 31
Glossary, 9

H

Hardware product version, 3
HMI communication, 16

I

Installation and commissioning, 40
    Procedure, 40
Instruction
    FTP_CMD, 27
    T_CONFIG, 27
    TCON, TSEND/TRCV, 26
    TDISCON, 26
    TMAIL_C, 26
    TSEND_C/TRCV_C, 26
    TUSEND/TURCV, 26
IP address
    IPv6, 19
    Via DHCP, 49
IP address band not permissible
    IPv4, 50
    IPv6, 50
IP configuration
    IPv4 / IPv6, 18
IP routing, 51
IPsec tunnel
    Number, 24

ISO transport (complying with RFC 8073), 16
ISO transport connections, 22
ISO-on-TCP (acc. to RFC 1006), 16
ISO-on-TCP connections, 22

L

LED display, 29
Logging, 20

M

MAC address, 4, 18
MIB, 94
Multicast
    via UDP, 16

N

NTP / NTP (secure), 56
NTP (secure), 20

O

Online diagnostics, 92
Online functions, 92
Online help of STEP 7, 40
OP connections
    Quantity, 23
Open User Communication (OUC), 16
Operating mode of the CPU, 41
OUC (Open User Communication), 88

P

Passive VPN connection establishment, 83
PG communication, 16
PG connections
    Quantity, 23
Port 8448, 93
Power supply modules
    Additional, 21
Program blocks - max. Data length, 22
Programmed communications connections, 54
Programmed connections
    Quantity, 23
PUT/GET
    Enable in CPU, 48

Q

Quantity
    Communications modules, 21

R

Recycling, 9
RUN → STOP, 41

S

S5/S7 addressing mode, 19
S7 communication, 16
S7 connections, 21
    Number of freely usable, 23
    R/H system, 16
Safety notices, 35
Security diagnostics, 93
SHA1 support (configuration/module replacement), 99
SIMATIC NET glossary, 9
SMTPS, 21
SNMP, 94
SNMP agent, 18
SNMPv3, 21
Special notes
    Connecting a switch, 49
STEP 7, 26
System data type
    FTP_..., 27
    TCON_..., 26
    TMail_..., 26
System data types (SDTs), 89

T

TCP (acc. to RFC 793), 16
TCP connections, 22
TCP connections for FTP, 24
Time-of-day synchronization, 18

U

UDP, 23
UDP (acc. to RFC 768), 16
UDP connections, 22

V

Virtual interface, 52
Virtual Private Network
    Definition, 76
VPN, (Virtual Private Network)
    Areas of application, 77
    Cell protection concept, 77

W

Web server, 19