

# SIEMENS

## SIMATIC NET

### S7-1500 - Industrial Ethernet CP 1543-1

#### Operating Instructions

#### Preface

---

Guide to the documentation

1

Product overview, functions

2

Installation, connecting up,  
commissioning, operation

3

Configuration, programming

4

Diagnostics and upkeep

5

Technical specifications

6

Approvals

7

## 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.

|  |
|--|
| <b>⚠ DANGER</b>  |
| indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken. |
| <b>⚠ WARNING</b>   |
| indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.  |
| <b>⚠ CAUTION</b>   |
| indicates that minor personal injury can result if proper precautions are not taken.                   |
| <b>NOTICE</b>  |
| 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:

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

### Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

### Disclaimer of Liability

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

# Preface

## 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.

## New in this issue

- Firmware version V2.1 with the following new functions:
  - Extended security settings using IP routing via the backplane bus  
See section IP routing (Page 35).

## Version history

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

## Replaced edition

Edition 10/2016

## Current manual release 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>)

## Sources of information and other documentation

See section Guide to the documentation (Page 9).

## Abbreviations and names

- CP

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

- STEP 7

The name STEP 7 is used to mean the STEP 7 Professional configuration tool.

## Conventions

Make sure you read the special notices below:

---

### Note

A notice contains important information on the product described in the documentation, handling the product or about parts of the documentation you should pay particular attention to.

---

## See also

Program blocks for OUC (Page 44)

Configuring the FTP server function (Page 49)

## 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\_86.pdf

## Security information

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

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

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit  
Link: (<http://www.siemens.com/industrialsecurity>)

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

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

## Firmware

## Firmware

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

## SIMATIC NET glossary

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

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

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

## 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

|          |   |           |
|----------|---|-----------|
|          | <b>Preface.....</b>   | <b>3</b>  |
| <b>1</b> | <b>Guide to the documentation .....</b>                                 | <b>9</b>  |
| <b>2</b> | <b>Product overview, functions.....</b>                                 | <b>11</b> |
| 2.1      | Product data.....   | 11        |
| 2.2      | Communication services.....   | 12        |
| 2.3      | Further functions .....   | 13        |
| 2.4      | Industrial Ethernet Security.....                                       | 15        |
| 2.5      | Configuration limits and performance data.....                          | 16        |
| 2.5.1    | General characteristic data.....  | 16        |
| 2.5.2    | Characteristics for Open User Communication (OUC) and FETCH/WRITE ..... | 16        |
| 2.5.3    | Characteristics of S7 communication .....                               | 18        |
| 2.5.4    | Characteristic data for FTP / FTPS mode.....                            | 19        |
| 2.5.5    | Characteristics security.....   | 19        |
| 2.6      | Requirements for use .....  | 20        |
| 2.6.1    | Configuration limits.....   | 20        |
| 2.6.2    | Project engineering.....  | 20        |
| 2.6.3    | Programming.....  | 21        |
| 2.7      | LEDs.....   | 22        |
| 2.8      | Gigabit interface .....   | 24        |
| <b>3</b> | <b>Installation, connecting up, commissioning, operation.....</b>       | <b>25</b> |
| 3.1      | Important notes on using the device .....                               | 25        |
| 3.1.1    | Notes on use in hazardous areas .....                                   | 25        |
| 3.1.2    | Notes on use in hazardous areas according to ATEX / IECEx.....          | 26        |
| 3.1.3    | Notes on use in hazardous areas according to UL HazLoc .....            | 27        |
| 3.1.4    | General notices on use in hazardous areas according to FM .....         | 27        |
| 3.2      | Installing and commissioning the CP 1543-1.....                         | 28        |
| 3.3      | Mode of the CPU - effect on the CP .....                                | 29        |
| <b>4</b> | <b>Configuration, programming .....</b>                                 | <b>31</b> |
| 4.1      | Security recommendations .....  | 31        |
| 4.2      | Network settings.....   | 34        |
| 4.3      | IP configuration .....  | 35        |
| 4.3.1    | Points to note about IP configuration .....                             | 35        |
| 4.3.2    | Restart after detection of a duplicate IP address in the network.....   | 35        |
| 4.3.3    | IP routing.....   | 35        |
| 4.4      | Security.....   | 36        |
| 4.4.1    | VPN .....   | 36        |
| 4.4.1.1  | Creating VPN tunnel communication between S7-1500 stations .....        | 37        |

|          |  |           |
|----------|--|-----------|
| 4.4.1.2  | Successfully establishing VPN tunnel communication between the CP 1543-1 and SCALANCE M..... | 39        |
| 4.4.1.3  | VPN tunnel communication with SOFTNET Security Client.....                                   | 39        |
| 4.4.1.4  | CP as passive subscriber of VPN connections.....   | 40        |
| 4.4.2    | Firewall .....   | 41        |
| 4.4.2.1  | Firewall sequence when checking incoming and outgoing frames.....                            | 41        |
| 4.4.2.2  | Notation for the source IP address (advanced firewall mode).....                             | 41        |
| 4.4.2.3  | HTTP and HTTPS not possible with IPv6.....   | 41        |
| 4.4.2.4  | Firewall settings for connections via a VPN tunnel.....                                      | 41        |
| 4.4.3    | Online functions .....   | 42        |
| 4.4.3.1  | Online diagnostics via port 8448.....  | 42        |
| 4.4.3.2  | Online diagnostics and downloading to station with the firewall activated .....              | 42        |
| 4.4.4    | Filtering of the system events .....   | 43        |
| 4.5      | Time-of-day synchronization.....   | 43        |
| 4.6      | Program blocks for OUC.....  | 44        |
| 4.7      | Setting up FTP communication.....  | 47        |
| 4.7.1    | The program block FTP_CMD (FTP client function) .....  | 47        |
| 4.7.2    | Configuring the FTP server function.....   | 49        |
| 4.8      | IP access protection with programmed communications connections.....                         | 52        |
| <b>5</b> | <b>Diagnostics and upkeep.....</b>   | <b>53</b> |
| 5.1      | Diagnostics options .....  | 53        |
| 5.2      | Diagnostics with SNMP .....  | 53        |
| 5.3      | Replacing a module without a programming device .....  | 56        |
| <b>6</b> | <b>Technical specifications.....</b>   | <b>57</b> |
| <b>7</b> | <b>Approvals.....</b>  | <b>59</b> |
|          | <b>Index.....</b>  | <b>65</b> |



# Guide to the documentation

## Introduction

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 and device manuals.

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

## Overview of the documentation on communication with S7-1500

The following table lists additional documents, which supplement this description of CP 1543-1 and are available in the Internet.

Table 1- 1 Configuration tools for the CP 1543-1

| Topic              | Documentation   | Most important contents   |
|--------------------|---|---|
| System description | System manual: S7-1500 Automation System<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59191792">https://support.industry.siemens.com/cs/ww/en/view/59191792</a> ) | <ul style="list-style-type: none"> <li>• Application planning</li> <li>• Installation</li> <li>• Connecting</li> <li>• Commissioning</li> </ul> |
| System diagnostics | Function manual: System diagnostics<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59192926">https://support.industry.siemens.com/cs/ww/en/view/59192926</a> )      | <ul style="list-style-type: none"> <li>• Overview</li> <li>• Diagnostics evaluation for hardware/software</li> </ul>                            |
| Communication      | Function manual: Communication<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59192925">https://support.industry.siemens.com/cs/ww/en/view/59192925</a> )           | <ul style="list-style-type: none"> <li>• Overview</li> </ul>  |
|                    | Function manual: Web Server<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59193560">https://support.industry.siemens.com/cs/ww/en/view/59193560</a> )              | <ul style="list-style-type: none"> <li>• Function</li> <li>• Operation</li> </ul>   |
|                    | Manual Industrial Ethernet Security<br>( <a href="https://support.industry.siemens.com/cs/ww/en/ps/15326/man">https://support.industry.siemens.com/cs/ww/en/ps/15326/man</a> )        | <ul style="list-style-type: none"> <li>• Overview and description of the security functions in Industrial Ethernet</li> </ul>                   |

| Topic   | Documentation  | Most important contents  |
|---|--|--|
|   | SIMATIC NET - Industrial Ethernet / PROFINET - system manual <ul style="list-style-type: none"> <li>Industrial Ethernet<br/>Link: (<a href="https://support.industry.siemens.com/cs/w/de/view/27069465">https://support.industry.siemens.com/cs/w/de/view/27069465</a>)</li> <li>Passive network components<br/>Link: (<a href="https://support.industry.siemens.com/cs/w/en/view/84922825">https://support.industry.siemens.com/cs/w/en/view/84922825</a>)</li> </ul> | <ul style="list-style-type: none"> <li>Ethernet networks</li> <li>Network configuration</li> <li>Network components</li> </ul>                           |
| Interference-free installation of control systems | Function Manual: Interference-free installation of control systems<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59193566">https://support.industry.siemens.com/cs/ww/en/view/59193566</a> )  | <ul style="list-style-type: none"> <li>Basics</li> <li>Electromagnetic compatibility</li> <li>Lightning protection</li> <li>Housing selection</li> </ul> |
| Cycle and response times                          | Function manual: Cycle and Response Times<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59193558">https://support.industry.siemens.com/cs/ww/en/view/59193558</a> )   | <ul style="list-style-type: none"> <li>Basics</li> <li>Calculations</li> </ul>   |

## SIMATIC manuals

All current manuals for SIMATIC products are available for download free of charge from the Internet:

Link: (<http://www.siemens.com/automation/service&support>)

## CP documentation in the Manual Collection (article number A5E00069051)

The "SIMATIC NET Manual Collection" DVD contains the device manuals and descriptions of all SIMATIC NET products current at the time it was created. It is updated at regular intervals.

## Version History / Current Downloads for the SIMATIC NET S7 CPs

The "Version History/Current Downloads for SIMATIC NET S7 CPs (Industrial Ethernet)" document provides information on all CPs available up to now for SIMATIC S7 (Industrial Ethernet).

The current versions of the document can be found on the Internet:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/109474421>)

## Product overview, functions

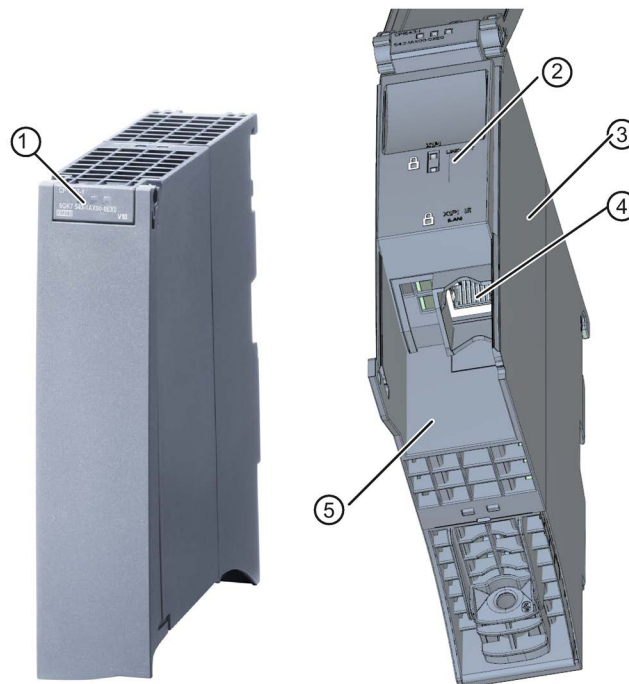
### 2.1 Product data

#### Article number, validity and product names

This description contains information on the following product

CP 1543-1  
 article number 6GK7 543-1AX00-0XE0  
 hardware product version 2  
 firmware version V2.1  
 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 2-1 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 MAC address printed on the module for module configuration! This ensures that you assign a unique MAC address in the subnet!

### Application

The CP is intended for operation in an S7-1500 automation system. It allows the S7-1500 to be connected to Industrial Ethernet.

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

## 2.2 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 (complying with RFC 793), ISO-on-TCP (complying with RFC 1006) and UDP (complying with RFC 768)

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

- 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 "SMTP-Auth" for authentication on an e-mail server.

- **S7 communication**

- PG communication
- Operator control and monitoring functions (HMI communication)
- Data exchange over S7 connections

- **IT functions**
  - FTP functions (File Transfer Protocol FTP/FTPS) for file management and access to data blocks on the CPU (client and server functions).
  - For e-mail see above (OUC)
- **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.

## 2.3 Further functions

### Timeofday synchronization over Industrial Ethernet using the NTP mode (NTP: Network Time Protocol)

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

The time 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 for secure time-of-day synchronization and transfer of the time of day.

### Addressable with the factoryset MAC address

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

### SNMP agent

The CP supports data queries over SNMP in version V1 (Simple Network Management Protocol). It delivers the content of certain MIB objects according to the MIB II standard 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 Programming (Page 21)).

Note: Does not apply to S7 connections.

## IP routing

The CP supports static IP routing (IPv4) to other CM 1542-1 V2.0 / CP 1543-1 V2.0.

For details, see section IP routing (Page 35).

## IPv6 addresses - area of use on the CP

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

- FTP server mode
- FETCH/WRITE access (CP is server)
- FTP client mode with addressing via a program block
- E-mail transfer with addressing via a program block

## 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; refer to the section Guide to the documentation (Page 9)

---

### 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.

## 2.4 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 1543-1 can be protected by a combination of different 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 Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)
  - Bandwidth limitation
  - Global firewall rules

The firewall protective function can be applied to the operation of single devices, several devices, or entire network segments.

- Logging

To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a syslog server.
- FTPS (explicit mode)

For encrypted transfer of files.
- NTP (secure)

For secure time-of-day synchronization and transmission
- SMTPS

For 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 31).

## 2.5 Configuration limits and performance data

### 2.5.1 General characteristic data

| Characteristic   | Explanation / values   |
|--|--|
| Total number of freely usable connections on Industrial Ethernet | 118<br>The value applies to the total number of connections of the following types: <ul style="list-style-type: none"><li>• S7 connections</li><li>• Connections for open communications services</li><li>• FTP (FTP client)</li></ul> |

---

#### 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.

---

### 2.5.2 Characteristics for Open User Communication (OUC) and FETCH/WRITE

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   | <ul style="list-style-type: none"> <li>• Number of configured and programmed +connections in total (ISO transport + ISO-on-TCP + TCP + UDP + FETCH/WRITE + e-mail): Max. 118</li> <li>Of which maximum:                             <ul style="list-style-type: none"> <li>– TCP connections: 1...118 <sup>1)</sup></li> <li>– ISO-on-TCP connections: 1...118</li> <li>– ISO transport connections: 1...118</li> <li>– Total number of UDP connections (specified and free) that can be configured: 1...118</li> <li>– Connection for e-mail: 1</li> <li>– Connections for FETCH/WRITE: 1...16</li> </ul> </li> </ul> <p>Notes:<br/> <sup>1)</sup>Avoid receive overload<br/>                     The flow control on TCP connections cannot control permanent overload of the recipient. You should therefore make sure that the processing capabilities of a receiving CP are not permanently exceeded by the sender (approximately 150200 messages per second).</p> |
| Maximum data length for program blocks  | <p>Program blocks allow the transfer of user data in the following lengths:</p> <ul style="list-style-type: none"> <li>• ISO-on-TCP, TCP, ISO transport: 1 to 64 kB</li> <li>• UDP: 1 to 1452 bytes</li> <li>• E-mail                             <ul style="list-style-type: none"> <li>– Job header + user data: 1 to 256 bytes</li> <li>– E-mail attachment: up to 64 kbytes</li> </ul> </li> </ul>  |
| LAN interface max. data field length generated by CP per protocol data unit (TPDU = transport protocol data unit) | <ul style="list-style-type: none"> <li>• sending                             <ul style="list-style-type: none"> <li>ISO transport, ISOonTCP, TCP: 1452 bytes / TPDU</li> </ul> </li> <li>• receiving                             <ul style="list-style-type: none"> <li>– ISO transport: 512 bytes / TPDU</li> <li>– ISO-on-TCP: 1452 bytes / TPDU</li> <li>– TCP: 1452 bytes / TPDU</li> </ul> </li> </ul>   |

**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, refer to the section Guide to the documentation (Page 9).

### Restrictions for UDP

- Restrictions UDP broadcast / multicast)

To avoid overloading the CP due to high broadcast / multicast frame traffic, the receipt of UDP broadcast / multicast on the CP is limited

- 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.

### 2.5.3 Characteristics of S7 communication

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

| Feature   | 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) | <ul style="list-style-type: none"><li>• for sending: 480 bytes / PDU</li><li>• for receiving: 480 bytes / PDU</li></ul> |
| Number of reserved OP connections   | 4   |
| Number of reserved PG connections   | 4   |
| Number of reserved connections for Web  | 2   |

---

#### 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.

---

## 2.5.4 Characteristic data for FTP / FTPS mode

### TCP connections for FTP

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

- FTP in client mode:

You can 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 in 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 (FB40) for FTP client mode

For communication, use the FTP 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.

## 2.5.5 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 140.90.120.0/16)
- Maximum 128 rules with limitation of the transmission speed ("bandwidth limitation")

## 2.6 Requirements for use

### 2.6.1 Configuration limits

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

- The number of CPs that can be operated in a rack depends on the CPU type being used.

By operating several CPs, you can increase the configuration limits listed below for the station as the 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.

Observe the information in the documentation on the CPU; see section Guide to the documentation (Page 9)

---

#### 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.

---

### 2.6.2 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. 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 version of STEP 7 is required:

| STEP 7 version                        | Functions of the CP  |
|---------------------------------------|--|
| STEP 7 Professional V12 SP1 or higher | The full functionality of the CP 1543-1 (6GK7 543-1AX00-0XE0) can be configured. |

## 2.6.3 Programming

### Program blocks

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

Table 2- 1 Instructions for communications services

| Protocol   | Program block (instruction)   | System data type   |
|------------|---|--|
| TCP        | Establish connection and send/receive data via:   | <ul style="list-style-type: none"> <li>• TCON_IP_v4</li> <li>• TCON_Configured</li> </ul>  |
| ISO-on-TCP | <ul style="list-style-type: none"> <li>• TSEND_C/TRCV_C or</li> <li>• TCON, TSEND/TRCV</li> </ul>                             | <ul style="list-style-type: none"> <li>• TCON_IP_RFC</li> </ul>  |
| ISO        | (termination of the connection using TDISCON possible)  | <ul style="list-style-type: none"> <li>• TCON_ISOnative</li> </ul>   |
| UDP        | <ul style="list-style-type: none"> <li>• TCON, TUSEND/TURCV</li> </ul> (termination of the connection using TDISCON possible) | <ul style="list-style-type: none"> <li>• TCON_IP_v4</li> </ul>   |
| E-mail     | <ul style="list-style-type: none"> <li>• TMAIL_C</li> </ul>   | <ul style="list-style-type: none"> <li>• TMail_v4*</li> <li>• TMail_v6*</li> <li>• TMAIL_FQDN*</li> </ul>  |
| FTP        | <ul style="list-style-type: none"> <li>• FTP_CMD</li> </ul>   | <ul style="list-style-type: none"> <li>• FTP_CONNECT_IPV4*</li> <li>• FTP_CONNECT_IPV6*</li> <li>• FTP_CONNECT_NAME*</li> <li>• FTP_FILENAME*</li> <li>• FTP_FILENAME_PART*</li> </ul> |

\*User-defined data type

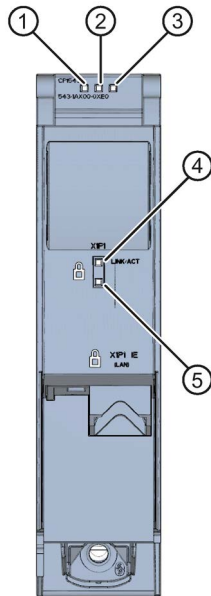
Table 2- 2 Instructions for configuration tasks

| Function                                | Program block (instruction)                                  | System data type  |
|---|--|---|
| Configuration of the Ethernet interface | <ul style="list-style-type: none"> <li>• T_CONFIG</li> </ul> | <ul style="list-style-type: none"> <li>• CONF_DATA</li> </ul> |

Refer to the documentation of the program blocks in the online help of STEP 7.

## 2.7 LEDs

### LEDs



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

Figure 2-2 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- 3 Meaning of the LEDs "RUN", "ERROR", "MAINT"

| RUN   | ERROR   | MAINT  | Meaning  |
|---|---|--|--|
| <br>LED off              | <br>LED off            | <br>LED off               | No supply voltage on the CP or supply voltage too low. |
| <br>LED lit green        | <br>LED lit red        | <br>LED lit yellow        | LED test during startup                                |
| <br>LED lit green        | <br>LED lit red        | <br>LED off               | Startup (booting the CP)                               |
| <br>LED lit green        | <br>LED off            | <br>LED off               | CP is in RUN mode.                                     |
| <br>LED lit green        | <br>LED flashing red   | <br>LED off               | No disruptions   |
| <br>LED lit green        | <br>LED flashing red   | <br>LED off               | A diagnostics event has occurred.                      |
| <br>LED lit green        | <br>LED off            | <br>LED lit yellow        | Maintenance, maintenance is demanded.                  |
| <br>LED lit green       | <br>LED off           | <br>LED flashing yellow  | Maintenance is required.                               |
| <br>LED flashing green | <br>LED off          | <br>LED off             | Downloading the user program                           |
| <br>LED flashing green | <br>LED off          | <br>LED off             | No CP configuration exists                             |
| <br>LED flashing green | <br>LED flashing red | <br>LED flashing yellow | Loading firmware                                       |
| <br>LED flashing green | <br>LED flashing red | <br>LED flashing yellow | Module fault<br>(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- 4 Meaning of the "LINK/ACT" LED

| LINK/ACT   |   | Meaning  |
|--|---|--|
|  green off      |  yellow off      | No connection to Ethernet<br>There is no Ethernet connection between the Ethernet interface of the CP and the communications partner.<br>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.  |
|  green on       |  yellow off      | Connection to Ethernet exists.<br>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.  |

## 2.8 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 28).



## 3.1 Important notes on using the device

### Safety notices on the use of the device

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

 **WARNING**

**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. Make sure 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).

### 3.1.1 Notes on use in hazardous areas

 **WARNING**

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

 **WARNING**

**EXPLOSION HAZARD**

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

 **WARNING**

**EXPLOSION HAZARD**

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

3.1 Important notes on using the device

 **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**

**DIN rail**

In the ATEX and IECEx area of application only the Siemens DIN rail 6ES5 710-8MA11 may be used to mount the modules.

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

 **WARNING**

**Requirements for the cabinet/enclosure**

To comply with EU Directive 94/9 (ATEX95), the enclosure or cabinet must meet the requirements of at least IP54 in compliance with EN 60529.

 **WARNING**

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

 **WARNING**

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

### 3.1.3 Notes on use in hazardous areas according to UL HazLoc

 **WARNING**

**EXPLOSION HAZARD**

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

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.

### 3.1.4 General notices on use in hazardous areas according to FM

 **WARNING**

**EXPLOSION HAZARD**

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

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

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


 **WARNING**

**EXPLOSION HAZARD**

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.

## 3.2 Installing and commissioning the CP 1543-1

### Installation and commissioning

|   |
|---|
|  <b>WARNING</b>  |
| <p><b>Read the system manual "S7-1500 Automation System"</b></p> <p>Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System" (references to documentation, refer to the section Guide to the documentation (Page 9)).</p> <p>Make sure that the power supply is turned off when installing/uninstalling the devices.</p> |

### Configuration

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

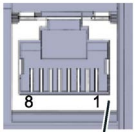
### Procedure for installation and commissioning

| 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.  | <p>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.</p> <p>You will find more detailed information on loading in the following sections of the STEP 7 online help:</p> <ul style="list-style-type: none"> <li>• "Compiling and loading project data"</li> <li>• "Using online and diagnostics functions"</li> </ul> |

## 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     |
| <br>Shielding | 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>)

## 3.3 Mode of the CPU - effect on the CP

You can change the mode of the CPU between RUN and STOP using the STEP 7 configuration software.

Depending on the operating status of the CPU, the CP behaves as described below.

### Changing the CPU from RUN to STOP:

When the CPU is in STOP mode, the CP remains in RUN and behaves as follows:

- For established connections (ISO transport, ISOonTCP, TCP, UDP connections), the following applies depending on the configuration:
  - Programmed connections are retained.
  - Configured connections are terminated.
- The following functions remain enabled:
  - The configuration and diagnostics of the CP (system connections for configuration, diagnostics, and PG channel routing are retained);
  - Web diagnostics
  - S7 routing function
  - Time-of-day synchronization

---

**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.

---

# Configuration, programming

## 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.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
- Check regularly for new features on the Siemens Internet pages.
  - Here you will find information on network security:  
Link: (<http://www.siemens.com/industrialsecurity>)
  - Here you will find information on Industrial Ethernet security:  
Link: (<http://w3.siemens.com/mcms/industrial-communication/en/ie/industrial-ethernet-security/Seiten/industrial-security.aspx>)
  - You will find an introduction to the topic of industrial security in the following publication:  
Link:  
([http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP01-0BA4\\_BR\\_Netzwerksicherheit\\_en\\_112015.pdf](http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP01-0BA4_BR_Netzwerksicherheit_en_112015.pdf))

### Physical access

Restrict physical access to the device to qualified personnel.

### Network attachment

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

## Security functions of the product

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

- Protection levels  
Configure access to the CPU under "Protection and 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 using the "bandwidth restriction" of the firewall, you can restrict the possibility of flooding and DoS attacks.  
The FETCH/WRITE functionality allows you to access any data of your PLC. 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.

## 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.



**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 configuring the port, 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.

| Protocol / function         | Port number (protocol) | Default of the port | Port status                              | Authentication                 |
|-----------------------------|------------------------|---------------------|--|--------------------------------|
| DHCP                        | 68 (UDP)               | Open                | Open after configuration (only outgoing) | No                             |
| DCP                         | 93 (UDP)               | Open                | Open                                     | No                             |
| DCE                         | 135 (TCP)              | Open                | Open                                     | Yes, when security is enabled. |
| S7 communication            | 102 (TCP)              | Open                | Open                                     | No                             |
| Online security diagnostics | 8448 (TCP)             | Closed              | Open after configuration                 |                                |
| NTP                         | 123 (UDP)              | Closed              | Open after configuration (only outgoing) | No                             |
| HTTP                        | 80 (TCP)               | Closed              | Open after configuration                 | No                             |
| HTTPS                       | 443 (TCP)              | Closed              | Open after configuration                 | Yes                            |

| Protocol / function | Port number (protocol) | Default of the port | Port status                          | Authentication    |
|---------------------|------------------------|---------------------|--------------------------------------|-------------------|
| FTP                 | 20 (TCP)<br>21 (TCP)   | Closed              | Open after configuration             | No                |
| FTPS                | 989 (TCP)<br>990 (TCP) | Closed              | Open after configuration             | Yes               |
| SNMP                | 161 (UDP)              | Open                | Open after configuration             | Yes (with SNMPv3) |
| SMTP                | 25 (TCP)               | Closed              | Open with block call (only outgoing) | No                |
| SMTPS               | 587 (TCP)              | Closed              | Open with block call (only outgoing) | No                |

## 4.2 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.

---

## 4.3 IP configuration

### 4.3.1 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.

---

### 4.3.2 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.

### 4.3.3 IP routing

#### IP routing via the backplane bus

The CP supports static IP routing (IPv4) to other CM 1542-1 / CP 1543-1. You can use IP routing, for example, for Web server access by lower-level modules.

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

#### Configuration

You can activate the IP routing in STEP 7 via the function "IP routing between communication modules". In the security settings, the corresponding function is called "IP routing via the backplane bus". When you activate the function, additional IP firewall rules are created which you can modify in the advanced firewall mode of the security settings.

IP routing runs via the configured default router. If you use several CPs in a station, of the modules in the station only one may be configured as a router.

## 4.4 Security

Note the range and application of the security functions of the CP in the section Industrial Ethernet Security (Page 15).

For the configuration limits, see section Characteristics security (Page 19).

The security functions are configured in STEP 7.

### 4.4.1 VPN

#### 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

#### 4.4.1.1 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.
- Both CPs are configured with a firmware version  $\geq$  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.

### Selecting the "Activate security features" check box

- After logging on, select the "Activate security features" check box for both CPs.  
You now have the security functions available 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.  
These properties define the default settings of the VPN group that you can change at any time.

---

### 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" check box is selected as default when you create a VPN group. You cannot deselect the check box.

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

### 4.4.1.2 Successfully establishing VPN tunnel communication between the CP 1543-1 and SCALANCE M

Creating VPN tunnel communication between the CP 1543-1 and SCALANCE M is the same as described in Procedure for S7-1500 stations (Page 37).

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

If the check box is not selected, the CP 1543-1 rejects establishment of the tunnel.

### 4.4.1.3 VPN tunnel communication with SOFTNET Security Client

Creating VPN tunnel communication between the CP SOFTNET Security Client and CP 1543-1 is the same as described in Procedure for S7-1500 stations (Page 37).

## 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 1543-1 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 establishment to the CP 1543-1.

To establish successful VPN tunnel communication to the CP 1543-1, 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 1543-1.
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 1543-1 can be established.

#### 4.4.1.4 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".



## 4.4.2 Firewall

### 4.4.2.1 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.

### 4.4.2.2 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 1543-1, 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.

### 4.4.2.3 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.

### 4.4.2.4 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 "Allow" for tunnel connections.

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

This applies to connections between a CP 1543-1 and for example a CP 343-1 Advanced, CP 443-1 Advanced, CP 1628 or CP 1243-1.

#### See also

Online diagnostics and downloading to station with the firewall activated (Page 42)

### 4.4.3 Online functions

#### 4.4.3.1 Online diagnostics via port 8448

##### Security diagnostics without opening port 102

If you want to perform security diagnostics without opening port 102, follow the steps below:

1. Select the CP in STEP 7.
2. Open the "Online & diagnostics" shortcut menu (right mouse button).
3. In the parameter group "Security > Status" click the "Connect online" button.

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

#### 4.4.3.2 Online diagnostics and downloading to station with the firewall activated

##### Setting the firewall for online functions

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

1. In the global security settings (see project tree), 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".
4. Now select the CP in the S7 station.
5. Enable the advanced firewall mode in the local security settings of the CP in the "Security > Firewall" parameter group.
6. Open the "IP rules" parameter group.
7. In the table, insert a new IP rule for the previously created global services as follows:
  - Action: Allow; "From external -> To station " with the globally created "Echo request" service
  - Action: Allow; "From station -> to external" with the globally created "Echo reply" service
8. For the IP rule for the Echo Request, enter the IP address of the engineering station in "Source IP address". This ensures that only ICMP frames (ping) from your engineering station can pass through the firewall.

#### 4.4.4 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.

## 4.5 Time-of-day synchronization

### General rules

The CP supports the following mode for timeofday synchronization:

- NTP mode (NTP: Network Time Protocol)

---

#### Note

##### Recommendation for setting the time

Synchronization with an 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

##### Special feature of time-of-day synchronization using NTP

If the option "Accept time from non-synchronized NTP servers" is not selected, the response is as follows:

If the CP receives a time of day frame from an unsynchronized NTP server with stratum 16, the time of day is not set according to the frame. In this case, none of the NTP servers is displayed as "NTP master" in the diagnostics; but rather only as being "reachable".

---

### Security

In the extended NTP configuration, you can create and manage additional NTP servers.

---

#### Note

##### Ensuring a valid time of day

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

---

## Configuration

For more detailed information on configuration, refer to the STEP 7 online help of the "Time-of-day synchronization" parameter group.

## 4.6 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
- 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.

## 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.

- **Configured connections:**
  - **TCON\_Configured**  
For transferring frames via TCP
- **Programmed connections:**
  - **TCON\_IP\_V4**  
For transferring frames via TCP or UDP
  - **TCON\_IP\_V4\_SEC**  
For the secure transfer of frames via TCP
  - **TCON\_QDN**  
For transferring frames via TCP or UDP
  - **TCON\_QDN\_SEC**  
For the secure transfer of frames via TCP
  - **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.

## 4.7 Setting up FTP communication

### 4.7.1 The program block FTP\_CMD (FTP client function)

#### Meaning

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

---

#### 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- 1 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

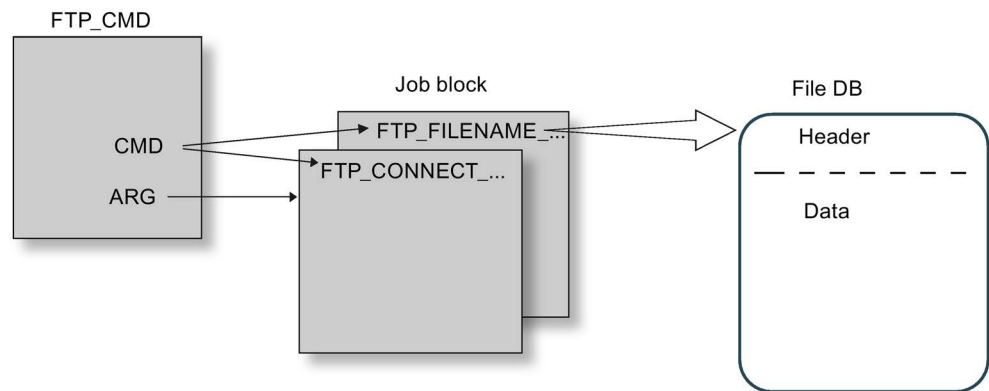
FTPS requires a comparison of the certificates between FTP server and FTP client. If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server. Import the certificate of the FTP server as a trusted certificate in the certificate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

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.

### 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).

### FTP access using the FTP\_CMD instruction - parameters 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.

---

### 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.

---

## 4.7.2 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".
- 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 CP firmware V2.0 and CPU firmware V2.0.

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).

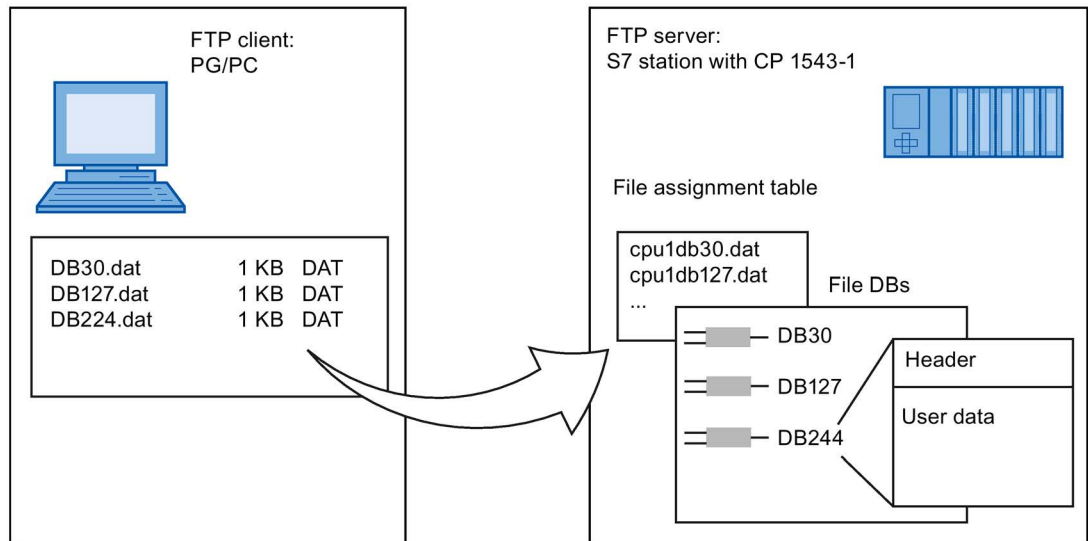


Figure 4-1 S7 CPU with CP 1543-1 as FTP server for the S7 CPU data

## 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                 |
|----------------|---|---|--|-------------------------|
| <b>Meaning</b> | Assignment of the CPU<br>Selectable from drop-down list | No. of the data block (file DB)<br>Selectable from drop-down list | The file name assigned to the file DB<br>Automatic name proposal; entry can be edited. | Informal comment        |
| <b>Example</b> | 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")

**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.

## 4.8 IP access protection with programmed communications connections

**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.

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

The configuration of IP access protection and the aspects of activated security are described in the online help of STEP 7.

## Diagnostics and upkeep

### 5.1 Diagnostics options

#### Diagnostics options

You have the following diagnostics options available for the module:

- The LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 22).

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

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

- Information on the online status of the module

- STEP 7: Diagnostics functions in the "Online > Online and diagnostics" menu

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

- General information on the module
- Diagnostics status
- Information on the Ethernet interface
- Security (with security enabled)

You can obtain further information on the diagnostics functions of STEP 7 in the STEP 7 online help.

- SNMP

You will find detailed information about the supported functions in the section Diagnostics with SNMP (Page 53).

### 5.2 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!

## 5.3 Replacing a module without a programming device

### General procedure

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

---

#### Note

##### Configured MAC address is adopted

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

---

### Module replacement: Special feature of IP address assignment from a DHCP server (IPv4)

During configuration of the CP you can specify the IP configuration in the properties dialog; one option is to obtain the IP address from a DHCP server.

---

#### Note

##### Recommendation: Configuring a client ID

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

Ideally, you should therefore configure IP as follows:

- Always configure a client ID and configure your DHCP server accordingly. This makes sure that after replacing the module, you always obtain the same IP address from the DHCP server.

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

---



## Technical specifications

Note the information in the System description of SIMATIC S7-1500 (Page 9).

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

| <b>Technical specifications - CP 1543-1</b>                                  |  |
|--|--|
| Product name   | CP 1543-1  |
| Article number   | 6GK7 543-1AX00-0XE0  |
| <b>Attachment to Industrial Ethernet</b>                                     |  |
| • Number   | 1 x Ethernet (gigabit) interface   |
| • Design   | RJ-45 jack   |
| • Transmission speed   | 10 / 100/ 1000 Mbps  |
| <b>Electrical data</b>   |  |
| Power supply   |  |
| • via S7-1500 backplane bus  | 15 V   |
| Current consumption  |  |
| • From backplane bus   | 350 mA   |
| • Power dissipation  | 5.3 W  |
| Insulation   |  |
| Insulation tested with   | 707 VDC (type test)  |
| <b>Design, dimensions and weight</b>   |  |
| 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  |
| <b>Permitted cable lengths (Alternative combinations per length range) *</b> |  |
| 0 ... 55 m   | <ul style="list-style-type: none"> <li>• Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180</li> <li>• Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet</li> </ul>   |
| 0 ... 85 m   | <ul style="list-style-type: none"> <li>• Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180</li> <li>• Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet</li> </ul> |

---

**Technical specifications - CP 1543-1**

---

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

---

**Product functions \*\***

---

\* For details, refer to the IK PI catalog, cabling technology

\*\* You will find the product functions in the section Product overview, functions (Page 11).

# Approvals

## 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>)

## EC declaration of conformity



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

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

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

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

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

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

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

The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft  
Division Process Industries and Drives  
Process Automation

DE-76181 Karlsruhe  
Germany

You will find the EC Declaration of Conformity on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15340/cert>)

The current versions of the standards can be seen in the EC Declaration of Conformity and in the certificates.

## IECEX

The product meet the requirements of explosion protection according to IECEx.

IECEX classification: Ex nA IIC T4 Gc

The product meets the requirements of the following standards:

- EN 60079-0  
Hazardous areas - Part 0: Equipment - General requirements
- EN 60079-15  
Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

You can see the current versions of the standards in the IECEx certificate that you will find on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15340/cert>)

The conditions must be met for the safe deployment of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 26).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/78381013>)

## ATEX



The product meets the requirements of the EC directive:2014/34/EC "Equipment and Protective Devices for Use in Potentially Explosive Atmospheres".

Applied standards:

- EN 60079-0  
Hazardous areas - Part 0: Equipment - General requirements
- EN 60079-15  
Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

The current versions of the standards can be seen in the EC Declaration of Conformity, see above.

ATEX approval: II 3 G Ex nA IIC T4 Gc

Test number: DEKRA 12 ATEX 0240X

The conditions must be met for the safe deployment of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 26).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find here:

- In the SIMATIC NET Manual Collection in "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>)

## EMC

Until 19.04.2016 the product meets the requirements of the EC Directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive).

Applied standards:

- EN 61000-6-4  
Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
- EN 61000-6-2  
Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments

## RoHS

The product meets the requirements of the EC directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Applied standard:

- EN 50581:2012

## 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 CP

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 (Page 27).

---

**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 사용하는 것을 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>)





# Index

## A

Autocrossing mechanism, 34  
Autosensing, 34

## B

Bandwidth limitation, 15  
Block execution time, 19

## C

Cell protection concept  
    VPN, 37  
Changing CPU mode  
    From RUN to STOP, 29  
Commissioning  
    Completeness of the STEP 7 project data, 28  
Configuration, 28  
Configuration and downloading the configuration data, 20  
Configuration of the Ethernet interface, 21  
    Instruction, 21  
Connecting a switch, 34  
Connection resources of the CPU, 16  
Connections for Web  
    Number, 18  
Crossover cable, 34

## D

Data storage of the configuration data of the CP, 56  
DHCP server, 56  
Diagnostics options, 53  
Disposal, 5  
Double addressing in the network, 35  
Downloading project data, 28  
Downloads, 10

## E

E-mail, 12, 17, 21  
EMC - electromagnetic compatibility, 59  
Ethernet interface, 11, 24  
    Pin assignment, 29

## F

FETCH/WRITE, 13, 17  
    S5/S7 addressing mode, 14  
Firewall, 15  
Firewall configuration, 52  
Firmware version, 11  
FTP, 21, 47  
FTP (FTP client), 16  
FTP in client mode  
    Configuration limits, 19  
FTP in server mode  
    Configuration limits, 19  
FTP\_CMD, 47  
FTPS, 47  
FTPS - Security, 52  
FTPS (explicit mode), 15

## G

Gateway, 40  
Gigabit specification, 24  
Global firewall rules, 15  
Glossary, 5

## H

Hardware product version, 11  
HMI communication, 12

## I

Installation and commissioning, 28  
    Procedure, 28  
Instruction  
    FTP\_CMD, 19, 21  
    T\_CONFIG, 21  
    TCON, TSEND/TRCV, 21  
    TDISCON, 21  
    TMAIL\_C, 21  
    TSEND\_C/TRCV\_C, 21  
    TUSEND/TURCV, 21  
IP access protection, 52

- IP address
  - IPv6, 14
  - Via DHCP, 35
- IP configuration
  - IPv4 / IPv6, 14
- IP routing, 35
- IPsec tunnel
  - Number, 19
- ISO, 21
- ISO transport (complying with RFC 8073), 12
- ISO transport connections, 17
- ISO-on-TCP, 21
- ISO-on-TCP (acc. to RFC 1006), 12
- ISO-on-TCP connections, 17
- IT functions, 13

## L

- LED display, 22
- Logging, 15

## M

- MAC address, 11, 13, 56
- Manual Collection, 10
- Maximum data length for program blocks, 17
- MIB, 53
- Module replacement
  - Special feature of IP address assignment from a DHCP server (IPv4), 56
- Multicast
  - via UDP, 12

## N

- NTP (secure), 15, 43
- NTP mode, 13
- NTP server, 43
- Number
  - Operable CPs, 20
- Number of connections, 17

## O

- Online help of STEP 7, 28
- OP connections
  - Number, 18
- Open User Communication (OUC), 12
- OUC (Open User Communication), 44
- Overall configuration limits, 20

## P

- Passive VPN connection establishment, 40
- PG communication, 12
- PG connections
  - Number, 18
- Port 8448, 42
- Power supply modules
  - Additional, 20
- PROFINET interface
  - LEDs, 24
- Program block, (Instruction)
- Programmed communications connections, 52

## R

- Recycling, 5

## S

- S5/S7 addressing mode, 14
- S7 communication, 12
- S7 connections, 12, 16
  - Number of freely usable, 18
- S7 routing function, 29
- Safety notices, 25
- Security diagnostics without port 102, 42
- Security SDTs, 45
- SIMATIC NET, 10
- SIMATIC NET glossary, 5
- SMTPS, 15
- SNMP, 53
- SNMP agent, 13
- SNMPv3, 15
- Special notes
  - Connecting a switch, 34
  - Ensuring a valid time of day, 43
  - Recommendation for setting the time, 43
  - Response if the reference to the FTP job block is missing, 49
- Stateful packet inspection (layer 3 and 4), 15
- STEP 7, 4, 20
- System data type
  - CONF\_DATA, 21
  - FTP\_CONNECT\_IPV4, 21
  - FTP\_CONNECT\_IPV6, 21
  - FTP\_CONNECT\_NAME, 21
  - FTP\_FILENAME, 21
  - FTP\_FILENAME\_PART, 21
  - TCON\_Configured, 21
  - TCON\_IP\_v4, 21, 21
  - TCON\_ISOnative, 21, 21

TMAIL\_FQDN, 21  
TMail\_v4, 21  
TMail\_v6, 21  
System data types (SDTs), 45

## T

TCON, 52  
TCP, 21  
TCP (acc. to RFC 793), 12  
TCP connections, 17  
TCP connections for FTP, 19  
Time synchronization, 13  
Time-of-day synchronization, 29

## U

UDP  
    Restrictions, 18  
UDP (acc. to RFC 768), 12  
UDP connections, 17  
UDP frame buffering, 18

## V

Version history, 10  
Virtual Private Network  
    Definition, 36  
VPN, (Virtual Private Network)  
    Areas of application, 36  
    Cell protection concept, 37

## W

Web diagnostics, 29  
Web server, 14

