

## SIMATIC NET

### S7-1500 - Industrial Ethernet SIMATIC CP 1545-1

#### Operating Instructions

#### Preface

#### Application and functions

**1**

#### LEDs, connectors

**2**

#### Connection, mounting, commissioning, disassembly

**3**

#### Configuration

**4**

#### Program blocks

**5**

#### Diagnostics and maintenance

**6**

#### Technical specifications

**7**

#### Approvals

**8**

#### Dimension drawings

**9**

#### Additional information

**A**

#### Syslog messages

**B**

## Legal information

### Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

#### **DANGER**

indicates that death or severe personal injury **will** result if proper precautions are not taken.

#### **WARNING**

indicates that death or severe personal injury **may** result if proper precautions are not taken.

#### **CAUTION**

indicates that minor personal injury can result if proper precautions are not taken.

#### **NOTICE**

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

### Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

### Proper use of Siemens products

Note the following:

#### **WARNING**

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

### Trademarks

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

### Disclaimer of Liability

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

# Preface

## CAUTION

To prevent injury, read the manual before use.

## Validity of the document

This document is valid for the following product:

- CP 1545-1  
Article number 6GK7545-1GX00-0XE0  
Hardware version 1  
Firmware version V1.1

Communication processor for connecting SIMATIC S7-1500 to Industrial Ethernet  
Communication functions: TCP/IP, UDP, S7, FTP Client/Server, E-mail, Connection to cloud systems via MQTT



Figure 1 S7-1500 with CP 1545-1 (right)

## Purpose of the document

The document describes the application and properties of the device. It supports you during configuration and shows maintenance and diagnostic options.

## New in this edition

Firmware version V1.1, including the following new functions:

- Improvement of the CloudConnect functionality, for example:
  - Linking the time trigger to the topic / group.
  - Export / import of the payload format
- Configurable CP diagnostics during runtime, refer to section CP diagnostics (Page 47).
- Configurable UDP buffering, refer to section Settings (Page 42).

Note the restrictions on DHCP and LLDP in the sections below.

- Special features on DHCP (Page 45)
- Security (Page 50)

## Replaced edition

Edition 12/2019

## Document on the Internet

You will also find the current issue of this document on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/man>)

## Required experience

To install, commission and operate the device, you require experience in the following areas:

- General electrical engineering
- Automation engineering / STEP 7 Professional

## Notes on this document

### Abbreviations and names

- **CP / device / module**

Designations for the communication processor CP 1545-1

- **ES**

Engineering station with STEP 7 Professional

- **Station**

SIMATIC S7 station

- **STEP 7**

Used for the configuration tool STEP 7 Professional

**Cross-references**

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

**Search**

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

**Sources of information and other documentation**

See below, Documentation guide.

You can find an application example of the CP on the following page:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/ae>)

You can find additional literature about S7-1500 in the "Documentation guide" section.

**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\_CP15451\_99.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 constitute one element of such a concept.

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

For additional information on industrial security measures that may be implemented, please visit

Link: (<http://www.siemens.com/industrialsecurity>)

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

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

## Firmware

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

## Note on firmware/software support

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

## Documentation guide

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

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

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

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

Table 1 Overview of the documentation for S7-1500

| Topic              | Documentation                                                                                                                                                                                                                                                                                                                                   | Most important contents                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| System description | System manual: S7-1500 Automation System ( <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 | System diagnostics ( <a href="https://support.industry.siemens.com/cs/ww/en/view/59192926">https://support.industry.siemens.com/cs/ww/en/view/59192926</a> ) function manual                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• Overview</li> <li>• Diagnostics evaluation for hardware/software</li> </ul>                            |
| Communication      | Communication ( <a href="https://support.industry.siemens.com/cs/ww/en/view/59192925">https://support.industry.siemens.com/cs/ww/en/view/59192925</a> ) function manual<br>Web server ( <a href="https://support.industry.siemens.com/cs/ww/en/view/59193560">https://support.industry.siemens.com/cs/ww/en/view/59193560</a> ) function manual | <ul style="list-style-type: none"> <li>• Overview</li> <li>• Function</li> <li>• Operation</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:<br/>(<a href="https://support.industry.siemens.com/cs/ww/de/view/27069465">https://support.industry.siemens.com/cs/ww/de/view/27069465</a>)</li> <li>Passive network components<br/>Link:<br/>(<a href="https://support.industry.siemens.com/cs/ww/en/view/84922825">https://support.industry.siemens.com/cs/ww/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 | Designing interference-free controllers<br>( <a href="https://support.industry.siemens.com/cs/ww/en/view/59193566">https://support.industry.siemens.com/cs/ww/en/view/59193566</a> ) function manual                                                                                                                                                                                                                                                                               | <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>                                                                           |

## CP documentation on DVD

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

## Device defective

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

## Decommissioning

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

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

## Recycling and disposal



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

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

Keep to the local regulations.

You will find information on returning the product on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/109479891>)

### **SIMATIC NET glossary**

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

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

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

### **Training, Service & Support**

You will find information on training, service and support in the multilanguage document "DC\_support\_99.pdf" on the Internet pages of Siemens Industry Online Support:

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

# Table of contents

|          |                                                                                 |           |
|----------|---------------------------------------------------------------------------------|-----------|
|          | <b>Preface .....</b>                                                            | <b>3</b>  |
| <b>1</b> | <b>Application and functions.....</b>                                           | <b>13</b> |
| 1.1      | Application .....                                                               | 13        |
| 1.2      | Communication services .....                                                    | 13        |
| 1.3      | Cloud communication.....                                                        | 14        |
| 1.4      | Further functions .....                                                         | 16        |
| 1.5      | Industrial Ethernet Security .....                                              | 18        |
| 1.6      | Configuration limits and performance data.....                                  | 19        |
| 1.6.1    | Configuration limits of communications modules .....                            | 19        |
| 1.6.2    | General characteristic data.....                                                | 20        |
| 1.6.3    | Characteristic data CloudConnect.....                                           | 20        |
| 1.6.4    | Characteristics of S7 communication.....                                        | 21        |
| 1.6.5    | Characteristic data for OUC and FETCH/WRITE.....                                | 21        |
| 1.6.6    | Characteristic data for FTP / FTPS mode .....                                   | 23        |
| 1.6.7    | Characteristics of security - firewall rules .....                              | 23        |
| 1.7      | Requirements for use.....                                                       | 24        |
| 1.7.1    | Usable CPUs.....                                                                | 24        |
| 1.7.2    | CPs .....                                                                       | 24        |
| 1.7.3    | Software requirements .....                                                     | 24        |
| <b>2</b> | <b>LEDs, connectors.....</b>                                                    | <b>25</b> |
| 2.1      | LEDs .....                                                                      | 25        |
| 2.2      | Gigabit interface .....                                                         | 27        |
| <b>3</b> | <b>Connection, mounting, commissioning, disassembly.....</b>                    | <b>29</b> |
| 3.1      | Important notes on using the device .....                                       | 29        |
| 3.1.1    | Notes on use in hazardous areas .....                                           | 29        |
| 3.1.2    | Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex ..... | 30        |
| 3.1.3    | Notes on use in hazardous areas according to UL HazLoc and FM.....              | 31        |
| 3.2      | Installation, removal and repairs in hazardous areas .....                      | 32        |
| 3.3      | Installation.....                                                               | 33        |
| 3.4      | Connecting up .....                                                             | 36        |
| 3.5      | Commissioning - Downloading the configuration data.....                         | 37        |
| 3.6      | Operating mode of the CPU: Reaction of the CP .....                             | 37        |
| 3.7      | Disassembly.....                                                                | 38        |
| <b>4</b> | <b>Configuration.....</b>                                                       | <b>39</b> |
| 4.1      | Security recommendations.....                                                   | 39        |

|          |                                                                                                          |    |
|----------|----------------------------------------------------------------------------------------------------------|----|
| 4.2      | STEP 7 Professional .....                                                                                | 42 |
| 4.3      | Settings .....                                                                                           | 42 |
| 4.4      | Restricting communications services in the CPU.....                                                      | 44 |
| 4.5      | IP configuration .....                                                                                   | 45 |
| 4.5.1    | Special features on DHCP .....                                                                           | 45 |
| 4.5.2    | Restart after detection of a duplicate IP address in the network.....                                    | 45 |
| 4.5.3    | IP routing.....                                                                                          | 46 |
| 4.5.4    | Programmed connections: Restriction of firewall rules.....                                               | 47 |
| 4.6      | DNS configuration .....                                                                                  | 47 |
| 4.7      | Communication with the CPU .....                                                                         | 47 |
| 4.7.1    | CP diagnostics.....                                                                                      | 47 |
| 4.8      | SNMP .....                                                                                               | 49 |
| 4.9      | Security .....                                                                                           | 50 |
| 4.9.1    | Security user.....                                                                                       | 50 |
| 4.9.2    | Firewall .....                                                                                           | 50 |
| 4.9.2.1  | Firewall sequence when checking incoming and outgoing frames .....                                       | 50 |
| 4.9.2.2  | Notation for the source IP address (advanced firewall mode) .....                                        | 51 |
| 4.9.2.3  | HTTP and HTTPS not possible with IPv6 .....                                                              | 51 |
| 4.9.2.4  | Settings for online security diagnostics and downloading to station with the firewall<br>activated ..... | 51 |
| 4.9.3    | Time-of-day synchronization .....                                                                        | 52 |
| 4.9.4    | Log settings - Filtering of the system events .....                                                      | 53 |
| 4.9.5    | VPN .....                                                                                                | 53 |
| 4.9.5.1  | Creating VPN tunnel communication between S7-1500 stations.....                                          | 54 |
| 4.9.5.2  | Establishment of VPN tunnel communication between the CP and SCALANCE M.....                             | 56 |
| 4.9.5.3  | VPN tunnel communication with SOFTNET Security Client .....                                              | 56 |
| 4.9.5.4  | CP as passive subscriber of VPN connections.....                                                         | 57 |
| 4.9.6    | Online functions .....                                                                                   | 57 |
| 4.9.7    | Certificates .....                                                                                       | 57 |
| 4.9.7.1  | Third-party certificates .....                                                                           | 57 |
| 4.9.7.2  | Certificate manager .....                                                                                | 58 |
| 4.9.7.3  | Handling certificates .....                                                                              | 58 |
| 4.10     | FTP server configuration .....                                                                           | 61 |
| 4.10.1   | Configuring the FTP server function .....                                                                | 61 |
| 4.10.2   | Layout and structure of the FTP configuration list .....                                                 | 63 |
| 4.10.3   | FTPS access.....                                                                                         | 63 |
| 4.11     | CloudConnect.....                                                                                        | 64 |
| 4.11.1   | Configuring the cloud access.....                                                                        | 64 |
| 4.11.1.1 | Overview of configuration .....                                                                          | 64 |
| 4.11.1.2 | Notes on data structuring and configuration .....                                                        | 65 |
| 4.11.1.3 | Configuration rules .....                                                                                | 65 |
| 4.11.1.4 | "CloudConnect" parameter group .....                                                                     | 68 |
| 4.11.1.5 | Onboarding in MindConnect IoT Extension.....                                                             | 72 |
| 4.11.1.6 | Operand areas and tags .....                                                                             | 73 |
| 4.11.2   | Configuring topics, groups and data points .....                                                         | 73 |
| 4.11.2.1 | Configuring topics or groups.....                                                                        | 73 |
| 4.11.2.2 | Configuring the data points .....                                                                        | 75 |
| 4.11.2.3 | Data types .....                                                                                         | 76 |

|          |                                                                     |            |
|----------|---------------------------------------------------------------------|------------|
| 4.11.2.4 | Trigger.....                                                        | 77         |
| 4.11.2.5 | Payload formats.....                                                | 81         |
| 4.11.2.6 | Import / export of payload.....                                     | 85         |
| 4.11.3   | Properties dialog of the topics.....                                | 91         |
| 4.11.3.1 | Opening the properties dialog.....                                  | 91         |
| 4.11.3.2 | Quality of Service (QoS).....                                       | 91         |
| 4.11.4   | Additional information.....                                         | 93         |
| 4.11.4.1 | Connection abort and data buffering.....                            | 93         |
| 4.11.4.2 | JSON escape sequences.....                                          | 94         |
| 4.11.4.3 | Permitted Characters.....                                           | 96         |
| <b>5</b> | <b>Program blocks.....</b>                                          | <b>99</b>  |
| 5.1      | Program blocks for communication.....                               | 99         |
| 5.2      | Changing the IP address during runtime.....                         | 103        |
| 5.3      | Block for the FTP client function.....                              | 104        |
| 5.3.1    | FTP_CMD.....                                                        | 104        |
| 5.3.2    | Input parameter - FTP_CMD.....                                      | 106        |
| 5.3.3    | Job blocks for FTP_CMD.....                                         | 107        |
| 5.3.4    | Output parameters and status information FTP_CMD.....               | 112        |
| 5.3.5    | Structure of the data block (file DB) for FTP client operation..... | 115        |
| <b>6</b> | <b>Diagnostics and maintenance.....</b>                             | <b>119</b> |
| 6.1      | Diagnostics.....                                                    | 119        |
| 6.1.1    | Diagnostics options.....                                            | 119        |
| 6.1.2    | Online security diagnostics via port 8448.....                      | 120        |
| 6.1.3    | Connect online.....                                                 | 121        |
| 6.1.4    | Diagnostics with SNMP.....                                          | 122        |
| 6.2      | Maintenance.....                                                    | 124        |
| 6.2.1    | Update firmware.....                                                | 124        |
| 6.2.2    | Replacing a module without a programming device.....                | 127        |
| <b>7</b> | <b>Technical specifications.....</b>                                | <b>129</b> |
| 7.1      | Technical specifications.....                                       | 129        |
| 7.2      | Pinout of the Ethernet interface.....                               | 130        |
| 7.3      | Permitted cable lengths - Ethernet.....                             | 130        |
| 7.4      | Permitted cable lengths - Gigabit Ethernet.....                     | 130        |
| <b>8</b> | <b>Approvals.....</b>                                               | <b>131</b> |
| <b>9</b> | <b>Dimension drawings.....</b>                                      | <b>137</b> |
| <b>A</b> | <b>Additional information.....</b>                                  | <b>139</b> |
| A.1      | Linking to other systems with FETCH/WRITE.....                      | 139        |
| <b>B</b> | <b>Syslog messages.....</b>                                         | <b>143</b> |
| B.1      | Structure of the Syslog messages.....                               | 143        |
| B.2      | Tags in Syslog messages.....                                        | 145        |
| B.3      | Messages.....                                                       | 146        |
| B.3.1    | Non-repudiation.....                                                | 146        |

|                   |            |
|-------------------|------------|
| <b>Index.....</b> | <b>147</b> |
|-------------------|------------|

# Application and functions

## 1.1 Application

### Application

The CP is intended for operation in an S7-1500 automation system. The CP enables the S7-1500 to be connected to Industrial Ethernet and to a cloud system.

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.

## 1.2 Communication services

### Communications services

The CP supports the following communication services:

- **Open User Communication (OUC)**

Open User Communication supports the following communications services via the CP using programmed or configured communications connections:

- ISO transport (complying with ISO/IEC 8073)
- TCP (IPv4/IPv6) (acc. to RFC 793 and 8200)

With the interface via TCPv4/v6 connections, the CP supports the socket interface to TCP/IP available on practically every end system.

- ISO-on-TCP (acc. to RFC 1006)
- UDP (acc. to RFC 768)
- Multicast over UDP connection

The multicast mode is made possible by selecting a suitable IP address when configuring connections.

- Sending e-mail via SMTP (port 25) or SMTPS (port 587) with authentication on an e-mail server.

For the blocks, see section Program blocks (Page 99).

- **MQTT**

MQTT for connecting the S7-1500 to a cloud system. For information on the communication functions and cloud systems, see section Cloud communication (Page 14).

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

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

  - FTP server
    - Can be activated via the configuration
  - FTP client
    - Configurable via program blocks.
    - For the blocks, see section Program blocks (Page 99).
- **E-mail**

See above (OUC).
- **HTTP/HTTPS**
  - Web server of the CPU: Monitoring devices and process data with HTTP/HTTPS
    - If you do not require the function, you can disable it in the STEP 7 configuration and disable port 80 ("Access to the Web server" parameter group).
- **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.

You will find detailed information on configuring the communication functions in the STEP 7 help system.

## 1.3 Cloud communication

### Protocols for the cloud connection

The CP supports the following protocols for communication with a cloud broker or cloud server:

- **MQTT**

According to OASIS standard version 3.1 / 3.1.1

## Cloud systems and communication functions

The CP supports the connection to cloud systems that support broker functionality with the MQTT protocol.

The configuration of cloud access ("Cloud operator") is adapted to communication with the following cloud systems:

- MindSphere (Siemens)

Service: MindConnect IoT Extension

Function of the CP:

- Publisher

- Other cloud

Profile for another cloud system

Function of the CP:

- Publisher
- Subscriber

For details, see below.

Possible cloud systems are:

- AWS (Amazon)

Service: IoT Core

- Azure (Microsoft)

Service: IoT Hub

- IBM Cloud (IBM)

Service: Watson IoT Platform

## Functions of the CP for cloud communication

The following table summarizes the support of functions with various cloud providers valid at the time of printing of the manual.

Ask your cloud provider which functions it supports.

Meaning of the symbols:

- +: Supported
- -: Not supported

| Function                      | MindSphere<br>(Siemens) | AWS<br>(Amazon) | Azure<br>(Microsoft) | IBM Cloud<br>(IBM) |
|-------------------------------|-------------------------|-----------------|----------------------|--------------------|
| Publisher function of the CP  | +                       | +               | +                    | +                  |
| Subscriber function of the CP | -                       | -               | -                    | +                  |
| QoS = 2                       | +                       |                 |                      |                    |
| MQTT via TLS                  | +                       | +               | +                    | +                  |

## Communication partner of the CP

- Publisher

A publisher publishes data to a cloud broker.

Together with the CP as a subscriber (only when communicating via "Other cloud"), the following devices can act as publishers:

- CP 1545-1

- Third-party device

Third-party devices, the configuration and payload format of the messages of which are compatible with the CP.

- Subscriber

A subscriber logs on to the cloud broker and subscribes to data of the publisher.

Together with the CP as a publisher, the following devices can act as subscribers:

- CP 1545-1

(only for communication via "Other cloud")

- Third-party device

Third-party devices, the configuration and payload format of the messages of which are compatible with the CP.

For details on the compatibility of communications processor and third-party devices, see section Configuration rules (Page 65).

## Secure communication certificate -

If you want to use secured cloud communication, select "MQTT over TLS" option under "Security > CloudConnect > Broker configuration".

In this parameter group you specify the broker certificate to be used, which you have previously imported in the global security settings and assigned to the CP.

If a partner (Publisher / Subscriber) that communicates with the CP via the cloud requires certificates for secure communication, use the certificate of the partner at the CP in the "Client certificate" drop-down list.

For information on the configuration, see "CloudConnect" parameter group (Page 68).

## 1.4 Further functions

### Time-of-day synchronization with 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.

The CP supports NTP (secure) for secure time transmission.

### 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 MIB objects according to the MIB II standard and Automation System MIB.

The CP supports SNMPv3 when security functions are activated.

### IP configuration (IPv4 / IPv6)

- 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, see section Program blocks (Page 99). Does not apply to S7 connections.

### IP routing

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

For details, see section IP routing (Page 46).

### IPv6 addresses - area of use on the CP

An IPv6 address can be used for the following communication services:

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

When using IPv6 addresses, make sure to configure the DNS server accordingly.

### 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. "Access to the Web server" can be activated for the Ethernet interface in the configuration.

Read the documentation for the Web server; see Preface (Page 3), Documentation guide.

---

**Note**

**Web server access via HTTPS**

The Web server of a SIMATIC S7-1500 station is located in the CPU. For this reason, when there is secure HTTPS access to the Web server of the station using the IP address of the CP, 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. The S7 addressing mode applies only to data blocks (DBs).

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

## **1.5 Industrial Ethernet Security**

### **All-round protection - the task of Industrial Ethernet Security**

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

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

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

### **Security functions of the CP for the S7-1500 station**

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

- Firewall
  - IP firewall with stateful packet inspection (Layer 3 and 4)
  - Firewall also for non-IP frames according to IEEE 802.3 (Layer 2)
  - Limitation of the transmission speed
  - Global and user-specific firewall rules

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

- Logging  
To allow monitoring, events can be stored in log files that can be read out using STEP 7 or can be sent automatically to a Syslog server.
- FTPS (explicit mode)  
For encrypted transfer of files.
- NTP (secure)  
For secure time-of-day synchronization
- 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 39).

## 1.6 Configuration limits and performance data

### 1.6.1 Configuration limits of communications modules

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

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

By operating several CMs/CPs, you can increase the configuration limits listed below for the station as a whole. The CPU does, however, have set limits for the entire configuration. The size of the configuration made available by a CP can be increased by using more than one CP within the framework of the system limits.

Note the information in the documentation of the CPU, see Preface (Page 3), Documentation guide.

---

#### **Note**

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

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

---

## 1.6.2 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.

## 1.6.3 Characteristic data CloudConnect

### Number of connections to the cloud

- Number of sessions with the broker  
Max. 1 session

### Amount of process data for the cloud connection

- Tags in the data area of S7 CPUs
  - Max. 500 tags

### Number of topics/groups

- Number of configurable topics or groups
  - Max. 500

### 1.6.4 Characteristics of S7 communication

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

| Characteristic                                                                                      | Explanation / values                                                                                                |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Total number of freely usable S7 connections on Industrial Ethernet                                 | Max. 118                                                                                                            |
| LAN interface - data field length generated by CP per protocol data unit (PDU = protocol data unit) | <ul style="list-style-type: none"><li>For sending: 480 bytes / PDU</li><li>For receiving: 480 bytes / PDU</li></ul> |
| Number of reservable OP connections *                                                               | Max. 4                                                                                                              |
| Number of reservable PG connections *                                                               | Max. 4                                                                                                              |
| Number of HTTP connections for Web                                                                  | Max. 4                                                                                                              |

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

#### Note

##### Maximum values for an S7-1500 station

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

### 1.6.5 Characteristic data for 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 | <p>Number of configured and programmed connections (ISO transport + ISO-on-TCP + TCP + UDP + FETCH/WRITE + email):</p> <ul style="list-style-type: none"><li>Max. 118 in total</li></ul> <p>Of which maximum:</p> <ul style="list-style-type: none"><li>TCP connections: 0...118</li><li>ISO-on-TCP connections: 0...118</li><li>ISO transport connections: 0...118</li><li>UDP connections (specified and free) in total: 0...118</li><li>Connection for e-mail: 0...1</li><li>Connections for FETCH/WRITE: 0...16</li></ul> |

| Characteristic                                                                                                    | Explanation / values                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 byte to 2 KB</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 kB</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 <p>ISO transport, ISOonTCP, TCP: 1452 bytes / TPDU</p> </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, see Preface (Page 3), Documentation guide.

**Restrictions for UDP**

- UDP broadcast / multicast

To avoid overloading the CP due to high broadcast/multicast frame traffic, the receipt of UDP broadcast/multicast on the CP can be limited; refer to section Settings (Page 42).

- UDP frame buffering

Length of the frame buffer: At least 7360 bytes

Following a buffer overflow, newly arriving frames that are not fetched by the user program are discarded.

## **1.6.6 Characteristic data for FTP / FTPS mode**

### **TCP connections for FTP**

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

- FTP client mode

You can use a maximum of 32 FTP sessions.

Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).

- FTP server mode

You can operate a maximum of 16 FTP sessions at the same time.

Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).

### **Program block FTP\_CMD for FTP client mode**

For communication, use the program block FTP\_CMD.

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

## **1.6.7 Characteristics of security - firewall rules**

### **Firewall rules (advanced firewall mode)**

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

The firewall rules are divided up as follows:

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

## 1.7 Requirements for use

### 1.7.1 Usable CPUs

The following CPUs can be used as local CPU of the communications module:

- Compatible CPUs

All CPUs that can be configured in STEP 7 as of firmware version V2.1 from the following series:

- Standard CPUs (CPU 15xx)
- Compact CPUs (CPU 15xxC)

Exceptions

- The following CPUs are not compatible:
  - H-CPU (CPU 1517H-x PN)
  - R-CPU (CPU 151xR-x PN)

---

#### Note

##### **Keep the firmware version of the communications modules up to date**

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

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

Information regarding product news and new firmware versions is available at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/dl>)

---

### 1.7.2 CPs

#### **Compatible communications modules**

The CP 1545-1 can be used in a rack beside a CP 1543-1 or CM 1542-1.

The CP 1545-1 cannot be used as a replacement part for a CP 1543-1.

### 1.7.3 Software requirements

#### **Software for configuration and online functions**

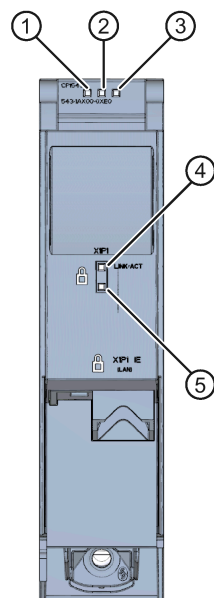
To configure and use the CP's full scope of functions, the following configuration tool is required:

- STEP 7 Professional V17

## LEDs, connectors

### 2.1 LEDs

#### LEDs



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

Figure 2-1 LED display of the CP 1545-1 (without front cover)

#### Meaning of the LED symbols

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

| Green LED | Red LED | Yellow LED | Description         |
|-----------|---------|------------|---------------------|
|           |         |            | LED off             |
|           |         |            | LED on (continuous) |
|           |         |            | LED flashes         |

## Meaning of the LED displays

The CP has the following 3 LEDs to display the current operating status and the diagnostics status: The table shows the meaning of the various combinations of LED states.

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

| RUN<br>(green)                                                                      | ERROR<br>(red)                                                                      | MAINT<br>(yellow)                                                                   | Meaning                                                                                                            |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
|    |    |    | No supply voltage on the CP or supply voltage too low                                                              |
|    |    |    | LED test during startup                                                                                            |
|    |    |    | CP startup                                                                                                         |
|    |    |    | CP is in RUN mode. No disruptions.                                                                                 |
|    |    |    | A diagnostics event has occurred.                                                                                  |
|    |    |    | Maintenance demanded                                                                                               |
|    |    |    | Downloading the user program                                                                                       |
|    |    |    | <ul style="list-style-type: none"> <li>Missing or incomplete CP configuration</li> <li>Loading firmware</li> </ul> |
|  |  |  | Module fault<br>(LEDs flashing synchronized)                                                                       |

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

The LED LINK/ACT (green/yellow) indicates the status and the activity of the port of the Ethernet interface:

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

| LINK/ACT                                                                                              |                                                                                                        | Meaning                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <br>green off      | <br>yellow off      | No connection to Ethernet<br>No Ethernet connection between CP and communication partner<br>No sending / receiving of data via Ethernet |
| <br>flashing green | <br>yellow off      | "LED flash test", see STEP 7 help ("Hardware diagnostics")                                                                              |
| <br>green on       | <br>yellow off      | Connection to Ethernet<br>Existing Ethernet connection between CP and communication partner                                             |
| <br>green on       | <br>flickers yellow | Send / receive data via Ethernet                                                                                                        |

## **2.2 Gigabit interface**

### **Ethernet interface with gigabit specification and security access**

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

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

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

You will find the pin assignment of the sub RJ-45 jack in section Pinout of the Ethernet interface (Page 130).



## Safety notices on the use of the device

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

## 3.1 Important notes on using the device

### 3.1.1 Notes on use in hazardous areas

#### **WARNING**

##### **Cleaning the housing**

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

Do not use any liquids or solvents.

#### **WARNING**

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

#### **WARNING**

##### **Power supply**

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

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

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

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

### 3.1 Important notes on using the device

 **WARNING**

**EXPLOSION HAZARD**

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

#### 3.1.2

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

 **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**

**Requirements for the cabinet**

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

 **WARNING**

**DIN rail**

Only the Siemens DIN rail 6ES5 710-8MA11 may be used for mounting the modules in the application area of ATEX, UKEX, IECEx and CCC-Ex.

 **WARNING**

**Suitable cables at high ambient temperatures in hazardous area**

At an ambient temperature of  $\geq 60^\circ\text{C}$ , use heat-resistant cables designed for an ambient temperature at least  $20^\circ\text{C}$  higher. The cable entries used on the enclosure must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB 3836.1.

 **WARNING**

**Transient overvoltages**

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

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

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

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

|                                                                                                  |
|--------------------------------------------------------------------------------------------------|
|  <b>WARNING</b> |
|--------------------------------------------------------------------------------------------------|

|                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                  |
|--------------------------------------------------------------------------------------------------|
|  <b>WARNING</b> |
|--------------------------------------------------------------------------------------------------|

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

|                                                                                                  |
|--------------------------------------------------------------------------------------------------|
|  <b>WARNING</b> |
|--------------------------------------------------------------------------------------------------|

|                         |
|-------------------------|
| <b>EXPLOSION HAZARD</b> |
|-------------------------|

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

|                                                                                                    |
|----------------------------------------------------------------------------------------------------|
|  <b>WARNING</b> |
|----------------------------------------------------------------------------------------------------|

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

|                                                                                                    |
|----------------------------------------------------------------------------------------------------|
|  <b>WARNING</b> |
|----------------------------------------------------------------------------------------------------|

|                         |
|-------------------------|
| <b>EXPLOSION HAZARD</b> |
|-------------------------|

|                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 Installation, removal and repairs in hazardous areas

### WARNING

#### Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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

### WARNING

#### Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

### WARNING

#### Improper installation of shielded cables

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

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

### WARNING

#### Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

### WARNING

#### Unprotected cable ends

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

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

**! WARNING****Insufficient isolation of intrinsically safe and non-intrinsically safe circuits**

Risk of explosion in hazardous areas

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

**! WARNING****Unauthorized repair of devices in explosion-proof design**

Risk of explosion in hazardous areas

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

## 3.3 Installation

**NOTICE****Improper mounting**

Improper mounting may damage the device or impair its operation.

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

**! WARNING****Open equipment**

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

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

## Installation

### NOTICE

#### Install and remove the device only when the power is off

Turn off the power supply to the station before you install or remove the module. Installing and removing modules with the power supply on can lead to damage to the modules and to loss of data.

### NOTICE

#### Installation location - Dependency of the temperature range

Note the dependency of the permitted temperature range on the installation location:

- Horizontal installation of the rack (DIN rail) means a vertical position of the modules.
- Vertical installation of the rack (DIN rail) means a horizontal position of the modules.

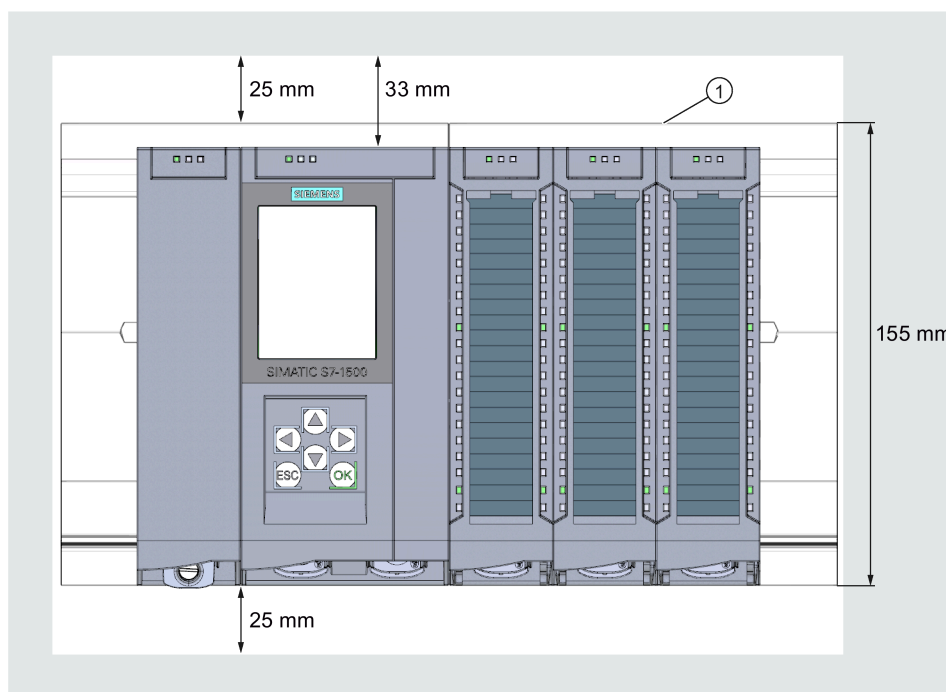
You will find the permitted temperature ranges in the section Technical specifications (Page 129).

#### Minimum clearances

Install the module in such a way that its upper and lower ventilation slits are not covered, allowing adequate ventilation as protection from overheating.

Keep to the following minimum clearances for the circulation of air when the rack is installed horizontally:

- Above the module: At least 33 mm
- Below the module: At least 25 mm



| Installation of the rack            | Installation position of the modules                                                |
|-------------------------------------|-------------------------------------------------------------------------------------|
| Horizontal installation of the rack |   |
| Vertical installation of the rack   |  |

**! WARNING**

**Read the system manual "S7-1500 Automation System"**

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System", see Preface (Page 3), Documentation guide.

## Procedure

When installing and connecting up, keep to the procedures described for installing I/O modules in the system manual "S7-1500 Automation System"; see Preface (Page 3), Documentation guide.

## 3.4 Connecting up

### WARNING

#### Power supply

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

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

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

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

## Terminal

### WARNING

#### Read the system manual "S7-1500 Automation System"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System", see Preface (Page 3), Documentation guide.

#### Power supply off

Make sure that the power supply is turned off when connecting the devices.

## Procedure

1. Connect the CP to the Industrial Ethernet via the RJ-45 socket (bottom side of the CP).  
For the pin assignment of the Ethernet interface, see section Pinout of the Ethernet interface (Page 130).
2. Switch on the power supply of the S7 station.
3. Close the front covers of the modules.

During operation, keep the hinged front panel closed.

## 3.5 Commissioning - Downloading the configuration data

### Requirement: Complete configuration

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

### Download

The remaining steps in commissioning involve downloading the STEP 7 project data.

The CP is supplied with the relevant configuration data by downloading the configuration data to the CPU.

The configuration data can be downloaded to the CPU via a memory card or any Ethernet/PROFINET interface of the S7-1500 station. To load the station via Ethernet, connect the engineering station on which the project data is located to the Ethernet interface of the CPU.

You will find more detailed information on loading in the following sections of the STEP 7 online help:

- "Compiling and loading project data"
- "Using online and diagnostics functions"

### Connection establishment

If you use the CP for cloud communication and all connections of the CP are set up, the CP automatically establishes the connection with the cloud after loading.

## 3.6 Operating mode of the CPU: Reaction of the CP

### Switching the CPU: RUN → STOP

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

---

#### Note

#### RUN/STOP LED of the CP

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

---

### 3.7 Disassembly

In the STOP state of the CPU, the CP remains in the RUN state. The following behavior applies to the CP:

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

## 3.7 Disassembly



### **WARNING**

#### **Improper disassembly**

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

For proper disassembly, observe the following:

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

# Configuration

## 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.
- Check regularly for new features on the Siemens Internet pages.
  - Here you can find information on Industrial Security:  
Link: (<http://www.siemens.com/industrialsecurity>)
  - Here you can find information on security in industrial communication:  
Link: (<https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security.html>)
  - You can find a selection of documentation on the topic of network security here:  
Link: (<https://support.industry.siemens.com/cs/ww/en/view/92651441>)
- Keep the firmware up to date. Check regularly for security updates for the firmware and use them.

Information regarding product news and new firmware versions is available at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/dl>)

### Physical access

Restrict physical access to the device to qualified personnel.

### Network attachment

Do not connect the PC directly to the Internet. If a connection from the CP to the Internet is required, enable the security functions or arrange for suitable protection before the CP, for example a SCALANCE S 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) deactivated.

- 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.
- Deactivate DHCP at interfaces to public networks such as the Internet, for example, to prevent IP spoofing.

**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    |
|-----------------------------|------------------------|---------------------|--------------------------|-------------------|
| DCP                         | 93 (UDP)               | Open                | Open                     | No                |
| S7 and online connections   | 102 (TCP)              | Open                | Open *                   | No                |
| Online security diagnostics | 8448 (TCP)             | Closed              | Open after configuration | No                |
| HTTP                        | 80 (TCP)               | Closed              | Open after configuration | No                |
| HTTPS                       | 443 (TCP)              | Closed              | Open after configuration | Yes               |
| FTP                         | 20 (TCP)<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) |

\* For information on avoiding opening port 102 during diagnostics, see section Online security diagnostics via port 8448 (Page 120).

### Ports of communication partners and routers

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

These can be:

- Broker port
  - MQTT unsecured: 1883 (TCP)
  - MQTT via TLS: 8883 (TCP)

The port number can be set in the configuration.

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP) - Open in CP on block call (outgoing only)
- SMTPS / 587 (TCP) - Open in CP on block call (outgoing only)
- Syslog / 514 (UDP)

## 4.2 STEP 7 Professional

### Configuration in STEP 7

You perform the configuration of the CP in STEP 7 Professional.

You will find the required STEP 7 version in the section Software requirements (Page 24).

## 4.3 Settings

### FETCH/WRITE

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

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

Access is possible from the following devices:

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

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

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

- TCP
- ISO-on-TCP
- ISO transport

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

### Requirements in the CPU configuration

You need to enable the FETCH/WRITE communication service in the CPU configuration, refer to section Restricting communications services in the CPU (Page 44).

### System memory

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

- Data blocks (DB)

Note the following:

- With access to DBs, the highest DB no. is 255.
- Activate the "S7 addressing" parameter in the TSAP table of the CP for access of S5 or S7 partners.

- Bit memory (M)
- Process image input (PII)
- Process image output (PIQ)
- I/O area inputs (PIW, PID, PIB)
- I/O area outputs (PQW, PQD, PQB)
- Counters (C)
- Timers (T)

### Link to non-SIMATIC systems

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

To be able to use this type of access also for PC applications, for example, you need to know the PDU structure of the jobs. Refer to the appendix Linking to other systems with FETCH/WRITE (Page 139).

## UDP frame buffering

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

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

## 4.4 Restricting communications services in the CPU

### Communications services without connections

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

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

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

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

- Option enabled

Access to CPU data from the client side is permitted.

A prerequisite for enabling this option is enabling an access option in the "Access level" parameter group. When the "No access (complete protection)" option is enabled, PUT/GET communication also cannot be enabled.

- Option disabled

Read and write access to CPU data is only possible with communication connections that require configuration or programming both for the local CPU and for the communications partner.

Connections for which the local CPU is only a server (no configuration/programming of communication with the partner) are not possible.

The following communications services of the CP relate to a CPU  $\geq$  V2.

When the option is disabled, the following is not possible:

- PUT/GET access via the CP
- FETCH/WRITE access via the CP

When the option is disabled, the following is possible:

- FTP access via the CP

## 4.5 IP configuration

### 4.5.1 Special features on DHCP

---

#### Note

#### DHCP not together with IPsec

The "VPN (IPsec)" and "DHCP" functions can each be used, but not at the same time.

---

### 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.

---

### DHCP: Aborting ISO transport connections

---

#### Note

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

---

### 4.5.2 Restart after detection of a duplicate IP address in the network

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

### Behavior when the CP starts up

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

### 4.5.3 IP routing

#### IP routing via the backplane bus

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

The function is supported by the following modules:

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

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

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

#### Restrictions

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

#### Configuration

You reach the function in STEP 7 via:

"Ethernet interface > Ethernet addresses > IP routing between communication modules"

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

Please note:

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

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

#### 4.5.4 Programmed connections: Restriction of firewall rules

##### Restrictions with programmed connections and configured security functions

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

---

**Note****Partner IP addresses not in firewall rules**

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

---

## 4.6 DNS configuration

### DNS server

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

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

## 4.7 Communication with the CPU

### 4.7.1 CP diagnostics

#### CP diagnostics

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

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

- Enable advanced CP diagnostics

Enabling the option allows use of the following diagnostic functions.

If the option is enabled, the "Diagnostics trigger tag" must be configured.

- Diagnostics trigger tag

If the user program of the CPU sets the "Diagnostics trigger tag" (BOOL) to 1, the CP updates the values of the configured variables for advanced diagnostics.

After writing the current values to the variables for advanced diagnostics, the CP sets the "Diagnostics trigger tag" to 0, signaling to the CPU that the updated values can be read from the variables.

### General

- CPU load

The variable (Byte) specifies the CPU processor load as a percentage.

- Memory Resources

The variable (Byte) specifies the utilization of the CP work memory (RAM) as a percentage.

### CloudConnect

The following options can only be used with enabled CloudConnect functions of the CP.

- Broker connection status

The tag (Bool) is set to 1 when the connection to the broker is established.

Value = 0 if no connection is established.

- Send buffer usage

The variable (Byte) specifies the allocation of the message buffer as a percentage.

In case of disruptions in the connection between CP and broker, the CP saves the frames in the frame memory.

- CPU sampling error

The tag (UDInt) specifies the number of scan errors since the last reset of the diagnostic trigger tag.

The cases in which not all DB tags for the cloud communication could be read during the configured "scan cycle" are counted, for example, due to a high communication load at the backplane bus.

With a new diagnostics request (Diagnostics trigger tag: 0 → 1), the counter is reset to zero.

## 4.8 SNMP

### SNMP

The CP supports the following SNMP versions:

- **SNMPv1**

Available with security functions disabled.

Note that with this read and write access to the module is possible. In this case, other settings are not possible.

The configuration of the community strings is only possible if the security functions are enabled.

The CP uses the following community strings to authenticate access to its SNMP agent via SNMPv1:

| Access to the SNMP agent in the CP | Community string for authentication in SNMPv1 *) |
|------------------------------------|--------------------------------------------------|
| Read access                        | public                                           |
| Read and write access              | private                                          |

\*) Note the use of lowercase letters!

---

#### Note

##### Security of the access

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

- **SNMPv3**

Available only when security functions are enabled

You can find additional details in the section Diagnostics with SNMP (Page 122).

### Configuration

- **"Enable SNMP"**

If the option is enabled, communication via SNMPv1 is enabled on the CP.

If the option is disabled, queries from SNMP clients are not replied to by the CP either via SNMPv1 or via SNMPv3.

## 4.9 Security

---

### Note

#### **No LLDP frames when security functions are enabled**

When the security functions are enabled, the CP does not send LLDP frames even if the LLDP mode is enabled in STEP 7.

---

You will find an overview of the range and use of the security functions in section Industrial Ethernet Security (Page 18).

For the configuration limits of the security functions refer to the section Characteristics of security - firewall rules (Page 23).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 50).

### 4.9.1 Security user

#### **Creating a security user**

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

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

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

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

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

### 4.9.2 Firewall

#### **4.9.2.1 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.

#### **See also**

Programmed connections: Restriction of firewall rules (Page 47)

#### 4.9.2.2 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, 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.

#### 4.9.2.3 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.

#### 4.9.2.4 Settings for online security 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.

##### Global security functions:

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

##### Local security functions of the CP:

Now select the CP in the S7 station.

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

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

---

**Note**

**Additional services for online security diagnostics and download**

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

---

### 4.9.3 Time-of-day synchronization

---

**Note**

**Recommendation for setting the time**

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

---

---

**Note**

**Ensuring a valid time of day**

If you use security functions, a valid time of day is 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.

---

### Synchronization method

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

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

- NTP
- NTP (secure)

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

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

## 4.9.4 Log settings - Filtering of the system events

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

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

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

## 4.9.5 VPN

---

### Note

#### DHCP not together with IPsec

The "VPN (IPsec)" and "DHCP" functions can each be used, but not at the same time.

---

### 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

#### 4.9.5.1 Creating VPN tunnel communication between S7-1500 stations

### Requirements

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

- Two S7-1500 stations have been configured.
- Participating CP 1543-1 are configured with a firmware version  $\geq$  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.

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

### Creating a security user

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

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

With all further logons, log on as user.

### "Activate security features" option enabled

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

### Creating the VPN group and assigning security modules

---

#### Note

#### Current date and current time of day on the security modules

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

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

### Configuring properties of the VPN group

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

### Result

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

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

#### 4.9.5.2 Establishment of VPN tunnel communication between the CP and SCALANCE M

Setting up VPN tunnel communication between the CP and SCALANCE M is essentially the same as described in Procedure for S7-1500 stations (Page 54).

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

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

#### 4.9.5.3 VPN tunnel communication with SOFTNET Security Client

Setting up VPN tunnel communication between the SOFTNET Security Client and the CP is essentially the same as described in Procedure for S7-1500 stations (Page 54).

### VPN tunnel communication works only if the internal node is disabled

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

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

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

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

Disable the node in the SOFTNET Security Client tunnel overview:

1. Remove the checkmark in the "Enable active learning" check box.  
The lower-level node initially disappears from the tunnel list.
2. In the tunnel list, select the required connection to the CP.

3. With the right mouse button, select "Enable all members" in the shortcut menu.

The lower-level node appears again temporarily in the tunnel list.

4. Select the lower-level node in the tunnel list.
5. With the right mouse button, select "Delete entry" in the shortcut menu.

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

#### 4.9.5.4 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".

#### 4.9.6 Online functions

#### 4.9.7 Certificates

##### 4.9.7.1 Third-party certificates

##### Certificates of cloud providers

For encrypted communication between the S7 station and broker (MQTT over TLS), you need the root CA certificate of the cloud provider and possibly device certificates or private keys.

The requirements are different for the various cloud providers.

Obtain the required files from your cloud provider or download them from its Internet page.

You can find notes on the required files and the relevant Web pages in the application example of the CP. You will find this document on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/ae>)

### 4.9.7.2 Certificate manager

#### Assignment of certificates

If you use communication with authentication for the CP, you need to import certificates of the communications partners into the STEP 7 project and download them to the CP with the configuration data.

1. Import third-party certificates of all communications partners using the certificate manager in the global security settings.
2. Then assign the certificates of all its communications partners to the CP, either:
  - Using the "Trusted certificates and root certification authorities" table in the global security settings
  - Using the "Certificates of the partner devices" table in the local certificate manager of the module (security)

In this table, also include the certificates of communications partners whose certificates were generated in the same STEP 7 project.

For a description of the procedure, refer to the section Handling certificates (Page 58).

### 4.9.7.3 Handling certificates

#### Certificate for authentication

If you have configured secure communication with authentication for the CP, own certificates and certificates of the communications partner will be required for communication to take place.

All nodes of a STEP 7 project with enabled security functions are supplied with certificates. The STEP 7 project is the certification authority.

---

**Note****No certificate with security functions disabled.**

If the security functions of the CP are disabled in the STEP 7 project, no certificate will be generated for the CP.

---

A certificate is created for every application of the CP that requests a certificate. It is shown in STEP 7 in "Global security settings > Certificate manager > Device certificates". As well as additional information, you will find the respective usage of the certificate there (service/application).

You can call up more information about the certificate by selecting the certificate in the table and selecting the shortcut menu "Show".

So that the CP can communicate with non-Siemens partners when the security functions are enabled, the relevant certificates of the partners must be exchanged during communication. To supply the CP with third-party certificates, follow the steps below:

1. Importing third-party certificates from communications partners  
⇒ Global security settings of the project (certificate manager)
2. Assigning certificates, either:
  - Global security settings > Certificate manager > "Trusted certificates and root certification authorities"
  - Local security settings of the CP > Certificate manager > "Certificates of the partner devices"

The steps are described in the following sections.

### Importing third-party certificates from communications partners

Import the certificates of the communications partners of third-party vendors using the certificate manager in the global security settings of the STEP 7 project. Follow the steps outlined below:

1. Save the third-party certificate in the file system of the PC of the connected engineering station.
2. In the STEP 7 project open the global certificate manager:  
Global security settings > Certificate manager
3. Open the "Trusted certificates and root certification authorities" tab.
4. Click in a row of the table can select the shortcut menu "Import".
5. In the dialog that opens, import the certificate from the file system of the engineering station into the STEP 7 project.

### Assigning certificates in the global security settings

Import the partner certificate via: Global security settings > Certificate manager > Trusted certificates > right mouse click. Assign the certificate to the CP (select certificate > right mouse click).

1. Open the "Trusted certificates and root certification authorities" tab.
2. Select the desired certificate.
3. Select "Assign" in the shortcut menu (right mouse button).
4. Select the desired module in the subsequent dialog.

After the assignment, the certificate appears in the "Certificates of the partner devices" table in the local certificate manager of the module.

### Assigning certificates locally

To be able to use an imported certificate for the CP, it needs to be displayed in the "Security" parameter group of the CP.

In this table, also include the certificates of communications partners whose certificates were generated in the same STEP 7 project.

Proceed as follows to import:

1. In the STEP 7 project select the CP.
2. Navigate to the parameter group "Security > Certificate manager".
3. In the table, double-click on the cell with the entry "<Add new>".

The "Certificate manager" table of the Global security settings is displayed.

4. In the table, select the required third-party certificate and to adopt it click the green check mark below the table.

The selected certificate is displayed in the local table of the CP.

### Exporting certificates for applications of third-party vendors (e.g. logging server)

For communication with applications of third-party vendors, the third-party application generally also requires the certificate of the CP.

You export the certificate of the CP for communications partners from third-party vendors in much the same way as when importing (see above). Follow the steps outlined below:

1. In the STEP 7 project open the global certificate manager:  
Global security settings > Certificate manager
2. Open the "Device certificates" tab.
3. In the table select the row with the required certificate and select the shortcut menu "Export".
4. Save the certificate in the file system of the PC of the connected engineering station.

Now you can transfer the exported certificate of the CP to the system of the third-party vendor.

#### Certificate for logging server

If you use a logging server in your system, export the SSL certificate for the authentication of the CP on the server.

### Change certificate: Subject Alternative Name

STEP 7 adopts the properties "DNS name", "IP address", and "URI" of the "Subject Alternative Name" (SAN) parameter from the STEP 7 configuration data.

You can change this parameter of a certificate in the certificate manager of the global security settings. To do this, select a certificate in the table of device certificates and call the shortcut menu "Renew". Properties of the parameter "Alternative name of the certificate owner" changed in STEP 7 are not adopted by the STEP 7 project.

## 4.10 FTP server configuration

### 4.10.1 Configuring the FTP server function

#### CP configuration

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

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

#### Requirements in the CPU configuration and programming

Use the following settings to allow FTP access:

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

#### 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:

- **Data blocks of the CPU**

Name of the directory:

/cpu1 / DBx

"DBx" is the name of the relevant data block e.g. DB10.

- **SIMATIC memory card of the CPU**

The function is supported as of the following firmware versions:

- CPU: V2.0
- CP 1543-1: V2.0
- CP 1545-1: V1.0

Name of the directory:

/mmc\_cpu1

Access to the following folders of the SIMATIC memory card is possible:

- /DATALOGS  
Directory for log files
- /RECIPES  
Directory for recipe files

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

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

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

**Reading/writing via DBs of the CPU**

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

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

For information on the structure of the file DB, refer to section Structure of the data block (file DB) for FTP client operation (Page 115).

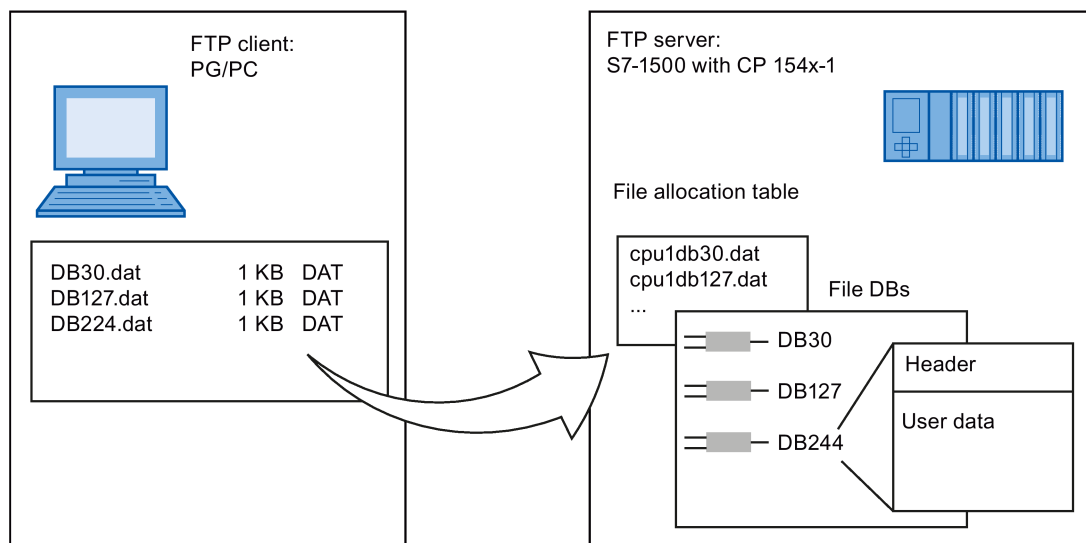


Figure 4-1 S7-CPU with CP 154x-1 as FTP server for the S7 CPU data

## 4.10.2 Layout and structure of the FTP configuration list

### 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 editable. | 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")

## 4.10.3 FTPS access

### 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.

## 4.11 CloudConnect

### 4.11.1 Configuring the cloud access

#### 4.11.1.1 Overview of configuration

##### Configuring cloud access - Overview

1. To allow the cloud application to access the process image, create the required DBs and DB tags in the local CPU.

The data points of the topics/groups (see below) access these DB tags; see section Operand areas and tags (Page 73).

2. Create at least one user with the role "NET Administrator" in the Global Security settings.
3. Enable the option "Activate security features" for the CP under the parameter group "Security".
4. Enable the option "Activate CloudConnect" for cloud communication of the CP.

Select the cloud provider:

- Siemens MindSphere - MindConnect IoT Extension
- Other cloud

For the supported cloud providers, refer to the section Cloud communication (Page 14).

Configure the other parameters; see section "CloudConnect" parameter group (Page 68).

5. If you configure encrypted communication (MQTT over TLS) with the broker, you need at least the relevant certificate and possibly a key of the cloud provider.

Obtain this from your cloud provider, possibly from its Internet pages, and import the files into the STEP 7 project and the CP. For the procedure, refer to the section Certificates (Page 57).

6. Then expand the project tree:

Station > Local modules > CP 1545-1 > Cloud connection

See section Configuring topics or groups (Page 73) for more on this.

Create a group or a topic.

7. Open the group or topic, insert data points and configure them.
8. Open the properties dialog of the topic / group via the "Properties" shortcut menu.
  - Configure the name and optional "Author" and "Comment" of the topic / group.
  - Configure the "Required Quality of Service (QoS)". See section Quality of Service (QoS) (Page 91) for more on this.
  - If required, configure a time trigger for the topic or group.

## 4.11.1.2 Notes on data structuring and configuration

### Data structures

To access the process data for cloud communication, the CP accesses the DB tags of the CPU. The data that is referenced in the DB tag is configured in the CP via data points.

Depending on the cloud provider, the data is structured differently for transfer to the broker:

- Other cloud (AWS / Azure / IBM Cloud)
  - Topics

A topic is the channel for the transfer of values of one or more data points.  
You can create several topics.  
No groups can be configured.
- Siemens MindSphere - MindConnect IoT Extension
  - Groups

A group can contain one or multiple data points.  
You can create one or more groups.
  - Topic

All groups are permanently assigned to the standard topic "s/us" of the MindConnect IoT Extension.

### Topic and group names

Configuration of the topic names:

- For the cloud provider MindConnect IoT Extension, the topic name "s/us" is a fixed name.
- For all other cloud providers, the topic names can be configured.

## 4.11.1.3 Configuration rules

### Configuration rules

Observe the following rules for configuration:

- **Data blocks**
  - Size

The number of variables in the DB is not limited.  
When you create arrays, only elements/tags of arrays with a maximum size of < 10000 elements can be published.

- **Topics / Groups**

- Quantity

- Maximum number per CP: 500

- Name

- Within a cloud application, the name of a topic must be unique.

- This applies to all participating publishers and subscribers.

- Also read the information in the Permitted Characters (Page 96) section.

- Size

- The number of data points that a topic or group may contain is additionally limited by the total amount of the payload, see below.

**Data points**

- Quantity

- Maximum number of data points per CP: 500

- Maximum number of data points per topic / group: 500

- The number of data points that a topic or group may contain is additionally limited by the total amount of the payload, see below.

- Name

- Within a topic, the name of a data point must be unique.

- Also read the information in the Permitted Characters (Page 96) section.

**Payload amount**

- Total amount of payload per topic / group

- Maximum 500000 Byte (corresponds to 500000 ASCII characters)

- Total amount of payload per CP

- Maximum 500000 Byte (corresponds to 500000 ASCII characters)

The amount of payload in the configuration depends on the payload format used. The size of the standard payload format with one data point and a data point name length of 21 ASCII characters is:

- JSON : 258 Byte

- XML : 363 Byte

- MindSphere - MindConnect IoT Extension : 160 Byte

If you use longer names or additional code components (e.g. additional attributes), you need to add these.

Example for the calculation of the payload amount:

With an amount of payload format of 500 ASCII characters for a data point, one data point per topic and 500 configured topics, the total amount of payload would be 250000 bytes.

Note:

Because the variables are replaced by values when the messages are published, the amount of payload on the network can be different to the amount of payload in the configuration.

## Consistency check of the subscriber

---

### Note

#### Consistency check of parameters for Publisher and Subscriber

If the CP as a subscriber receives data from a publisher during runtime, the subscriber checks the following parameters supplied by the publisher in the user data for each value received:

- Topic name
- Data point name
- Data type

The station name of a publisher is not evaluated by the CP as a subscriber.

### Evaluation

Result of the consistency check:

- Parameters identical  
If these three parameters of the publisher are identical with the parameters configured in the subscriber and if the QualityCode of the message is "GOOD", the subscriber writes the received data into the data block of its CPU.
  - Parameters not identical  
If one or more of these three publisher parameters do not match the parameters configured in the subscriber, the subscriber discards the data.
- 

## Recommendations

When transferring data in a hierarchically structured system, it is generally advisable to name the components according to this hierarchical structure.

The later assignment and evaluation of the published data is facilitated if the names refer to the process data of the stations.

Examples:

- Topic/group name  
You want to name a group or a topic "Motor5". The data is assigned to the S7 station "Station1".  
Example of a topic name:  
"Station1\_Motor5"
- Example of a data point:  
"Plant1\_Unit1\_Aggregate1\_DB\_1\_Signal1"

### Data points and DBs

Within a cloud application, individual publishers can publish data for multiple subscribers. Individual subscribers can subscribe to data from multiple publishers.

For better clarity of the data and to reduce the possibility of identical names, the following procedure is recommended for configuration:

- Data blocks

In a CPU, create separate DBs only for the publisher function and only for the subscriber function.

- Data point name / DB number

If you use the number of the data block (DB) that the data point accesses as part of the data point name, it is easier to assign the data point.

- Publisher

- Create a separate DB for every subscriber for the CP as a publisher.
- If a CP subscribes to data from multiple publishers, configure a different DB number for the respective DB intended for this subscriber with the different publishers.

This prevents tags from different publishers from having an identical data point name if the data point names use the DB number as part of the name.

- Subscriber

Create a separate DB for each publisher for the CP as a subscriber.

Comment:

Subscribed data can only be written in DB tags. For further processing, the user program must access the DB tags. This prevents subscribed data from changing the process image directly during receiving.

The described recommendations are not mandatory but increase the clarity when assigning data and reduces the possibility of identical names.

#### 4.11.1.4 "CloudConnect" parameter group

##### Requirement

Activation of the security functions is a requirement for the configurability of cloud communication.

If you disable the security functions later, note that all previously configured cloud data will be lost, except for the data points and topics or groups.

##### General

- **Activate CloudConnect**

Activates communication with a cloud system via the Ethernet interface of the CP.

- **Cloud provider**

Select the desired cloud provider:

- Siemens MindSphere - MindConnect IoT Extension
- Other cloud (profile for other cloud system)

- **Device name**

Validity: MindConnect IoT Extension only

For the meaning, see Onboarding in MindConnect IoT Extension (Page 72).

Do not use quotation marks (") in the name; this results in the messages being sent twice. See also Permitted Characters (Page 96).

- **Scan cycle of variables**

Cycle (ms) in which the DB tags of the CPU are queried.

Range of values: 100..4294967295 ms

---

**Note**

**Volume of transferred data**

The value of the parameter has direct effects on the transferred data volume.

When the trigger condition of a value trigger is met, the data is transferred to the broker with each scan cycle of variables. See also the note in section Trigger (Page 77).

**Data loss**

If you configure a very short scan cycle of variables together with a very large number of data points, it can occur with some brokers that not all of the published data can be read from the input buffer of the cloud server.

Note also the function of the frame memory, see section Connection abort and data buffering (Page 93).

---

- **Topics with time stamp**

When this option is enabled, the current time stamp is added to each value at the time of each publication.

## Broker configuration

- **MQTT / MQTT via TLS**

Alternatively, select one of the following protocol variants:

- MQTT (unencrypted transmission)
- MQTT via TLS (encrypted transmission)

- **Minimum TLS version**

Defines the TLS version used by the CP and the partner.

- **Broker certificate**

The parameter is only active when you have enabled encrypted transmission "MQTT via TLS". In this case, you need a certificate from your cloud provider.

Default setting: "Automatic". With the "Automatic" setting, a certificate from the trusted certificates is assigned.

To manually assign the certificate, follow these steps.

- Import the partner certificate:

Global security settings > Certificate manager > Trusted certificates > right mouse click

- Assign the certificate to the CP:

Select certificate in the "Trusted certificates" list > right mouse click

The certificate appears in the "Certificates of the partner devices" list on the CP in the parameter group "Security > Certificate manager".

- Now select the imported certificate in the "Broker certificate" drop-down list.

- **Broker address**

Address of the broker server (IPv4 address or host name)

- **Broker port**

Port number of the broker server

- Port 1883 is preset for unencrypted transmission (MQTT).
- Port 8883 is preset for encrypted transmission (MQTT via TLS).

- **Client ID**

Enter the client ID that was assigned by your service provider or that you defined.

Max. 255 characters from the ASCII band (hex) 0x20 .. 0x7F

- **Client certificate**

The CP certificate is only used for secure cloud communication (MQTT via TLS).

When a partner (Cloud / Publisher / Subscriber) that communicates with the CP requires certificates for secure communication, use the certificate of the CP. The client certificate is automatically created by STEP 7, used for the CP, and displayed in the output field of the parameter.

**Handling the certificates:**

The corresponding certificates must be exchanged for secure communication:

- Exporting the certificate of the CP or the STEP 7 project

For the CP certificate to be used, the CA certificate of the TIA project must be imported to the cloud server as trusted certificate. To do so, export the CA certificate with the matching hash algorithm from the global security settings:

"Security settings > Security features > Certificate manager > Certificate Authority (CA)" > Certificate selection > Shortcut menu "Export".

Then transfer the certificate to the cloud server.

- Importing the certificate of the communication partner

You must import the respective certificate from the communication partner as a trusted certificate into your STEP 7 project. To do this, follow these steps:

Save the certificate in the file system of the STEP 7 project computer. Import the certificate in the global security settings:

"Security settings > Security features > Certificate manager > Trusted certificates and root certification authorities" > Selection of an empty table row > Shortcut menu "Import".

The procedure depends on the cloud being used.

For some clouds, such as AWS, for example, you must assign this certificate to the CP as device certificate. To do this, follow these steps:

- Assigning the cloud certificate to the CP (depending on the cloud)

Requirement: You have imported the certificate of the cloud in the global security settings as described above.

Select the certificate in the "Trusted certificates and root certification authorities" list, click on the shortcut menu "Assign" and select the CP in the next dialog.

The certificate is now displayed in the local Certificate manager of the CP in the "Certificates of the partner devices" list.

- **Clean session**

When this option is enabled, the session information is deleted when the connection is terminated.

When the option is disabled, the session information is retained when the connection is terminated.

---

**Note**

**Recommendation: Enable "Clean session"**

It is recommended that you enable the parameter.

If QoS is configured with a value > 0 and "Clean session" is disabled, unclear situations can arise in the event of connection aborts with respect to pending acknowledgments.

---

## Broker monitoring

- **Keepalive interval**

Monitoring time of the connection with the broker

If no further data is pending for transmission within the configured monitoring time after the data is sent or if the CP does not receive a packet from the broker, the CP sends a keep-alive packet (PINGREQ) to the broker which it must acknowledge (PINGRESP).

Note the effect of the parameter on the response to connection aborts, see section Connection abort and data buffering (Page 93).

Changes to the value after commissioning are applied after another "Download to device".

**Broker authentication**

- **Enable authentication**

When this option is enabled, the connection to the broker is established with authentication. If possible, use TLS to transmit the user name and password.

When the option is disabled, the connection is established anonymously.

- **User name**

Enter the user name that was assigned by your service provider or that you defined.

- **Password**

Enter the password that was assigned by your service provider or that you defined.

**4.11.1.5 Onboarding in MindConnect IoT Extension****Device parameters**

With a connection to Siemens MindSphere - MindConnect IoT Extension, two parameters are used to identify your device during the Onboarding process once the connection is established between the CP and MindConnect IoT Extension.

- **Device Name**

The CP is registered with the Onboarding process under this name.

The Device name is displayed in MindConnect IoT Extension at the following location:  
Device > Device profile > "NAME"

You assign the name in the parameter group "Security > CloudConnect > General" of the CP.

The default name is composed as follows:

<PLC name>.<CP name>

Impermissible characters are deleted from the components of the name. Note the rules for assigning names, see Permitted Characters (Page 96).

- **Device Type**

The parameter cannot be configured and is permanently set with the following string:

– c8y\_MQTTDevice

The parameter is required in MindConnect IoT Extension to determine the device type.

The Device type is displayed in MindConnect IoT Extension at the following location:  
Device > Device profile > "Type"

You can find additional information on setting up the IoT Extension on the Internet at:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625>)

#### 4.11.1.6 Operand areas and tags

##### Operand area

Tags from the following operand areas of the CPU can be used for the transfer of data of the S7 station:

- Data block (global DB)

Note during the configuration in the properties dialog of the DB:

- Enable the attribute "DB accessible from OPC UA".

##### Configuring the DB tags

Select the following options when configuring the DB tags:

- "Accessible from HMI/OPC UA"
- "Writable from HMI/OPC UA" (required for write access)

You can find the data types that can be used for the cloud connection in the section Data types (Page 76).

#### 4.11.2 Configuring topics, groups and data points

##### 4.11.2.1 Configuring topics or groups

##### Configuration under different cloud operators

By selecting the cloud provider, you determine whether topics or groups are configured for the data transmission.

- MindConnect IoT Extension

You can create several groups.

A group can contain multiple data points.

In IoT Extension, a group corresponds to the structure characteristic "Series". All groups are permanently assigned to the standard topic "s/us".

Select the station in the project tree and expand it:

> Station > Local modules > CP 1545-1 > Cloud connection > Groups

Click "Add group". A Publisher group is created and the Topic editor opens.

- Other cloud

You can create several topics.

A topic can contain multiple data points.

Select the station in the project tree and expand it:

> Station > Local modules > CP 1545-1 > Cloud connection > Published topics / Subscribed topics

Take note of which function (Publisher / Subscriber) is supported together with your cloud provider, see section Cloud communication (Page 14).

Click "Add topic". A topic is created and the Topic editor opens.

For information on the further configuration of the groups or topics, see section Configuring the data points (Page 75).

## Opening the Topic editor

Open the Topic editor as follows:

1. Expand the project tree:

Station > Local modules > CP 1545-1 > Cloud connection > Published topics or groups / "Subscribed topics"

2. You can open the Topic editor in two ways:

- By double-clicking "Add topic" or "Add group"
- By double-clicking on an existing topic or group

## Opening the payload editor

When the Topic editor is open, you can see the following two tabs in the upper right corner:

- Topic editor
- Payload editor

You can switch between the two editors by clicking on the tabs.

In the Payload editor, you define the format of the payload to be published, see section Payload formats (Page 81).

To edit the payload format outside STEP 7, see section Import / export of payload (Page 85).

---

### Note

#### Configuring the payload format for publishers only

Note that the payload format is only configured for data that is published.

---

## 4.11.2.2 Configuring the data points

### Inserting data points in a topic / group

Open a topic / group with a double-click.

In the topic / group, click in the "PLC tag" cell of the first free line of the table.

Select the desired DB tag of a DB of the CPU via the object selection dialog. For the DB tags, see Operand areas and tags (Page 73).

The DB tag is transferred to the table as a data point, the properties and parameters are displayed below.

The table lists all configurable data points.

### Configuring data points

- **Name**  
Configured name of the data point
- **PLC tag**  
Configured name of the DB variable
- **Data type**  
Configured data type of the data point  
For the supported data types, see Data types (Page 76).
- **Attribute**  
⇒ Validity: MindConnect IoT Extension  
The attribute is applied to the user data as <ADDITIONAL\_ATTRIBUTE>; see section Payload formats (Page 81).  
With a connection to IoT Extension, the attribute is interpreted as a label of the physical units of the respective data point. The standard units are:
  - C = Temperature in degrees Celsius
  - P = Pressure in bars
  - mm = Length in millimeters
  - km/h = Speed in km/h
  - m/s<sup>2</sup> = Acceleration in m/s<sup>2</sup>
  - % = Size in percent
  - %RH = Relative humidity in percent
  - A = Current in amperes
  - V = Voltage in volts

- W = Power in watts
- kWh = Energy in kilowatt hours
- VAh = Apparent energy in volt ampere hours
- dBm = Transmit power in decibel-milliwatts (logarithmic ratio)
- lux = Illuminance in lux (lm/m<sup>2</sup>)

Other compound units of the SI system can also be specified, for example:

m/h, m/s, m, km, mW, kW, mWh, mA, VAh

- **Trigger**

For information on the configuration, see Trigger (Page 77).

### 4.11.2.3 Data types

#### Supported data types

The table lists the configurable data types.

If needed, check whether the data types are supported by your broker.

<DATAPOINT\_TYPE> indicates the data type on publication. For the publication of the payload and the tag, <DATAPOINT\_TYPE> see section Payload formats (Page 81).

Table 4- 1 Data types available for Cloud access

| S7 data types (bits)   | <DATAPOINT_TYPE> | Remarks                  |
|------------------------|------------------|--------------------------|
| BOOL (1)               | BOOL             | Values transferred: 0, 1 |
| BYTE (8)               | UINT8            |                          |
| CHAR (8)               | CHAR             | No WCHAR                 |
| USINT (8)              | UINT8            |                          |
| INT (16)               | INT16            |                          |
| UINT (16)              | UINT16           |                          |
| WORD (16)              | UINT16           |                          |
| REAL (32)              | SINGLE_FLOAT     |                          |
| DWORD (32)             | UINT32           |                          |
| DINT (32)              | INT32            |                          |
| UDINT (32)             | UINT32           |                          |
| LREAL (64)             | DOUBLE_FLOAT     |                          |
| STRING (2..256 Char) * | S7_STRING *      | No WSTRING               |
| DATE_AND_TIME (64) *   | S7_DT *          |                          |
| DTL (96) *             | S7_DTL *         |                          |

\* No support for Siemens MindSphere

#### 4.11.2.4 Trigger

##### Time and volume of the transmitted data

###### Requirements for the transmission of data to the cloud

The following conditions must be met to transfer a value:

- The data point is assigned to a topic in the configuration.
- At least one trigger condition is met.

###### Time of transfer

You specify the time when the values of data points are transferred to the broker for each data point with the "Trigger".

When configuring a value trigger and a time trigger, both have equal rights. As soon as one of the two trigger conditions is met, the transfer is triggered.

###### Volume of transferred data

The following data is transferred together to the broker as soon as the value of a data point is pending for transfer:

- Other cloud  
Transfer values of all data points of a topic
- MindConnect IoT Extension  
Transfer values of all data points of a group

###### Duration of transfer (value trigger)

---

###### Note

###### Volume of the transferred data

Note that the settings for all triggers have an effect on the amount of data transferred.

###### Value trigger

The data of a topic or a group are transferred as long as the trigger condition is fulfilled.

###### Value trigger + time trigger

Different value triggers and an additional time trigger each initiate the transfer of the entire topic or group.

---

###### Note

###### Transfer in "Scan cycle of variables"

When the trigger condition of a value trigger is met, the data is transferred to the broker with each scan cycle of variables.

---

You configure the "Scan cycle of variables" on the CP in the parameter group "Security > CloudConnect > ", see section "CloudConnect" parameter group (Page 68).

## Trigger

You use the triggers to specify the conditions that initiate transmission of the saved value to the Cloud or the broker.

The following trigger types are available:

- **Time trigger**

A time trigger is applied to all data points of the topic / user group.

The time trigger is configured in the properties dialog of the topic / group.

The following types of triggers are available:

- Cyclic
- Time (daily / weekly / monthly)

---

### Note

#### Time trigger with migration of the CP V1.0

Projects from predecessor versions that contain the CP with firmware version 1.0 demonstrate the following behavior for the time trigger with migration of the CP to firmware version 1.1:

Time triggers of the data points configured in predecessor versions are transferred to the topic or group with CP V1.1. If multiple time triggers were configured in a topic or group, the first found time trigger is applied.

---

- **Value trigger**

One value trigger can be configured for each tag:

The following types of triggers are available:

- Deviation (transfer on deviation)
- Threshold LOW / Threshold HIGH
- Range inside / Range outside

See below for the meaning.

## Trigger types

### Time trigger

- Cyclic

Cyclic transmission - configurable in milliseconds

The value is transmitted cyclically.

- Once daily

The value is transferred once a day at the configured time.

- Once weekly  
The value is transferred once a week.
- Once monthly  
The value is transferred once a month.  
Note:  
If a month has fewer days than the configured day (e.g. the 31st), no value is transferred at the end of the month.

### Value trigger

For all value triggers, note the value range of the data type of the respective data point. The respective trigger value is configured depending on the value range.

- Deviation  
The value is transferred as soon as it deviates by the configured amount from the last value stored in the CPU.  
The transfer is triggered on occurrence of the following conditions:
  - New value > (last saved value + positive deviation)
  - New value < (last saved value - positive deviation)
  - New value > (last saved value - negative deviation)
  - New value < (last saved value + negative deviation)
- Threshold LOW  
The value is transferred as soon as it drops below the configured value.  
The transfer is triggered on occurrence of the following conditions:
  - New value < configured threshold LOW
- Threshold HIGH  
The value is transferred as soon as it exceeds the configured value.  
The transfer is triggered on occurrence of the following conditions:
  - New value > configured threshold HIGH
- Range within  
The value is transferred as soon as it is inside the configured range.  
The transfer is triggered on occurrence of the following conditions:
  - Low range limit < New value < High range limit
- Range outside  
The value is transferred as soon as it is outside the configured range.  
The transfer is triggered on occurrence of the following conditions:
  - Low range limit > New value
  - High range limit < New value

The value ranges of the value triggers depend on the data type of the data point.

## Data and trigger types

Not every data type supports all the trigger types. The table lists the configurable data types and specifies the supported trigger types for each data type.

Meaning of the symbols:

- +: Supported
- -: Not supported

Table 4- 2 Trigger support of data types

| S7 data type<br>type (bits / bytes) | Supported triggers |                  |
|-------------------------------------|--------------------|------------------|
|                                     | Time trigger       | Value trigger    |
| Bool (1)                            | +                  | x (only value 0) |
| Byte (8)                            | +                  | +                |
| Char (8)                            | +                  | +                |
| USInt (8)                           | +                  | +                |
| Int (16)                            | +                  | +                |
| UInt (16)                           | +                  | +                |
| Word (16)                           | +                  | +                |
| Real (32)                           | +                  | +                |
| DWord (32)                          | +                  | +                |
| DInt (32)                           | +                  | +                |
| UDInt (32)                          | +                  | +                |
| LReal (64)                          | +                  | +                |
| String (2..256 Char)                | +                  | -                |
| Date_And_Time (8)                   | +                  | -                |
| DTL (12)                            | +                  | -                |

## Value ranges of the data types

Threshold values are configured for the trigger types "Deviation", "Threshold LOW", "Threshold HIGH", "Range within" and "Range outside".

The most important data types that are suitable for threshold triggers have the following value ranges:

- Bool: 0 / 1
- Byte: 0...255 / -128...+127
- Char: 0...255
- USInt: 0...255
- Int: -32768...+32767
- UInt: 0...65535
- Word: -32768...+32767 / 0...65535
- DInt: -2147483648...+2147483647

- UInt: 0...4294967295
- DWord: -2147483647...+2147483647 / 0...4294967295
- Real: +1.175495e-38...+3.402823e+38
- LReal: +12.2250738585072014e-308...+1.7976931348623157e+308

### Value ranges of S7 analog input modules

With a positive integer (Int: 0...32767), 270 corresponds to about 1% of the raw value of an S7 analog input module (27648 = 100%).

#### 4.11.2.5 Payload formats

### Compatibility between CPs with firmware version V1.0 and V1.1

If you use the Subscriber function of the CP with firmware version V1.1, you can use the publisher data (JSON) of a CP with firmware version V1.0 for subscribing data.

### User data format

Different cloud systems use different formats when transferring user data. The CP outputs the user data in the following formats, depending on the connected cloud system ("Cloud provider" parameter):

- MindConnect IoT Extension  
Format for MindSphere / IoT Extension (Siemens)
- JSON  
Format for other cloud  
Cloud services that expect JSON format for processing topics.
- XML  
(not used)

The CP uses the UTF-8 character encoding for formatting the user data.

### Payload format "MindConnect IoT Extension"

```
200, "{{Pub_data point_1.NAME}}", "{{GROUP}}", "{{Pub_data  
point_1.VALUE}}", "{{Pub_data point_1.ADDITIONAL_ATTRIBUTE}}",  
"{{PUBLISH_TIMESTAMP}}"
```

**Payload format "JSON"**

```
{
  "Timestamp" : "{{PUBLISH_TIMESTAMP}}",
  "DataItems" : [
    {
      "Variable" : "{{Pub_data point_1.NAME}}",
      "Type" : "{{Pub_data point_1.TYPE}}",
      "Value" : "{{Pub_data point_1.VALUE}}",
      "QualityCode" : "{{Pub_data point_1.QUALITY_CODE}}"
    },
    {
      "Variable" : "{{Pub_data point_2.NAME}}",
      "Type" : "{{Pub_data point_2.TYPE}}",
      "Value" : "{{Pub_data point_2.VALUE}}",
      "QualityCode" : "{{Pub_data point_2.QUALITY_CODE}}"
    }
  ]
}
```

**Code components**

The code for formatting the user data consists of the components listed below.

The following description of the individual code components is structured as follows:

- **Code component**

<Syntax>

Meaning

- Examples (not for all components)

**Code components: Syntax and meaning**

- **200**

200

Function code (MindConnect IoT Extension)

- **Time stamp**

{{PUBLISH\_TIMESTAMP}}

Meaning: Time of the publication

- Example:

Syntax: "{{PUBLISH\_TIMESTAMP}}"

Results in string: "2018-08-20T13:58:16.192313634+00:00"

- **Data point / Variable**

{{Pub\_data point\_n.NAME}}

Name of the data point

- **Group**  
`{{GROUP}}`  
Group name (MindConnect IoT Extension)
- **Value**  
`{{Pub_data point_n.VALUE}}`  
Value of the data point
- **Attribute**  
`{{Pub_data point_n.ADDITIONAL_ATTRIBUTE}}`  
Attribute (MindConnect IoT Extension)
- **Data type**  
`{{Pub_data point_n.TYPE}}`  
Data type of the data point output by the device  
For the output of the data types, see section Operand areas and tags (Page 73).
- **QualityCode**  
`{{Pub_data point_n.QUALITY_CODE}}`  
Quality status of the value  
See below for the meaning.

### Sequences not permitted in the payload content

The following sequences are not permitted in the payload content:

- `{{#`
- `{{^`
- `{{/`
- `{{>`
- `{{&`
- `{{{`

### Example of transferred payload (JSON)

Below you will find an example of the transferred user data of a topic.

The topic contains three variables of an S7 station for the data points "DP1", "DP2" and "DP3".

The value of the "DataItems" key is an array with the objects of the three variables.

```
{  
  "Timestamp": "{{PUBLISH_TIMESTAMP}}",  
  "DataItems": [  
    {
```

```

    "Variable" : "{{DP1.NAME}}",
    "Type" : "{{DP1.TYPE}}",
    "Value" : "{{DP1.VALUE}}",
    "QualityCode" : "{{DP1.QUALITY_CODE}}"
  },
  {
    "Variable" : "{{DP2.NAME}}",
    "Type" : "{{DP2.TYPE}}",
    "Value" : "{{DP2.VALUE}}",
    "QualityCode" : "{{DP2.QUALITY_CODE}}"
  },
  {
    "Variable" : "{{DP3.NAME}}",
    "Type" : "{{DP3.TYPE}}",
    "Value" : "{{DP3.VALUE}}",
    "QualityCode" : "{{DP3.QUALITY_CODE}}"
  }
}

```

## Escape sequences

Escape sequences which adapt the code according to the protocol used can be used to convert certain special characters.

Special characters can occur within the following name components, for example:

- Station name
- Topic name
- Group name

The following escape sequences are supported by the CP:

- JSON PubSub

Standard JSON escape sequences

For the escape sequences used, see JSON escape sequences (Page 94).

- XML

Standard XML escape sequences

- CSV

Standard CSV escape sequences

The publisher converts the respective special characters into escape sequences.

For the subscriber, the escape sequences are converted into the reverse direction.

## QualityCode

### Transmission and QualityCode

The "QualityCode" quality status of a data point is also transferred with the user data. The status indicates the validity of the value.

The status is set by the CP as a publisher and has the following value range:

- GOOD

The value is valid.

- BAD

The value of the variable is not valid or not current. Possible causes:

- CPU in STOP
- Value not current
- Error while reading the variable

The value of the status has the following effect on the transmission:

- Publisher → Cloud

The publication of CP messages as a publisher is independent of the value of the status.

- Cloud → Subscriber

The receipt of messages by the CP as a subscriber is independent of the value of the status.

However, when a message with the status "BAD" is received, the value is not written to the CPU by the CP as subscriber.

### 4.11.2.6 Import / export of payload

#### Editing the payload format outside STEP 7

If you want to define the format of your payload outside STEP 7 or if you want to continue using or editing the format defined in the STEP 7 project, you can import and export the format.

You can import/export the data in XML format.

#### Exporting and importing payload

First check if the correct cloud operator is selected in the "CloudConnect" parameter group of the CP:

- For topics: Other cloud
- For groups: Siemens MindSphere - MindConnect IoT Extension

Proceed as follows to export/import:

1. Expand the project tree:  
Station > Local Modules > CP 1545-1
2. Select the "Cloud connection" entry.
3. In the shortcut menu, click on "Export CloudConnect Data" or "Import CloudConnect data".  
The window for importing or exporting the file in \*.XML format is opened.

**Notes:**

- When you omit an optional element/attribute, it will receive the respective default value.
- If the \*.XML file contains invalid entries, a corresponding error message is displayed.
- Only published topics (and possibly subscribed topics) or subscribed groups may be present.  
Topics and groups may not be imported or exported at the same time.
- For you to import tags into data points, the tags must be available in the CPU of the target device.

If the tag name contained in the XML file is not found during the import, the respective field will remain empty after the import. To still be able to use the data point, you must select a tag for the data point.

**Note**

**No syntax check**

Imported user data files are not checked for syntax errors by STEP 7 or the CP. An incorrect syntax can prevent cloud communication.

If you edit the user data yourself, then pay close attention to the correctness of the syntax.

## XML syntax and permitted values

| Syntax                                 | Element / Attribute                                                                           | Permissible data types / value range                                                           | Meaning / remark                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <PublishedGroups> or <PublishedTopics> |                                                                                               |                                                                                                |                                                                                                      |
| <General Comment>                      | <ul style="list-style-type: none"> <li>• Comment</li> <li>• Author</li> <li>• Name</li> </ul> | <ul style="list-style-type: none"> <li>• String</li> <li>• String</li> <li>• String</li> </ul> | <ul style="list-style-type: none"> <li>• Optional</li> <li>• Optional</li> <li>• Required</li> </ul> |
| <QoS>                                  |                                                                                               | Integer / 0...2                                                                                | Optional                                                                                             |

| Syntax                                                                                                                                                                                                                  | Element / Attribute                                                                                                                          | Permissible data types / value range                                                                                                                                                                                                                                                     | Meaning / remark                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;TimeTrigger&gt;</code><br><code>&lt;Cyclic&gt;</code><br>or<br><code>&lt;TimeTrigger&gt;</code><br><code>&lt;Date&gt;</code>                                                                                  | <ul style="list-style-type: none"> <li>CycleTime</li> <li>Frequency</li> <li>TimeOfTheDay</li> <li>Weekday</li> <li>DayOfTheMonth</li> </ul> | <ul style="list-style-type: none"> <li>Integer / 10...4294967295 ms</li> <li>String / Daily, Weekly, Monthly</li> <li>Integer / 0...1439 minutes (00:00 ... 23:59)</li> <li>String / Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday</li> <li>Integer / 1...31</li> </ul> | <ul style="list-style-type: none"> <li>Required for element <code>TimeTrigger &gt; Cyclic</code></li> <li>Required for element <code>TimeTrigger &gt; Date</code></li> <li>Optional</li> <li>Optional</li> <li>Optional</li> </ul> |
| <code>&lt;DataPoints&gt;</code><br><code>&lt;DataPoint&gt;</code><br><code>&lt;General Name&gt;</code><br><code>&lt;DataPoints&gt;</code><br><code>&lt;DataPoint&gt;</code><br><code>&lt;General&gt; &lt;Tag&gt;</code> | <ul style="list-style-type: none"> <li>Name</li> </ul>                                                                                       | <ul style="list-style-type: none"> <li>String</li> <li>String</li> </ul>                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Required</li> <li>Optional</li> </ul>                                                                                                                                                       |
| <code>&lt;DataPoints&gt;</code><br><code>&lt;DataPoint&gt;</code><br><code>&lt;ValueTrigger&gt;</code>                                                                                                                  | <ul style="list-style-type: none"> <li>Type</li> <li>Value</li> <li>RangeLow</li> <li>RangeHigh</li> </ul>                                   | <ul style="list-style-type: none"> <li>String / Deviation, Lower Threshold, Upper Threshold, Outside Range, Inside Range</li> <li>String</li> <li>String</li> <li>String</li> </ul>                                                                                                      | <ul style="list-style-type: none"> <li>Required for element <code>ValueTrigger</code></li> <li>Optional</li> <li>Optional</li> <li>Optional</li> </ul>                                                                             |
| <code>&lt;Payload&gt;</code>                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>Format</li> <li>Customize</li> </ul>                                                                  | <ul style="list-style-type: none"> <li>String / XML, JSON, MindConnect IoT Extension, Custom</li> <li>Bool / true, false</li> <li><code>&lt;![CDATA[Contents]]&gt;</code></li> </ul> <p>To allow content, see section Payload formats (Page 81).</p>                                     | <ul style="list-style-type: none"> <li>Required</li> <li>Optional</li> <li>Optional</li> </ul>                                                                                                                                     |
| <code>&lt;SubscribedTopics&gt;</code>                                                                                                                                                                                   |                                                                                                                                              |                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                    |
| <code>&lt;General&gt;</code>                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>Comment</li> <li>Author</li> <li>Name</li> </ul>                                                      | <ul style="list-style-type: none"> <li>String</li> <li>String</li> <li>String</li> </ul>                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Optional</li> <li>Optional</li> <li>Required</li> </ul>                                                                                                                                     |
| <code>&lt;QoS&gt;</code>                                                                                                                                                                                                |                                                                                                                                              | Integer / 0...2                                                                                                                                                                                                                                                                          | Optional                                                                                                                                                                                                                           |
| <code>&lt;DataPoints&gt;</code><br><code>&lt;DataPoint&gt;</code><br><code>&lt;General&gt;</code><br><code>&lt;DataPoints&gt;</code><br><code>&lt;DataPoint&gt;</code><br><code>&lt;General&gt; &lt;Tag&gt;</code>      | <ul style="list-style-type: none"> <li>Name</li> </ul>                                                                                       | <ul style="list-style-type: none"> <li>String</li> <li>String</li> </ul>                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Required</li> <li>Optional</li> </ul>                                                                                                                                                       |

## XML structure with example values

```

<?xml version="1.0" encoding="UTF-8"?>
<CloudConnectData>
  <PublishedTopics>
    <PublishedTopic>
      <General Name="Published Topic_1" Author="Ben Utzer"
        Comment="My published topic"/>
    
```

```

    <QoS>1</QoS>
    <TimeTrigger>
      <Date Frequency="Daily" TimeOfDay="720"/>
    </TimeTrigger>
    <DataPoints>
      <DataPoint>
        <General Name="Published_datapoint_1">
          <Tag>"Data_block_1"."Enabled"</Tag>
        </General>
      </DataPoint>
      <DataPoint>
        <General Name="Published_datapoint_2">
          <Tag>"Data_block_1"."LastStatusMsg"</Tag>
        </General>
      </DataPoint>
      <DataPoint>
        <General Name="Published_datapoint_3">
          <Tag>"Data_block_1"."ErrorCount"</Tag>
        </General>
        <ValueTrigger Type="Deviation" Value="1"/>
      </DataPoint>
    </DataPoints>
    <Payload Format="XML" Customize="true">
      <![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<root>
  <!-- Custom plant identification number -->
  <MyCustomXMLTag>0123456789</MyCustomXMLTag>
<DataItems>
  <DataItem>
    <Variable>{{Published_datapoint_1.NAME}}</Variable>
    <Type>{{Published_datapoint_1.TYPE}}</Type>
    <Value>{{Published_datapoint_1.VALUE}}</Value>
  </DataItem>
  <DataItem>
    <Variable>{{Published_datapoint_2.NAME}}</Variable>

```

```

    <Type>{{Published_datapoint_2.TYPE}}</Type>
    <Value>{{Published_datapoint_2.VALUE}}</Value>
  </DataItem>
  <DataItem>
    <Variable>{{Published_datapoint_3.NAME}}</Variable>
    <Type>{{Published_datapoint_3.TYPE}}</Type>
    <Value>{{Published_datapoint_3.VALUE}}</Value>
    <QualityCode>{{Published_datapoint_3.QUALITY_CODE}}</QualityCode>
  </DataItem>
</DataItems>
</root>]]>
  </Payload>
</PublishedTopic>
<PublishedTopic>
  <General Name="Published Topic_2" Author="Ben Utzer"
    Comment="Another published topic"/>
  <QoS>2</QoS>
  <TimeTrigger>
    <Cyclic CycleTime="500"/>
  </TimeTrigger>
  <DataPoints>
    <DataPoint>
      <General Name="Published_datapoint_1">
        <Tag>"Data_block_1"."Actuation_Speed"</Tag>
      </General>
      <ValueTrigger Type="Inside Range" RangeLow="150"
        RangeHigh="300"/>
    </DataPoint>
    <DataPoint>
      <General Name="Published_datapoint_2">
        <Tag>"Data_block_1"."X-Position"</Tag>
      </General>
      <ValueTrigger Type="Outside Range" RangeLow="0"
RangeHigh="200"/>
    </DataPoint>
  </DataPoints>

```

```

        <Payload Format="XML"/>
    </PublishedTopic>
    <PublishedTopic>
        <General Name="Published Topic_3" Author="Ben Utzer"
            Comment="Yet another published topic"/>
        <QoS>0</QoS>
        <TimeTrigger>
            <Date Frequency="Weekly" Weekday="Wednesday"/>
        </TimeTrigger>
        <DataPoints>
            <DataPoint>
                <General Name="Published_datapoint_1">
                    <Tag>"Data_block_2"."ManufacturedItems"</Tag>
                </General>
                <ValueTrigger Type="Lower Threshold" Value="50"/>
            </DataPoint>
            <DataPoint>
                <General Name="Published_datapoint_2">
                    <Tag>"Data_block_1"."RejectedQuality"</Tag>
                </General>
                <ValueTrigger Type="Upper Threshold" Value="3"/>
            </DataPoint>
        </DataPoints>
    </PublishedTopic>
</PublishedTopics>
<SubscribedTopics>
    <SubscribedTopic>
        <General Name="Subscribed Topic_3" Author="Ben Utzer"
            Comment="My subscribed topic"/>
        <QoS>2</QoS>
        <DataPoints>
            <DataPoint>
                <General Name="Subscribed_datapoint_1">
                    <Tag>"Data_block_2"."In_Storage"</Tag>
                </General>
            </DataPoint>

```

```
<DataPoint>
  <General Name="Subscribed_datapoint_2">
    <Tag>"Data_block_2"."Required"</Tag>
  </General>
</DataPoint>
</DataPoints>
</SubscribedTopic>
</SubscribedTopics>
</CloudConnectData>
```

### 4.11.3 Properties dialog of the topics

#### 4.11.3.1 Opening the properties dialog

When you open the CP in the navigation area below the local modules, the properties dialog may be opened in two ways:

- When selecting a topic / group via the shortcut menu (right click)
- When the Topic editor is open, use the "Properties" button above the data point table

The following parameter groups are available:

- General
- Quality of Service (QoS)

For information on the configuration, refer to section Quality of Service (QoS) (Page 91).

- Trigger

A time trigger is applied to all data points of the topic / user group.

For configuration of the Time trigger, see section Trigger (Page 77).

#### 4.11.3.2 Quality of Service (QoS)

##### Properties of a topic - Quality of Service (QoS)

The parameter becomes accessible when you expand the CP in the navigation area under the local modules and open the properties dialog of a topic via the shortcut menu.

- **Required Quality of Service (QoS)**

This is where you define the desired transmission behavior (Quality of Service) of this topic.

The configured value should be fulfilled by the broker if possible. Check which reaction is performed by the broker you use if it does not meet the required QoS level. Some brokers

select the level closest to the required level in this case. Other brokers output an error message.

- QoS 0

Transfer no more than once

The CP sends the topic once to the broker. The CP does not expect an acknowledgment.

If the topic is not received by the broker, it is lost.

- QoS 1

Transfer at least once

The CP sends the topic to the broker until it receives a PUBACK packet as acknowledgment from the broker.

- QoS 2

Transfer exactly once

The CP sends the topic and waits until it receives the two-step acknowledgment from the broker as specified.

This version represents the highest level of quality, but it is also associated with the highest administrative burden for the client as well as the server.

Default setting: 0

## 4.11.4 Additional information

### 4.11.4.1 Connection abort and data buffering

#### Reaction of the CP to connection aborts

The response to connection aborts is as follows:

- **Connection abort between CP and CPU (CPU in STOP)**
  - During the connection abort:

The CP publishes messages with empty strings for the values and the QualityCode "BAD".
  - After the connection has returned:

When the trigger condition is met, the CP publishes messages with current values and the QualityCode "GOOD".
- **Connection abort between CP and cloud - cable pulled on CP**
  - During the connection abort:

The CP does not publish any messages.
  - After the connection has returned:

For information on the behavior, see the following section.
- **Connection abort between CP and cloud - cloud server not reachable**

For information on the behavior, see the following section.

#### Response to connection abort depending on the QoS value

The response of the CP to an aborted connection with the cloud server depends on the configured QoS value.

- **QoS = 0**
  - During the connection abort:

The CP publishes messages with the current values.

After each time a message is sent, the CP starts the "Keepalive interval" to monitor the connection with the broker. If the CP does not receive a packet from the CP within this monitoring time, it sends a PINGREQ packet to the broker.

If the CP does not receive a PINGRESP packet from the broker, it terminates the connection after 1.5 times the keepalive interval. The CP then attempts to establish the connection again.

The CP does not buffer any published messages.
  - After the connection has returned:

The CP publishes messages with the current values.

- QoS = 1 / 2

- During the connection abort:

The CP publishes messages with current values and waits for acknowledgments from the broker for each message. The CP only deletes published messages from its send buffer after acknowledgment from the broker.

Depending on the QoS value that the broker uses, it sends the following acknowledgments:

- QoS = 1: PUBACK
- QoS = 2: PUBREC + PUBREL

If the CP does not receive an acknowledgment from the broker for any of the most recently published messages (max. 16), it does not send any further messages.

If the CP does not receive a packet from the broker within the monitoring time (keepalive interval), it sends a PINGREQ packet to the broker. If the CP does not receive a PINGRESP packet from the broker, it terminates the connection after 1.5 times the keepalive interval. The CP then attempts to establish the connection again.

- After the connection has returned:

After the connection is re-established, the CP waits for the acknowledgments still pending.

After the acknowledgments are received, the CP first publishes the messages from the frame memory and then the newly accumulated messages.

### Data buffering in the frame memory

The CP saves accumulating messages that have not yet been published in its frame memory. This has a capacity of 3500 messages.

The frame memory operates chronologically; in other words, the oldest data is sent first (FIFO principle). When the maximum capacity is exceeded, the oldest messages are overwritten.

#### 4.11.4.2 JSON escape sequences

##### JSON escape sequences

When using the JSON format for the payload, the following characters are converted into escape sequences by the CP as a publisher.

With the CP as a subscriber, the escape sequences are converted in the reverse direction.

| Characters | JSON escape sequence | Note             |
|------------|----------------------|------------------|
| \n         | \\n                  | New line *       |
| \r         | \\r                  | Line break *     |
| \t         | \\t                  | Tab *            |
| \"         | \\"                  | Quotation marks  |
| \\         | \\\\                 | Double backslash |
| \\u0000    | \\u0000              |                  |

| Characters | JSON escape sequence | Note |
|------------|----------------------|------|
| \u0001     | \\u0001              |      |
| \u0002     | \\u0002              |      |
| \u0003     | \\u0003              |      |
| \u0004     | \\u0004              |      |
| \u0005     | \\u0005              |      |
| \u0006     | \\u0006              |      |
| \u0007     | \\u0007              |      |
| \b         | \\u0008              |      |
| \t         | \\u0009              |      |
| \n         | \\u000A              |      |
| \u000b     | \\u000B              |      |
| \f         | \\u000C              |      |
| \r         | \\u000D              |      |
| \\u000e    | \\u000E              |      |
| \u000f     | \\u000f              |      |
| \u0010     | \\u0010              |      |
| \u0011     | \\u0011              |      |
| \u0012     | \\u0012              |      |
| \u0013     | \\u0013              |      |
| \u0014     | \\u0014              |      |
| \u0015     | \\u0015              |      |
| \u0016     | \\u0016              |      |
| \u0017     | \\u0017              |      |
| \u0018     | \\u0018              |      |
| \u0019     | \\u0019              |      |
| \u001a     | \\u001a              |      |
| \u001b     | \\u001b              |      |
| \u001c     | \\u001c              |      |
| \u001d     | \\u001d              |      |
| \u001e     | \\u001e              |      |
| \u001f     | \\u001f              |      |
| \u007F     | \\u007F              |      |

\* Not configurable in STEP 7 as name component

### 4.11.4.3 Permitted Characters

#### Characters not allowed for names

The following characters are not permitted for names:

- 0x22 (")  
Quotation marks are generally not permitted.
- 0x20 (SP)  
Spaces are allowed within most names. Exception: CloudConnect data point  
Leading and trailing spaces are automatically deleted.

#### Permitted characters

See below for ASCII character sets.

| Parameter                                                                          | Characters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Number of characters |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Name of: <ul style="list-style-type: none"> <li>• DB variable *</li> </ul>         | Permitted characters: <ul style="list-style-type: none"> <li>• Standard characters (numbers, letters)</li> <li>• Special characters 0x21 .. 0x7E</li> <li>• Special characters <math>\geq</math> 0x80</li> </ul>                                                                                                                                                                                                                                                                                                                                           |                      |
| CloudConnect * <ul style="list-style-type: none"> <li>• Data point name</li> </ul> | Permitted characters: <ul style="list-style-type: none"> <li>• Standard characters (numbers, letters)</li> <li>• Special characters <math>\geq</math> 0x80</li> <li>• Special characters 0x21 .. 0x60 with exceptions</li> </ul> The following are not permitted: <ul style="list-style-type: none"> <li>• Space</li> <li>• ! / . &lt; &gt; ^ \ # ! &amp; = { }</li> <li>• Tabs</li> </ul> The following strings are also not permitted: <ul style="list-style-type: none"> <li>• PUBLISH_TIMESTAMP</li> <li>• DATAPOINT_ARRAY</li> <li>• GROUP</li> </ul> |                      |

| Parameter                                                   | Characters                                                                                                                                                                                                                                       | Number of characters |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| CloudConnect *<br>• Topic name<br>(does not apply to Group) | Permitted characters:<br>• Standard characters (numbers, letters)<br>• Special characters $\geq$ 0x80<br>• Special characters 0x21 .. 0x7E with exceptions<br>The following are not permitted:<br>• # + /<br>• \$ as first character in the name |                      |
| CloudConnect *<br>• Device name                             | Permitted characters:<br>• Standard characters (numbers, letters)<br>• Special characters $\geq$ 0x80<br>• Special characters 0x60<br>• Special characters 0x21 .. 0x7E with exceptions<br>The following are not permitted:<br>• " ' /           | 1 ... 128            |
| Name of:<br>• NTP server<br>• Host<br>• S7 station, CPU, CP | Permitted characters according to RFC1035 and RFC1123:<br>• Standard characters (numbers, letters)<br>No station names with digits only<br>• 0x2D ( - ) .. 0x2E ( . )                                                                            |                      |
| User names, passwords                                       | Permitted characters:<br>• Standard characters (numbers, letters)<br>• Following special characters:<br>– 0x2D ( - )<br>– 0x2E ( . )<br>– 0x40 ( @ )<br>– 0x5F ( _ )                                                                             |                      |

\* Cloud messages in JSON format: The escape sequences of the JSON standard apply to special characters in station names, topic names and data point names.

## ASCII character sets

The ASCII characters are listed with their hexadecimal code and the corresponding characters.

**Standard characters**

- 0x30 .. 0x39

0 1 2 3 4 5 6 7 8 9

- 0x41 .. 0x5A

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- 0x61 .. 0x7A

a b c d e f g h i j k l m n o p q r s t u v w x y z

**Special characters < 0x80**

- 0x21 .. 0x2F

! " # \$ % & ' ( ) \* + , - . /

- 0x3A .. 0x40

: ; < = > ? @

- 0x5B .. 0x60

[ \ ] ^ \_ `

- 0x7B .. 0x7E

{ | } ~

**Special characters ≥ 0x80 (ISO/IEC 8859-1)**

- 0x80, 0x82 .. 0x89, 0x8A .. 0x8C, 0x8E, 0x91 .. 0x9C, 0x9E .. 0x9F

€ , f „ ... † ‡ ^ % ¢ Š ‹ Œ Ž ‘ ’ “ ” • — ~ ™ š › œ ž Ÿ

- 0xA1 .. 0xAC, 0xAE .. 0xB5, 0xB8 .. 0xBF

ı Œ £ ¤ ¥ ¦ § ¨ © ª « ¬ ® ¯ ° ± ² ³ ´ µ ¶ · ¸ ¹ º » ¼ ½ ¾ ¿

- 0xC0 .. 0xFF

À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

# Program blocks

## 5.1 Program blocks for communication

### Using the program blocks

The program blocks (instructions) listed below can be used for communication between S7 stations.

Communication via program blocks is not configured. The configurable program blocks are available as an interface in your STEP 7 user program.

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

Recommendation: If possible, use the current version of a module.

---

#### 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 Open User Communication (OUC)

You can find the program blocks in STEP 7 in the "Instructions > Communication > Open User Communication" task card.

The following blocks are available:

- **TSEND\_C / TRCV\_C**

Compact blocks for:

- Connection establishment/termination and sending data
- Connection establishment/termination and receiving data

Use alternatively blocks for connection setup / disconnection and separate blocks for sending / receiving data:

- **TCON / TDISCON**

Connection establishment / connection termination

- **TUSEND / TURCV**

Sending and receiving data via UDP

- **TSEND / TRCV**

Sending and receiving data via TCP or ISOonTCP

- **TMAIL\_C**

Sending e-mails

To transfer encrypted e-mails, the precise time of day is required on the CP. Configure the time-of-day synchronization.

For changing configuration data of the CP during runtime:

- **T\_CONFIG**

Program-controlled configuration of the IP parameters

Refer to the information on T\_CONFIG and on the SDTs "IF\_CONF\_..." in the section Changing the IP address during runtime (Page 103).

---

**Note**

**Requirement in the CP configuration**

To be able to change the IP parameters program-controlled, the option "IP address is set directly at the device" must be enabled in the configuration of the IP address of the Ethernet interface of the CP.

---

## Block for the FTP client of the CP

You can find the program blocks in STEP 7 in the "Instructions > Communication > Communication processor > SIMATIC NET CP".

- **FTP\_CMD**

Block for the FTP client function

Setting up FTP connections and transferring files to and from an FTP server

Refer to the description in the section Block for the FTP client function (Page 104).

## Connection descriptions in system data types (SDTs)

The blocks listed above use the CONNECT parameter for the relevant connection description.

TMAIL\_C uses the parameter MAIL\_ADDR\_PARAM.

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

Create the SDT required for every connection description as a data block (global DB).

The SDT type is not created by selecting an entry from the "Data type" drop-down list in the declaration table of the block, but by entering the name manually in the "Data type" box, for example "TCON\_IP\_V4". The corresponding SDT is then created with its parameters.

**Using the SDTs**

- **TCON\_IP\_v4**  
For transferring data via TCP or UDP
- **TCON\_QDN**  
For TCP or UDP communication via the fully qualified domain name (FQDN) (IPv4 / IPv6)
- **TCON\_Configured**  
For transferring data via a configured TCP connection
- **TCON\_IP\_RFC**  
For transferring data via ISO-on-TCP (direct communication between two S7 stations)
- **TCON\_ISOnative**  
For transferring data via ISO transport connections
- **TADDR\_Param**  
For transferring data via UDP
- **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 its name (FQDN)

For secure transfer:

- **TCON\_IP\_V4\_SEC**  
For the secure transfer of data via TCP or UDP
- **TCON\_QDN\_SEC**  
For secure TCP or UDP communication via the fully qualified domain name (FQDN) (IPv4 / IPv6)
- **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.

## 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 communication partner even if identical blocks of data are being sent.

Connection can be terminated after successful data transmission. A connection is also terminated by calling TDISCON.

### Note

#### Connection abort

If an existing connection is aborted by the communication 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.

## Program blocks - overview

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

Table 5- 1 Blocks of the Open User Communication

| Protocol   | Program block (instruction)                                                                                     | System data type                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP        | <ul style="list-style-type: none"> <li>TSEND_C/TRCV_C</li> <li>or</li> <li>TCON/TDISCON + TSEND/TRCV</li> </ul> | <ul style="list-style-type: none"> <li>TCON_IP_v4</li> <li>TCON_Configured</li> <li>TCON_QDN</li> <li>TCON_IP_V4_SEC</li> <li>TCON_QDN_SEC</li> </ul>              |
| ISO-on-TCP |                                                                                                                 | <ul style="list-style-type: none"> <li>TCON_IP_RFC</li> </ul>                                                                                                      |
| ISO        |                                                                                                                 | <ul style="list-style-type: none"> <li>TCON_ISOnative</li> </ul>                                                                                                   |
| UDP        | <ul style="list-style-type: none"> <li>TCON/TDISCON + TUSEND/TURCV</li> </ul>                                   | <ul style="list-style-type: none"> <li>TCON_IP_v4</li> <li>TCON_QDN</li> <li>TADDR_Param</li> <li>TCON_IP_V4_SEC</li> <li>TCON_QDN_SEC</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_V6_SEC</li> <li>TMai_FQDN</li> <li>TMAIL_V4_SEC</li> <li>TMAIL_QDN_SEC</li> </ul> |

Table 5- 2 Block for communication services of the CP

| Protocol | Program block (instruction)                               | System data type                                                                                                                                                        |
|----------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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> |

Table 5- 3 Block for configuration of the Ethernet interface or an NTP/DNS server

| Function                                | Program block (instruction)                                | System data type                                                                                                                                |
|-----------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration of the Ethernet interface | <ul style="list-style-type: none"> <li>T_CONFIG</li> </ul> | <ul style="list-style-type: none"> <li>IF_CONF_V4</li> <li>IF_CONF_V6</li> <li>IF_CONF_NTP</li> <li>IF_CONF_DNS</li> <li>IF_CONF_MAC</li> </ul> |

## 5.2 Changing the IP address during runtime

### Changing address parameters during runtime

You can change the following address parameters of the CP at runtime controlled by the program:

- IP address
- Subnet mask
- Router address

Program-controlled changing of the IP parameters is supported by program blocks. The program blocks access address data stored in a suitable system data type (SDT).

Apart from the address parameters of the CP, with T\_CONFIG the address parameters of DNS servers (IF\_CONF\_DNS) and NTP servers (IF\_CONF\_NTP) can also be changed program controlled.

The following program blocks and system data types can be used:

- **T\_CONFIG**

Together with SDT:

- IF\_CONF\_V4
- IF\_CONF\_V6
- IF\_CONF\_MAC
- IF\_CONF\_DNS
- IF\_CONF\_NTP

The address parameters can only be configured with temporary validity in the CP. In the respective "IF\_CONF\_..." SDT, the "Mode" = 2 parameter must be set.

---

**Note**

**No feedback from the CP**

"T\_CONFIG" does not support feedback from the CP to the CPU. Errors in the block call or in setting the address parameter are not reported. The block outputs "BUSY" or "DONE" regardless of whether the address parameter was set.

---

You will find detailed information on programming the blocks in the STEP 7 information system.

**Requirements in the CP configuration**

To be able to change the IP parameters program controlled, the option "IP address is set directly at the device" must be enabled in the configuration of the IP address of the Ethernet interface of the CP.

## 5.3 Block for the FTP client function

### 5.3.1 FTP\_CMD

#### FTP\_CMD

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

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

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

---

**Note**

**FTPS: Comparing certificates**

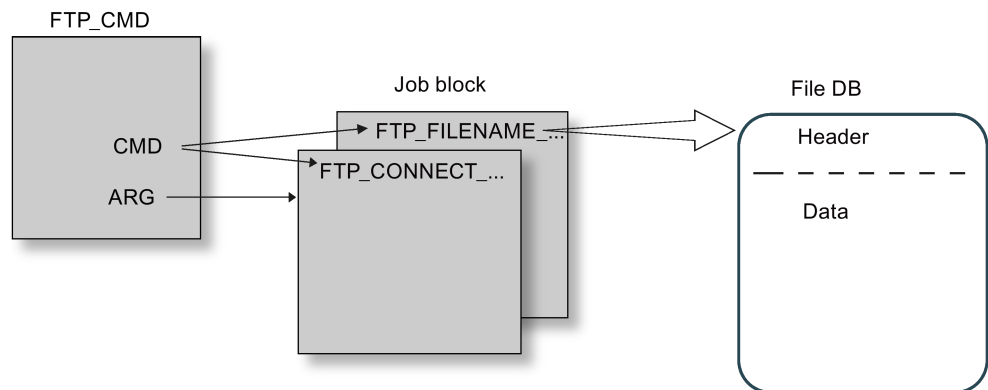
FTPS requires a comparison of the certificates between FTP server and FTP client. If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate needs to be imported from the FTP server. Import the certificate of the FTP server as a trusted certificate in the certificate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

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

### 5.3.2 Input parameter - FTP\_CMD

#### Explanation of the input parameters

You supply the FTP\_CMD instruction with the following input parameters:

Table 5- 4 Formal parameters of the FTP\_CMD instruction - input parameters

| Parameter | Declaration | Data type | Memory area                     | Meaning / remarks                                                                                                                                                                                                                                                                                                                                   |
|-----------|-------------|-----------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| REQ       | Input       | BOOL      | E, A, M, DB, L                  | Starts the send job on a rising edge.                                                                                                                                                                                                                                                                                                               |
| ID *      | INPUT       | INT       | 1, 2 ... 64                     | The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.                                                                                                                                                                                                                                                    |
| CMD *     | INPUT       | BYTE      | See following table "Commands". | FTP command to be executed when the instruction is called. You will find value ranges for the FTP command types after the table.<br>The FTP command specified here must be specified identically in the job block (ARG parameter).<br>If a command is not supported by the CP firmware, an error message with STATUS = 8F6B <sub>H</sub> is output. |
| ARG *     | INPUT       | VARIANT   | See following table "Commands". | Job block<br>References the data area with the execution parameters suitable for the FTP command. Specific data types (UDT) are used depending on the FTP command. The UDTs are shown below.<br>The ANY data type is not permitted for the pointer to be specified here!                                                                            |

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

#### FTP commands in the "CMD" parameter

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

Table 5- 5 Command types

| CMD (command type) | Relevant job blocks / UDT                                | Meaning / handling                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 (NOOP)           | *                                                        | The called FB does not execute any actions. The status codes are set as follows when these parameters are supplied:<br>DONE=1; ERROR=0; STATUS=0                                                                                                                                                    |
| 1 (CONNECT)        | FTP_CONNECT_IPV4<br>FTP_CONNECT_IPV6<br>FTP_CONNECT_NAME | FTP connection establishment<br>With this command, the FTP client establishes an FTP connection to an FTP server (port 21).<br>The connection is available under the connection ID specified here for all further FTP commands. Data is then exchanged with the FTP server specified for this user. |

| CMD (command type) | Relevant job blocks / UDT | Meaning / handling                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 (STORE)          | FTP_FILENAME              | This function call transfers a data block (file DB) from the FTP client (S7-CPU) to the FTP server.<br>Caution: If the file (file DB) already exists on the FTP server, it will be overwritten.                                                                                                                                                                              |
| 3 (RETRIEVE)       | FTP_FILENAME              | This function call transfers a file from the FTP server to the FTP client (S7-CPU).<br>Caution: If the data block (file DB) on the FTP client already contains a file, it will be overwritten.                                                                                                                                                                               |
| 4 (DELETE)         | FTP_FILENAME              | With this function call, you delete a file on the FTP server.                                                                                                                                                                                                                                                                                                                |
| 5 (QUIT)           | *                         | With this function call, you close the FTP connection specified in "ID".                                                                                                                                                                                                                                                                                                     |
| 6 (APPEND)         | FTP_FILENAME              | Similar to "STORE", the "APPEND" command saves a file on the FTP server. With "APPEND", the file on the FTP server is, however, not overwritten. The new content is appended to the existing file.<br>If the file (file DB) does not exist on the FTP server, it will be created.                                                                                            |
| 7 (RETR_PART)      | FTP_FILENAME_PART         | Using the "RETR_PART" command (retrieve part) , you can request a section of a file from the FTP server.<br>If very large files are involved, this allows you to restrict the read to the part you currently require.<br>To do this, you need to know the structure of the file.<br>Enter the required part of the file using the two parameters "OFFSET" and "LEN" in FB40. |

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

### 5.3.3 Job blocks for FTP\_CMD

#### Meaning

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

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

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

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

Table 5- 6 FTP\_CONNECT\_IPV4

| Parameter           | Type       | Range of values        | Meaning / remarks                                                                                                                                                                                                                                                                                |
|---------------------|------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InterfaceID         | HW_ANY     |                        | Module start address<br>When you call an instruction, you transfer the module start address of the CP in the LADDR parameter.<br>You will find the module start address of the CP in the configuration of the CP under:<br>"Properties>Addresses>Inputs"                                         |
| ID                  | CONN_OUC   | 1, 2...64              | The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.                                                                                                                                                                                                 |
| ConnectionType      | BYTE       | 0                      | Connection type "FTP"                                                                                                                                                                                                                                                                            |
| ActiveEstablishment | BOOL       | TRUE                   | TRUE = active connection establishment                                                                                                                                                                                                                                                           |
| FTPCmd              | BYTE       | 1                      | FTP command "CONNECT"<br>FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 106).<br>Note:<br>The FTP command specified here must be specified identically in the CMD input parameter. |
| CertIndex           | BYTE       | 0 = FTP<br>1 = FTPS    | Here, choose between the protocol types FTP or FTPS.<br>Note on FTPS:<br>If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.                                                                                     |
| UserName            | STRING[32] | 'benutzer'             | User name for the login on the FTP server                                                                                                                                                                                                                                                        |
| Password            | STRING[32] | 'passwort'             | Password for the login on the FTP server                                                                                                                                                                                                                                                         |
| FTPserverIPAddr     | IP_V4      | ADDR(1) ...<br>ADDR(4) | IP address of the FTP server as Array[1..4] of Byte, where 1 byte specifies one block of the address.<br>Example: ADDR(1) specifies the first address block (the first byte of the address).                                                                                                     |

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

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

Table 5- 7 FTP\_CONNECT\_IPV6

| Parameter   | Type     | Range of values | Meaning / remarks                                                                                                                                                                                                                                        |
|-------------|----------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InterfaceID | HW_ANY   |                 | Module start address<br>When you call an instruction, you transfer the module start address of the CP in the LADDR parameter.<br>You will find the module start address of the CP in the configuration of the CP under:<br>"Properties>Addresses>Inputs" |
| ID          | CONN_OUC | 1, 2...64       | The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.                                                                                                                                                         |

| Parameter           | Type       | Range of values         | Meaning / remarks                                                                                                                                                                                                                                                                                |
|---------------------|------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ConnectionType      | BYTE       | 0                       | Connection type "FTP"                                                                                                                                                                                                                                                                            |
| ActiveEstablishment | BOOL       | TRUE                    | TRUE = active connection establishment                                                                                                                                                                                                                                                           |
| FTPCmd              | BYTE       | 1                       | FTP command "CONNECT"<br>FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 106).<br>Note:<br>The FTP command specified here must be specified identically in the CMD input parameter. |
| CertIndex           | BYTE       | 0 = FTP<br>1 = FTPS     | Here, choose between the protocol types FTP or FTPS.<br>Note on FTPS:<br>If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.                                                                                     |
| UserName            | STRING[32] | 'user'                  | User name for the login on the FTP server                                                                                                                                                                                                                                                        |
| Password            | STRING[32] | 'password'              | Password for the login on the FTP server                                                                                                                                                                                                                                                         |
| FTPserverIPAddr     | IP_V6      | ADDR(1) ...<br>ADDR(16) | IP address of the FTP server as Array[1..16] of Byte, where 2 bytes specify one block of the address.<br>Example: ADDR(1) + ADDR(2) specify the first address block.                                                                                                                             |

### Job block for FTP connection establishment with server name

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

Table 5- 8 FTP\_CONNECT\_NAME

| Parameter           | Type     | Range of values     | Meaning / remarks                                                                                                                                                                                                                                                                                |
|---------------------|----------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InterfaceID         | HW_ANY   |                     | Module start address<br>When you call an instruction, you transfer the module start address of the CP in the LADDR parameter.<br>You will find the module start address of the CP in the configuration of the CP under:<br>"Properties>Addresses>Inputs"                                         |
| ID                  | CONN_OUC | 1, 2...64           | The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.                                                                                                                                                                                                 |
| ConnectionType      | BYTE     | 0                   | Connection type "FTP"                                                                                                                                                                                                                                                                            |
| ActiveEstablishment | BOOL     | TRUE                | TRUE = active connection establishment                                                                                                                                                                                                                                                           |
| FTPCmd              | BYTE     | 1                   | FTP command "CONNECT"<br>FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 106).<br>Note:<br>The FTP command specified here must be specified identically in the CMD input parameter. |
| CertIndex           | BYTE     | 0 = FTP<br>1 = FTPS | Here, choose between the protocol types FTP or FTPS.<br>Note on FTPS:<br>If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.                                                                                     |

| Parameter     | Type        | Range of values | Meaning / remarks                         |
|---------------|-------------|-----------------|-------------------------------------------|
| UserName      | STRING[32]  | 'benutzer'      | User name for the login on the FTP server |
| Password      | STRING[32]  | 'passwort'      | Password for the login on the FTP server  |
| FTPserverName | STRING[254] |                 | IP address of the FTP server              |

### Job block for write and read access and other FTP commands

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

Table 5- 9 FTP\_FILENAME

| Parameter           | Type                          | Range of values     | Meaning / remarks                                                                                                                                                                                                                                                                                                           |
|---------------------|-------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InterfaceID         | HW_ANY                        |                     | Module start address<br>When you call an instruction, you transfer the module start address of the CP in the LADDR parameter.<br>You will find the module start address of the CP in the configuration of the CP under:<br>"Properties>Addresses>Inputs"                                                                    |
| ID                  | CONN_OUC                      | 1, 2...64           | The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.                                                                                                                                                                                                                            |
| ConnectionType      | BYTE                          | 0                   | Connection type "FTP"                                                                                                                                                                                                                                                                                                       |
| ActiveEstablishment | BOOL                          | TRUE                | TRUE = active connection establishment                                                                                                                                                                                                                                                                                      |
| FTPcmd              | BYTE                          | 2, 3, 4, 6          | FTP command "STORE / RETRIEVE / DELETE / APPEND"<br>FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 106).<br>Note:<br>The FTP command specified here must be specified identically in the CMD input parameter. |
| CertIndex           | BYTE                          | 0 = FTP<br>1 = FTPS | Here, choose between the protocol types FTP or FTPS.<br>Note on FTPS:<br>If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.                                                                                                                |
| DataBlockNumber     | UINT                          |                     | The data block specified here contains the file DB to be read / written.                                                                                                                                                                                                                                                    |
| LenFilename         | UINT                          | 0...1000            | The "LenFilename" parameter for specifying the total length of the file name is not evaluated.<br>Instead, the length information in the string of the "Filename" parameter is evaluated.                                                                                                                                   |
| Filename            | ARRAY[0..3] OF<br>STRING[254] |                     | File name of the destination or source file.<br>The four strings for the file name are concatenated and transferred to the server as a complete string.                                                                                                                                                                     |

## Job block for the RETR\_PART FTP command

The following data structure is used for the RETR\_PART FTP command.

Table 5- 10 FTP\_FILENAME\_PART

| Parameter           | Type     | Range of values     | Meaning / remarks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|----------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InterfaceID         | HW_ANY   |                     | Module start address<br>When you call an instruction, you transfer the module start address of the CP in the LADDR parameter.<br>You will find the module start address of the CP in the configuration of the CP under:<br>"Properties>Addresses>Inputs"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ID                  | CONN_OUC | 1, 2...64           | The FTP jobs are handled on FTP connections. The parameter identifies the connection being used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ConnectionType      | BYTE     | 0                   | Connection type "FTP"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ActiveEstablishment | BOOL     | TRUE                | TRUE = active connection establishment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| FTPcmd              | BYTE     | 7                   | FTP command "RETR_PART"<br>FTP command that executes when the instruction is called. You can find the value ranges for the command types in the section Input parameter - FTP_CMD (Page 106).<br>The FTP command specified here must be specified identically in the CMD input parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CertIndex           | BYTE     | 0 = FTP<br>1 = FTPS | Here, choose between the protocol types FTP or FTPS.<br>Note on FTPS: If the FTP server is configured outside the STEP 7 project of the FTP client, the certificate must be imported from the FTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Offset              | DWORD    |                     | Offset in bytes starting at which the file will be read.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Length              | DWORD    |                     | Sublength in bytes that is read starting at the value specified in "OFFSET".<br>Special features: <ul style="list-style-type: none"> <li>If "DW#16#FFFFFFFF" is specified, the available rest of the file will be read.<br/>Result OK (DONE = 1, STATUS = 0) if no other error occurred.</li> <li>When OFFSET &gt; length of the original file:<br/>Length of the destination file (ACT_LENGTH in file DB): 0 bytes on the CPU.<br/>Result OK (DONE = 1, STATUS = 0) if no other error occurred.</li> <li>When OFFSET + LEN &gt; length of the original file (and LEN ≠ 0xFFFFFFFF):<br/>Length of the destination file (ACT_LENGTH in file DB): Available bytes starting at "OFFSET".<br/>Result OK (DONE = 1, STATUS = 0) if no other error occurred.</li> </ul> |
| DataBlockNumber     | UINT     |                     | The data block specified here contains the file DB to be read / written.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Parameter   | Type                          | Range of values | Meaning / remarks                                                                                                                                                                         |
|-------------|-------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LenFilename | UINT                          | 0...1000        | The "LenFilename" parameter for specifying the total length of the file name is not evaluated.<br>Instead, the length information in the string of the "Filename" parameter is evaluated. |
| Filename    | ARRAY[0..3] OF<br>STRING[254] |                 | File name of the destination or source file.<br>The four strings for the file name are concatenated and transferred to the server as a complete string.                                   |

### Parameter supply for command types NOOP and QUIT

Supply the FTP\_CMD with a reference to a job block with the following command types as well:

CMD = 0 (NOOP)

CMD = 5 (QUIT)

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

#### Note

#### Response if the reference to the FTP job block is missing

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

## 5.3.4 Output parameters and status information FTP\_CMD

### Parameters BUSY, DONE and ERROR

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

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

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

## Evaluating status codes

### Note

#### Evaluation

- Evaluation for BUSY = 0

Do not evaluate the status displays until BUSY = 0.

- Status 8FxxH

For entries coded with status 8FxxH, refer to the information in the STEP 7 Standard and System Functions reference manual. The chapter describing error evaluation with the RET\_VAL output parameter contains detailed information.

Table 5- 11 FTP\_CMD: Meaning of the STATUS parameter in conjunction with DONE and ERROR

| DONE | ERROR | STATUS | Meaning                                                                                                                                                                                                                                                                |
|------|-------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    | 0     | 0000H  | No job is being executed.                                                                                                                                                                                                                                              |
| 1    | 0     | 0000H  | the job was completed without error.                                                                                                                                                                                                                                   |
| 0    | 0     | 7001H  | The job was initiated for the first time.                                                                                                                                                                                                                              |
| 0    | 0     | 7002H  | Job still running.                                                                                                                                                                                                                                                     |
| 0    | 1     | 80C4H  | Communication error (occurs temporarily, it is usually best to repeat the job in the user program).                                                                                                                                                                    |
| 0    | 1     | 8183H  | The configuration does not match the job parameters.                                                                                                                                                                                                                   |
| 0    | 1     | 8401H  | Unknown error<br>Possible causes: <ul style="list-style-type: none"> <li>• A timeout was detected on the connection.</li> <li>• The FTP server has aborted the connection.</li> </ul> Remedy: Send the QUIT and CONNECT commands again to re-establish the connection. |
| 0    | 1     | 8402H  | The connection has an error status.<br>The timeout of the connection may have been exceeded or the FTP server may have terminated the connection.<br>Remedy: Send the QUIT and CONNECT commands to re-establish the connection.                                        |
| 0    | 1     | 8403H  | Login has failed.                                                                                                                                                                                                                                                      |
| 0    | 1     | 8404H  | FTP server is not obtainable.                                                                                                                                                                                                                                          |
| 0    | 1     | 8405H  | Transfer has failed.                                                                                                                                                                                                                                                   |
| 0    | 1     | 8406H  | Timeout for current action                                                                                                                                                                                                                                             |
| 0    | 1     | 8407H  | File was not found on the FTP server.                                                                                                                                                                                                                                  |
| 0    | 1     | 8408H  | Transfer not possible.                                                                                                                                                                                                                                                 |
| 0    | 1     | 8409H  | File could not be fetched.                                                                                                                                                                                                                                             |
| 0    | 1     | 8410H  | Setting the TCP port for the data connection has failed.                                                                                                                                                                                                               |
| 0    | 1     | 8411H  | Offset information does not match.                                                                                                                                                                                                                                     |
| 0    | 1     | 8412H  | Error changing the specified directory                                                                                                                                                                                                                                 |
| 0    | 1     | 8413H  | Error receiving data                                                                                                                                                                                                                                                   |
| 0    | 1     | 8414H  | Error sending data                                                                                                                                                                                                                                                     |
| 0    | 1     | 8415H  | Specified CMD (command type) was rejected by the client.                                                                                                                                                                                                               |
| 0    | 1     | 8416H  | Connection was closed by the FTP server.                                                                                                                                                                                                                               |

### 5.3 Block for the FTP client function

| DONE | ERROR | STATUS | Meaning                                                                                                                                                   |
|------|-------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    | 1     | 8418H  | Error in the user data. Possible causes: <ul style="list-style-type: none"> <li>File name is empty.</li> <li>Data length is "0".</li> <li>etc.</li> </ul> |
| 0    | 1     | 8419H  | There is no socket resource available to open a data connection.                                                                                          |
| 0    | 1     | 8420H  | There is no socket resource available to open a control connection.                                                                                       |
| 0    | 1     | 8421H  | Error opening the file DB to be read                                                                                                                      |
| 0    | 1     | 8422H  | Error opening the file DB to be written                                                                                                                   |
| 0    | 1     | 8423H  | Connection establishment to the FTP server has failed.                                                                                                    |
| 0    | 1     | 8424H  | Internal error                                                                                                                                            |
| 0    | 1     | 8425H  | Format error in the domain name                                                                                                                           |
| 0    | 1     | 8426H  | There are too many DNS queries pending.                                                                                                                   |
| 0    | 1     | 8427H  | The specified DNS server could not assign the specified domain name.                                                                                      |
| 0    | 1     | 8428H  | There is no connection resource available.                                                                                                                |
| 0    | 1     | 8429H  | Unknown channel ID                                                                                                                                        |
| 0    | 1     | 8430H  | The file DB is too short.                                                                                                                                 |
| 0    | 1     | 8431H  | Error when writing to the file DB.                                                                                                                        |
| 0    | 1     | 8432H  | Error when reading from the file DB.                                                                                                                      |
| 0    | 1     | 8433H  | Error when accessing the file DB.                                                                                                                         |
| 0    | 1     | 8434H  | Action was aborted.                                                                                                                                       |
| 0    | 1     | 8435H  | Channel will be reset.                                                                                                                                    |
| 0    | 1     | 8436H  | Unexpected server reply                                                                                                                                   |
| 0    | 1     | 8437H  | Certificate could not be verified.                                                                                                                        |
| 0    | 1     | 8438H  | Unknown error occurred.                                                                                                                                   |
| 0    | 1     | 8439H  | The FTP command causes an error. The cause must be looked for on the FTP server (REST command).                                                           |
| 0    | 1     | 8440H  | The FTP server does not support the requested SSL protocol.                                                                                               |
| 0    | 1     | 8446H  | After the FTP password was sent to the FTP server, an unexpected code was returned by the FTP server.                                                     |
| 0    | 1     | 8451H  | An error was signaled when attempting to change the transmission mode from binary to ASCII.                                                               |
| 0    | 1     | 8455H  | A memory request has failed on the CM/CP.                                                                                                                 |
| 0    | 1     | 8460H  | A problem has occurred handling SSL/TLS.                                                                                                                  |
| 0    | 1     | 8469H  | Interface error<br>The specified output interface could not be used.<br>Remedy:<br>Set the interface to be used for outgoing connections.                 |
| 0    | 1     | 8475H  | The SSL certificate or the SSH md5 fingerprint was not considered trusted.                                                                                |
| 0    | 1     | 8476H  | Nothing was received from the FTP server. In the current status, an incorrect response must be assumed.                                                   |
| 0    | 1     | 8477H  | The specified "Crypto engine" (cryptographic module) was not found.                                                                                       |
| 0    | 1     | 8478H  | The attempt to set the selected SSL "Crypto engine" as the default failed.                                                                                |
| 0    | 1     | 8480H  | A problem has occurred with the certificate of the FTP client.                                                                                            |
| 0    | 1     | 8481H  | The specified number could not be used.                                                                                                                   |
| 0    | 1     | 8482H  | The FTP server uses encoding that is not supported.                                                                                                       |

| DONE | ERROR | STATUS            | Meaning                                                                                                                                                                                                                                                                                                                                  |
|------|-------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    | 1     | 8484 <sub>H</sub> | The maximum file size was exceeded.                                                                                                                                                                                                                                                                                                      |
| 0    | 1     | 8485 <sub>H</sub> | The file DB was modified while being processed to be sent or the file DB is incorrectly structured.                                                                                                                                                                                                                                      |
| 0    | 1     | 8489 <sub>H</sub> | Data could not be sent. There is not enough memory available for the action on the FTP server.                                                                                                                                                                                                                                           |
| 0    | 1     | 8492 <sub>H</sub> | The file already exists. The file will not be overwritten.                                                                                                                                                                                                                                                                               |
| 0    | 1     | 8496 <sub>H</sub> | A problem occurred reading the SSL CA certificate.                                                                                                                                                                                                                                                                                       |
| 0    | 1     | 8497 <sub>H</sub> | An unexpected error occurred in the SSH session.                                                                                                                                                                                                                                                                                         |
| 0    | 1     | 8498 <sub>H</sub> | It was not possible to terminate the SSL connection.                                                                                                                                                                                                                                                                                     |
| 0    | 1     | 8499 <sub>H</sub> | The socket is not ready for sending/receiving. Wait until it is ready and try again.                                                                                                                                                                                                                                                     |
| 0    | 1     | 8501 <sub>H</sub> | The SSL certificate check of the FTP server failed.                                                                                                                                                                                                                                                                                      |
| 0    | 1     | 8507 <sub>H</sub> | A timeout has occurred establishing the connection during the active FTP session while waiting for the FTP server.                                                                                                                                                                                                                       |
| 0    | 1     | 8F54 <sub>H</sub> | The "EXIST" bit in the file DB header is not set.                                                                                                                                                                                                                                                                                        |
| 0    | 1     | 8F55 <sub>H</sub> | Header status bit: Locked                                                                                                                                                                                                                                                                                                                |
| 0    | 1     | 8F56 <sub>H</sub> | The NEW bit in the file DB header was not reset                                                                                                                                                                                                                                                                                          |
| 0    | 1     | 8F6B <sub>H</sub> | Possible causes: <ul style="list-style-type: none"> <li>• Bad value for the CMD parameter<br/>Values from 0 to 15 are permitted.</li> <li>• An FB40 command is not supported.</li> </ul> Possible cause: Incorrect firmware of the CP<br><br>Remedy: Firmware update (with older CPs, use the functions FC 40...FC 44 instead of FB 40.) |
| 0    | 1     | 8F7F <sub>H</sub> | Internal error, for example, illegal ANY reference.                                                                                                                                                                                                                                                                                      |

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

#### How it works

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

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

#### Data consistency

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

## Creating a file DB

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

The size of the field must match the specification of "MAX\_LENGTH" in the header.

## File DB header for FTP client mode

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

| Parameter | Type | Value / meaning                                                                                                                                                                                                                                                                                                                                 | Supply                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXIST     | BOOL | <p>The EXIST bit indicates whether the user data area contains valid data.</p> <p>The retrieve FTP command executes the job only when EXIST=1.</p> <ul style="list-style-type: none"> <li>• 0: The file DB does not contain valid user data (file does not exist).</li> <li>• 1: The file DB contains valid user data (file exists).</li> </ul> | <p>The DELETE FTP command sets EXIST=0.</p> <p>The STORE FTP command sets EXIST=1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LOCKED    | BOOL | <p>The LOCKED bit is used to restrict access to the file DB.</p> <ul style="list-style-type: none"> <li>• 0: The file DB can be accessed.</li> <li>• 1: The file DB is locked.</li> </ul>                                                                                                                                                       | <p>The "STORE" and "RETRIEVE" FTP commands set LOCKED=1 when they are executed if the bit was previously at 0.</p> <p>The user program on the S7 CPU can also set or reset LOCKED during write access to achieve data consistency.</p> <p>This results in mutual locking between the user program and FTP handling to ensure consistency.</p> <p>Recommended sequence in the user program:</p> <ol style="list-style-type: none"> <li>1. Check LOCKED bit (if = 0)</li> <li>2. Set WRITEACCESS bit = 0</li> <li>3. Check LOCKED bit (if = 0)</li> <li>4. Set LOCKED bit = 1</li> <li>5. Write data</li> <li>6. Set LOCKED bit = 0</li> </ol> |

| Parameter      | Type          | Value / meaning                                                                                                                                                                                                                                                                                                                                                                 | Supply                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NEW            | BOOL          | <p>The NEW bit indicates whether data has been modified since the last read access.</p> <ul style="list-style-type: none"> <li>0: The content of the file DB is unchanged since the last write access. The user program of the S7 CPU has registered the last modification.</li> <li>1: The user program of the S7 CPU has not yet registered the last write access.</li> </ul> | <p>After execution, the "RETRIEVE" FTP command sets NEW=1.</p> <p>After reading the data, the user program in the S7 CPU must set NEW=0 to allow a new "RETRIEVE" command.</p>                                                                                                                                                                                          |
| WRITEACCESS    | BOOL          | <ul style="list-style-type: none"> <li>0: The user program has write access rights for the file DBs on the S7 CPU.</li> <li>1: The user program has no write access rights for the file DBs on the S7 CPU.</li> </ul>                                                                                                                                                           | <p>During the configuration of the DB, the bit is set to an initialization value.</p> <p>Recommendation:</p> <p>Whenever possible, the bit should remain unchanged! In special situations, adaptation during operation is possible.</p>                                                                                                                                 |
| ACT_LENGTH     | DINT          | <p>Current length of the user data area.</p> <p>The content of this field is only valid when EXIST = 1.</p>                                                                                                                                                                                                                                                                     | <p>The current length is updated following write access.</p>                                                                                                                                                                                                                                                                                                            |
| MAX_LENGTH     | DINT          | <p>Maximum length of the user data area (length of the entire DB less 20 bytes header).</p>                                                                                                                                                                                                                                                                                     | <p>The maximum length should be specified during configuration of the DB.</p> <p>The value can also be modified by the user program during operation.</p>                                                                                                                                                                                                               |
| FTP_REPLY_CODE | INT           | <p>Unsigned integer (16-bit) containing the last reply code from FTP as a binary value.</p> <p>The content of this field is only valid when EXIST = 1.</p>                                                                                                                                                                                                                      | <p>Updated by the FTP protocol handler with the FTP command processing of the server.</p>                                                                                                                                                                                                                                                                               |
| DATE_TIME      | DATE_AND_TIME | <p>Date and time of the last modification to the file.</p> <p>The content of this field is only valid when EXIST = 1.</p>                                                                                                                                                                                                                                                       | <p>The current date is updated following a write access.</p> <p>If the function for forwarding the time of day is used, the entry corresponds to the time that was passed on.</p> <p>If the function for forwarding the time of day is not used, a relative time is entered. The reference is the startup time of the CP (initialization value: 01.01.1994 00:00h).</p> |



# Diagnostics and maintenance

## 6.1 Diagnostics

### 6.1.1 Diagnostics options

You have the following diagnostics options available for the module:

#### LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 25).

#### CP diagnostics during runtime

Via the configuration, you can enable writing of diagnostics information into variables of the CPU; refer to section CP diagnostics (Page 47).

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

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

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

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

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

#### Diagnostics

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

- General  
General information on the module
- Diagnostics status  
Information on the diagnostics status
- Ethernet interface  
Address and statistical information

## 6.1 Diagnostics

- Time  
Specification of the current time in the module and the time source
- Security  
Status information and log entries

### Functions

You can run the following functions here:

- Firmware update  
For a description, see section Update firmware (Page 124).
- Assign IP address
- Assign PROFINET device name
- Save service data

## STEP 7: Online connection

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

For the procedure, refer to the section Connect online (Page 121).

## Web server

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

For access to the content, see Preface (Page 3), Documentation guide.

## SNMP

You will find detailed information about the supported functions in the section Diagnostics with SNMP (Page 122).

## 6.1.2 Online security diagnostics via port 8448

### Security diagnostics via port 8448

Requirements:

- With an activated firewall, access must be enabled.

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

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

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

For more information, refer to section Settings for online security diagnostics and downloading to station with the firewall activated (Page 51).

### 6.1.3 Connect online

#### Online functions

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

#### Establishing an online connection via Ethernet

##### Procedure:

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

You can use the  icon to the right of the drop-down list to check the settings of the interface.

7. In the "Connect with interface/subnet" drop-down list, select the interface of the station
8. Click "Start search".

If a connection is possible, the station is displayed.

9. Select the station in the table of target devices.

The path is possible both via the CP or the CPU.

10. Click "Connect".

##### Terminate online connection

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

#### See also

Online functions (Page 57)

## 6.1.4 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:

- Address 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 6- 1 Access rights in the SNMP agent

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

\*) Note the use of lowercase letters!

**Note****Security of the access**

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

## 6.2 Maintenance

**! CAUTION****Hot surfaces**

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

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

**! WARNING****Cleaning the housing**

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

Do not use any liquids or solvents.

**! WARNING****Unauthorized repair of devices in explosion-proof design**

Risk of explosion in hazardous areas

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

### 6.2.1 Update firmware

**New firmware versions of the CP**

If a new firmware version is available for the CP, you will find this on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/dl>)

Firmware files have the file format \*.upd.

Save the firmware file on your PC.

There are different ways of loading a new firmware file on the CP:

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

---

**Note****SD card only for firmware file**

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

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

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

---

---

**Note****Duration of the firmware update**

Downloading a new firmware file can take several minutes.

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

---

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

**Requirements:**

- The CPU of the station is accessible via Ethernet.
- The engineering station and the CPU are located in the same subnet.
- The new firmware file is stored on your engineering station.
- The engineering station is connected to the network.
- The relevant STEP 7 project is open on the engineering station.

**Procedure:**

1. Select the station that you want to update with a new firmware.
2. Enable the online functions using the "Connect online" icon.
3. In the "Connect online" dialog, select the Ethernet interface in the "Type of PG/PC interface" list box.
4. Select the CPU of the station.

5. Click on "Start search" to search for the module in the network and to specify the connection path.

When the module is found it is displayed in the table.

6. Connect using the "Connect" button.

The "Connect online" wizard guides you through the remaining steps in installation.

7. Select the CPU in the network view and select the "Online & Diagnostics" shortcut menu (right-click).

8. In the navigation panel of the Online & Diagnostics view, select the entry "Functions > Firmware update".

9. Using the "Browse" button (parameter group "Firmware loader") search for the new firmware file in the file system of the engineering station.

10. Start to download the firmware with the "Start update" button when the correct version of the signed firmware is displayed in the "Status" output box.

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

## Loading the firmware via the SD card

You can find detailed information on using an SD card in the S7-1500 System Manual, see Preface (Page 3), Documentation guide.

### Requirements:

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

### Procedure:

1. Set the operating mode switch of the CPU to STOP.

Ensure that no write functions (e.g. online or test functions) are active in the STOP state.

2. Remove the SIMATIC Memory Card with the configuration data from the slot of the CPU.
3. Insert the SD card with the firmware file in the card slot of the CPU.

The firmware update starts shortly after the card has been inserted. The display shows the following: "STOP - FW UPDATE"

If errors occur, appropriate messages are displayed.

After completing the firmware update, the display shows a result page.

A successful firmware update can be recognized by the following LED pattern from the CPU:

- RUN lights up yellow.
- MAINT flashing yellow.

4. Remove the SD card and insert the SIMATIC Memory Card again.
5. Set the operating mode switch of the CPU to RUN.

The CP uses the new firmware during startup.

For the LED pattern of the CP during the startup, see section LEDs (Page 25).

## 6.2.2 Replacing a module without a programming device

### Configuration data when swapping modules

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

---

#### Note

##### Configured MAC address is adopted

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

---

### Swapping modules for address reference via DHCP (IPv4)

One option in the IP configuration of the CP is to obtain the IP address from a DHCP server.

---

#### Note

##### Recommendation: Configuring a client ID

When replacing modules, remember that the factoryset MAC address of the new module is different from the previous module.

When the factory default MAC address of the new module is sent to the DHCP server, the DHCP server returns a different or no IP address.

Ideally, you should therefore configure IP as follows:

- Always configure a client ID and configure your DHCP server accordingly. This ensures that the CP always receives the same IP address from the DHCP server after swapping a module.

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

---



# Technical specifications

## 7.1 Technical specifications

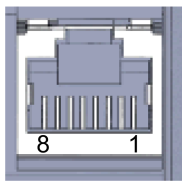
| Technical specifications - CP 1545-1               |                                                                                                                                                                                                                                                                                                                                                                              |                                                                |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Article number                                     | 6GK7545-1GX00-0XE0                                                                                                                                                                                                                                                                                                                                                           |                                                                |
| Attachment to Industrial Ethernet                  |                                                                                                                                                                                                                                                                                                                                                                              |                                                                |
| Quantity                                           | 1 x gigabit interface (X1 P1)                                                                                                                                                                                                                                                                                                                                                |                                                                |
| Design                                             | RJ-45 jack, galvanically isolated                                                                                                                                                                                                                                                                                                                                            |                                                                |
| Properties                                         | <ul style="list-style-type: none"><li>• Standard<ul style="list-style-type: none"><li>• 1000BASE-T, IEEE 802.3ab</li></ul></li><li>• Transmission speeds<ul style="list-style-type: none"><li>• 10 / 100 / 1000 Mbps</li></ul></li><li>• Other properties<ul style="list-style-type: none"><li>• Half duplex/full duplex, autocrossover, autonegotiation</li></ul></li></ul> |                                                                |
| Power supply                                       |                                                                                                                                                                                                                                                                                                                                                                              |                                                                |
| Design                                             | Via S7-1500 backplane bus (15 V)                                                                                                                                                                                                                                                                                                                                             |                                                                |
| Further electrical data                            |                                                                                                                                                                                                                                                                                                                                                                              |                                                                |
| Current consumption (typical)                      | 300 mA from S7-1500 backplane bus                                                                                                                                                                                                                                                                                                                                            |                                                                |
| Effective power loss (typical)                     | 4.5 W                                                                                                                                                                                                                                                                                                                                                                        |                                                                |
| Insulation                                         | Tested to:                                                                                                                                                                                                                                                                                                                                                                   | DC 780 V (type test)                                           |
| Overvoltage category according to IEC / EN 60664-1 | Category II                                                                                                                                                                                                                                                                                                                                                                  |                                                                |
| Permitted ambient conditions                       |                                                                                                                                                                                                                                                                                                                                                                              |                                                                |
| Ambient temperature                                | During operation with the rack installed horizontally                                                                                                                                                                                                                                                                                                                        | 0 °C ... +60 °C                                                |
|                                                    | During operation with the rack installed vertically                                                                                                                                                                                                                                                                                                                          | 0 °C ... +40 °C                                                |
|                                                    | During storage                                                                                                                                                                                                                                                                                                                                                               | -40 °C ... +70 °C                                              |
|                                                    | During transportation                                                                                                                                                                                                                                                                                                                                                        | -40 °C ... +70 °C                                              |
| Relative humidity                                  | During operation                                                                                                                                                                                                                                                                                                                                                             | ≤ 95 % at 25 °C, no condensation                               |
| Permitted contaminant concentration                | Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3                                                                                                                                                                                                                                                                                                         |                                                                |
|                                                    | <ul style="list-style-type: none"><li>• SO<sub>2</sub></li></ul>                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"><li>• &lt; 0,5 ppm</li></ul> |
|                                                    | <ul style="list-style-type: none"><li>• H<sub>2</sub>S</li></ul>                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"><li>• &lt; 0,1 ppm</li></ul> |
| Design, dimensions and weight                      |                                                                                                                                                                                                                                                                                                                                                                              |                                                                |
| Module format                                      | Compact module S7-1500, single width                                                                                                                                                                                                                                                                                                                                         |                                                                |
| Degree of protection                               | IP20                                                                                                                                                                                                                                                                                                                                                                         |                                                                |
| Weight                                             | 320 g                                                                                                                                                                                                                                                                                                                                                                        |                                                                |
| Dimensions (W x H x D)                             | 35 x 147 x 129 mm                                                                                                                                                                                                                                                                                                                                                            |                                                                |
| Mounting type                                      | S7-1500 standard rail mounting                                                                                                                                                                                                                                                                                                                                               |                                                                |

You can find additional data in the section Application and functions (Page 13) as well as in the S7-1500 System Manual, see Preface (Page 3), Documentation guide.

## 7.2 Pinout of the Ethernet interface

### Pinout of the gigabit Ethernet interfaces

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

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

## 7.3 Permitted cable lengths - Ethernet

| Permitted cable lengths - Ethernet | Alternative combinations per length range                                                                                                                                                                                                                        |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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> |
| 0 ... 100 m                        | <ul style="list-style-type: none"> <li>Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180</li> <li>Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet</li> </ul>                                                                    |

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

## 7.4 Permitted cable lengths - Gigabit Ethernet

| Permitted cable lengths - Gigabit Ethernet | Alternative combinations                                                                                                                                         |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 ... 60 m                                 | <ul style="list-style-type: none"> <li>Max. 60 m IE FC TP Flexible Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE</li> </ul> |
| 0 ... 100 m                                | <ul style="list-style-type: none"> <li>Max. 90 m IE FC TP Standard Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE</li> </ul> |

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

# 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>)

## Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/25625/cert>)

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

## Address for declarations of conformity

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

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

## EC declaration of conformity



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

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

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

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

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

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

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

## UK Declaration of Conformity



Importer UK:

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

The product meets the requirements of the following directives:

- UKEX Regulations

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

- EMC Regulations

SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

- RoHS Regulations

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

**ATEX / IECEx / UKEX / CCC-Ex**

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

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

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 30).

The product meets the explosion protection requirements outlined below.

**IECEx**

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

The product meets the requirements of the standards:

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

**ATEX**

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

The product meets the requirements of the standards:

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

**UKEX**

Classification: II 3 G Ex ec IIC T4 Gc, Certificate no.: DEKRA 21UKEX0003 X

The product meets the requirements of the standards:

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

Importer UK: Siemens plc (see above)

**CCC-Ex**

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

The product meets the requirements of the following standards:

- GB 3836.1  
Hazardous areas - Part 0: Equipment - General requirements
- GB 3836.8  
Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

## EMC

The CP meets the requirements of the following directives:

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

Applied standards:

- EN 61000-6-2

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

- EN 61000-6-4

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

## RoHS

The CP meets the requirements of the following directives:

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

Applied standard: EN IEC 63000

c(UL)us



Applied standards:

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

Report / UL file: E 85972 (NRAG, NRAG7)

## cULus Hazardous (Classified) Locations



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

Applied standards:

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

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

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

Report / UL file: E223122 (NRAG, NRAG7)

Note the conditions for the safe deployment of the product according to the section Link: (<https://support.industry.siemens.com/cs/ww/en/view/78381013>).

---

#### 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.

### Marking for the customs union



EAC (Eurasian Conformity)

Eurasian Economic Union of Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan

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

### 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/25625/cert>)

## Dimension drawings

All dimensions in the dimension drawings are in millimeters.

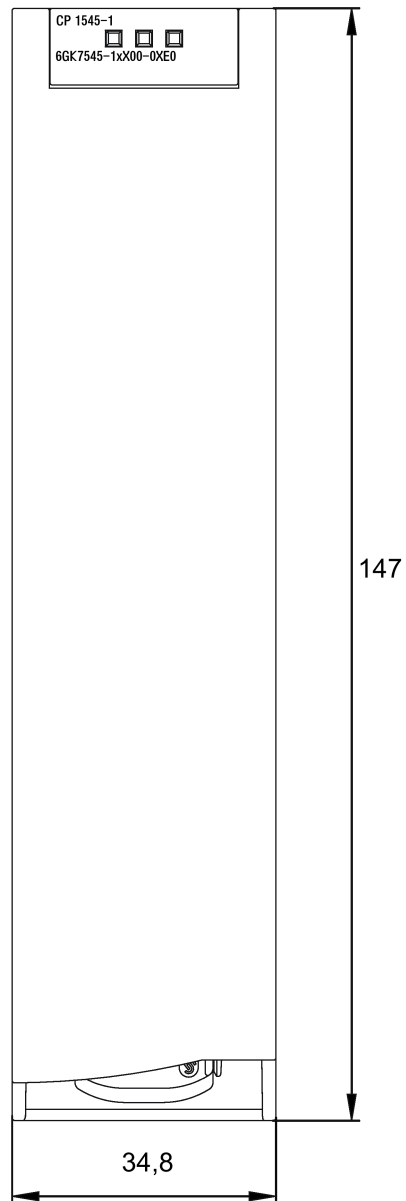


Figure 9-1 Front view

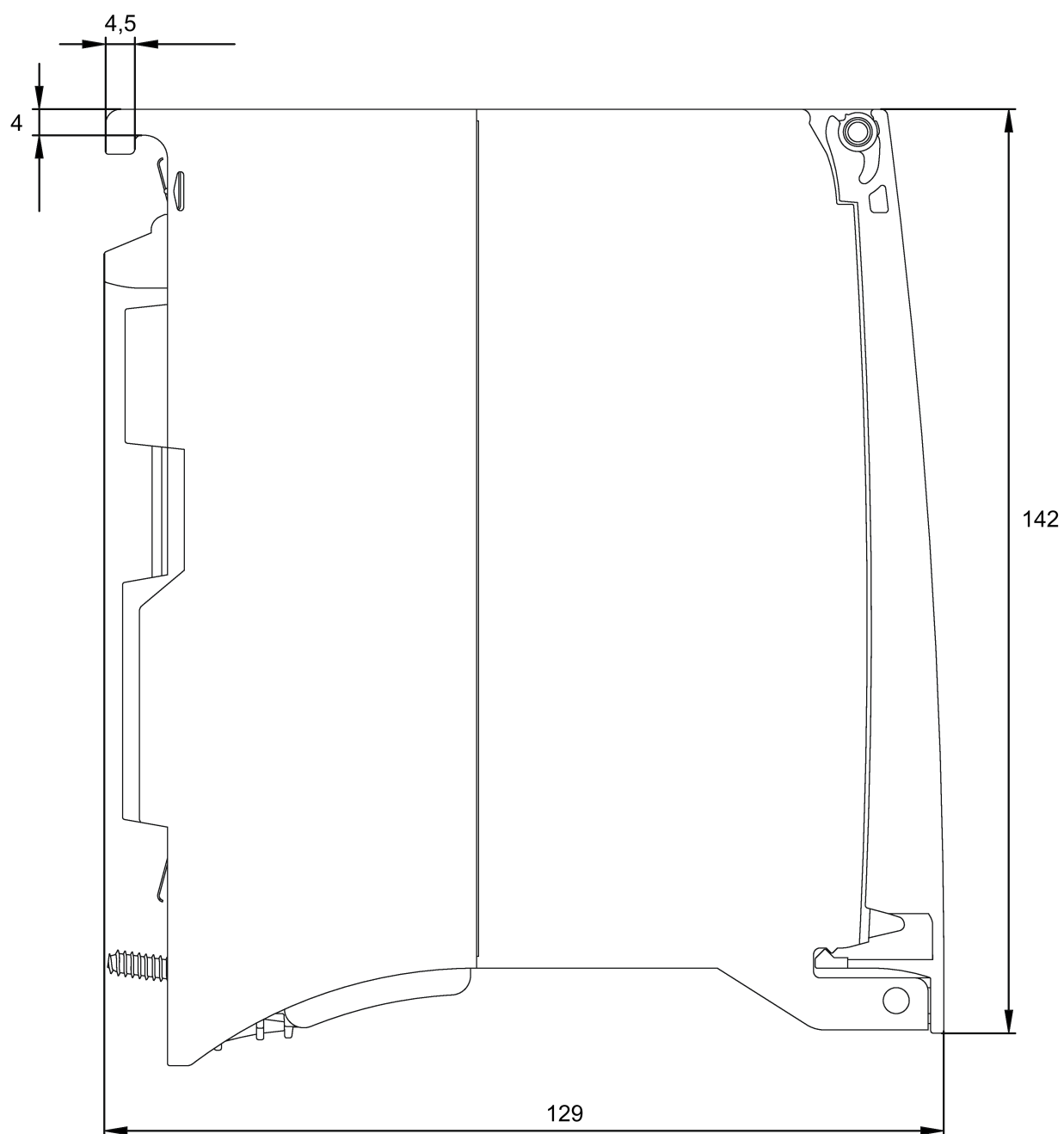


Figure 9-2 Side view

## Additional information

### A.1 Linking to other systems with FETCH/WRITE

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

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

#### Structure of WRITE frame

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

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

#### Structure of FETCH frame

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

| FETCH request frame |                  |        | FETCH response frame |                  |        |
|---------------------|------------------|--------|----------------------|------------------|--------|
| 0                   | System ID        | = "S"  | 0                    | System ID        | = "S"  |
| 1                   |                  | = "5"  | 1                    |                  | = "5"  |
| 2                   | Length of header | = 0x10 | 2                    | Length of header | = 0x10 |
| 3                   | ID OP code       | = 0x01 | 3                    | ID OP code       | = 0x01 |

## A.1 Linking to other systems with FETCH/WRITE

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

## Parameter values

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

| <b>S7 address area</b> | <b>PI/PQ</b>                                                                                                        | <b>C</b>                                                                     | <b>T</b>                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| ORG ID                 | 05 <sub>H</sub>                                                                                                     | 06 <sub>H</sub>                                                              | 07 <sub>H</sub>                                                              |
|                        | Source/destination data from/to I/O modules<br>With source data input modules, with destination data output modules | Source/dest data from/to counter cells                                       | Source/dest data from/to timer cells                                         |
| DBNR                   | irrelevant                                                                                                          | irrelevant                                                                   | irrelevant                                                                   |
| Start address          | I/O byte no. from which the data is read or written.                                                                | Number of the counter cell from which the data is read or written.           | Number of the timer cell from which the data is read or written.             |
| Permitted range        | 0...127<br>digital I/O 128...255<br>anal. I/O                                                                       | 0...255                                                                      | 0...255                                                                      |
| Quantity               | Length of the source/destination data block in bytes                                                                | Length of the source/destination data block in words (counter cell = 1 word) | Length of the source/destination data block in words (counter cell = 1 word) |
| Permitted range        | 1...256                                                                                                             | 1                                                                            | 1                                                                            |



# Syslog messages

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

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

## B.1 Structure of the Syslog messages

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

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

| Part / Parameter | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HEADER</b>    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| PRI              | Priority of the Syslog message, divided into: <ul style="list-style-type: none"> <li>Severity (Severity)               <p>Possible values:</p> <ul style="list-style-type: none"> <li>– 0 Emergency</li> <li>– 1 Alert</li> <li>– 2 Critical</li> <li>– 3 Error</li> <li>– 4 Warning</li> <li>– 5 Notice</li> <li>– 6 Information</li> <li>– 7 Debug</li> </ul> </li> <li>Facility (Origin)               <p>Possible values, e.g.: Sub-system, service, user</p> </li> </ul> |
| VERSION          | Version number of the Syslog specification                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| TIMESTAMP        | Time stamp of the device as local time including time zone and correction for daylight saving/standard time<br>Format: YYYY-MM-DDThh:mm:ss.msmsmsms+xx:yy<br>Example: 2010-01-01T02:03:15.0003+02:00                                                                                                                                                                                                                                                                          |

| Part / Parameter       | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HOSTNAME               | Identifies the source device by either: <ul style="list-style-type: none"> <li>FQDN</li> <li>IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX</li> <li>IPv6 address according to RFC4291 Section 2.2</li> <li>Host name</li> </ul> "-" is output if information is missing.<br>In the product: The configured IPv4 address of the process interface P2                                                                                                                                                                                                                                                                                                 |
| APP-NAME               | Device or application from which the message originates. "-" is output if information is missing.<br>In the product: "-"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| PROCID                 | The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.<br>In the product: "-"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MSGID                  | ID to identify the message. "-" is output if information is missing.<br>In the product: "-"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>STRUCTURED-DATA</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| timeQuality            | The structured data element "timeQuality" provides information on system time with the two parameters "tzKnown" and "isSynced".<br>Example: [timeQuality tzKnown="0" isSynced="0"] <ul style="list-style-type: none"> <li>tzKnown           <p>This parameter specifies whether the time zone is known in the source device.</p> <ul style="list-style-type: none"> <li>1 = known</li> <li>0 = unknown</li> </ul> </li> <li>isSynced           <p>This parameter specifies whether the source device is synchronized with a reliable external time source, e.g. via NTP.</p> <ul style="list-style-type: none"> <li>1 = synchronized</li> <li>0 = not synchronized</li> </ul> </li> </ul> |
| <b>MSG</b>             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MESSAGE                | Message text as ASCII string (English)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

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

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

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

## B.2 Tags in Syslog messages

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

The output messages can contain the following variables:

| Variable                                         | Description                                                                                                                                             | Format                               | Possible values or example                                               |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------|
| {IP address}                                     | IPv4 address according to RFC1035<br>IPv6 address according to RFC4291 Section 2.2                                                                      | %d.%d.%d.%d<br>XXX.XXX.XXX.XXX       | 192.168.1.105<br>2001:DB8::8:800:200C:417A                               |
| {FQHN}                                           | Fully Qualified Host Name: Completely specified host name; specification as domain (FQDN) or as IP address.                                             | FQDN: host1.com<br>IPv4: %d.%d.%d.%d | server1<br>192.168.1.105                                                 |
| {Src port}<br>{Dest port}                        | Port number (decimal)                                                                                                                                   | %d                                   | 0 ... 65535                                                              |
| {Src mac}<br>{Dest mac}                          | Source/destination MAC address                                                                                                                          | %02x:%02x:%02x:%02x:%02x:%02x        | 00:0C:29:2F:09:B3                                                        |
| {Protocol}                                       | Layer 4 protocol or service used that generated the event.                                                                                              | %s                                   | UDP   TCP   WBM   Telnet   SSH   Console   PNIO   PB   OPC   TFTP   SFTP |
| {Group}                                          | Name for identification of the group (string without spaces)                                                                                            | %s                                   | ITservice                                                                |
| {User name}                                      | String (without spaces) that identifies the authenticated user by his or her name.                                                                      | %s                                   | <Name>                                                                   |
| {Local interface}                                | Symbolic name of the local interface                                                                                                                    | %s                                   | Console                                                                  |
| {Action user name} or<br>{Destination user name} | Identifies the destination user based on his/her name. This is not the authenticated user.                                                              | %s                                   | <First name>.<Name>                                                      |
| {Role}                                           | Symbolic name of the role                                                                                                                               | %s                                   | Administrator                                                            |
| {Time minute}<br>{Timeout}                       | Number of minutes                                                                                                                                       | %d                                   | 44                                                                       |
| {Time second}                                    | Number of seconds                                                                                                                                       | %d                                   | 44                                                                       |
| {Failed login count}                             | Number of failed login attempts                                                                                                                         | %d                                   | 10                                                                       |
| {Max sessions}                                   | Maximum number of sessions                                                                                                                              | %d                                   | 10                                                                       |
| {Trigger pin}                                    | String (without spaces) for an IO pin that triggered the event.                                                                                         | %s                                   | DI1                                                                      |
| {Firewall rule}                                  | String (with spaces) for a firewall rule set                                                                                                            | %s                                   | Rule1                                                                    |
| {Subject}                                        | String (with spaces) for the subject in the certificate. Used as part of the certificate-based authentication and must also include Unicode characters. | %s<br>With UTF8 code: %S             | Subject                                                                  |
| {Config detail}                                  | String (with spaces) for the identification of a part of the configuration                                                                              | %s                                   | OpenVPN                                                                  |
| {Connection name}                                | Name of the VPN connection                                                                                                                              |                                      | Connection_1                                                             |

| Variable                 | Description                                 | Format | Possible values or example |
|--------------------------|---------------------------------------------|--------|----------------------------|
| {Firewall accept}        | Firewall action executed (accepted package) |        | ACCEPT                     |
| {Firewall action reject} | Firewall action executed (rejected package) |        | REJECT DROP                |
| {Length}                 | Length of the network packet (in bytes)     | %d     | 52                         |
| {Network interface}      | Symbolic name of a network interface        | %s     | vlan 1                     |

## B.3 Messages

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

### B.3.1 Non-repudiation

|              |                                                                            |
|--------------|----------------------------------------------------------------------------|
| Message text | {Protocol}: User {User name} has changed configuration.                    |
| Example      | Console: User admin has changed configuration.                             |
| Explanation  | User has changed the configuration data by loading new configuration data. |
| Severity     | Info                                                                       |
| Facility     | local0                                                                     |
| Standard     | IEC 62443-3-3 Reference: SR 2.12                                           |

# Index

## A

Abbreviations/acronyms, 4  
Article number, 3

## C

Cell protection concept  
    VPN, 54  
CloudConnect, 64  
Compatibility  
    V1.0 - V1.1, 81  
Configuration limits  
    Communications modules, 19  
Connection abort, 85  
Connection resources of the CPU, 20  
Connections for Web  
    Quantity, 21  
Cross-references (PDF), 5

## D

Data buffering, 94  
Data management - Configuration data, 127  
Data transmission (cloud), 77  
DHCP, 127  
Disposal, 7  
DNS server - program-controlled change, 103  
Double addressing in the network, 45

## E

E-mail, 13  
E-mail connection, 21  
Ethernet interface, 27  
    Configuration via T\_CONFIG, 103

## F

FETCH/WRITE, 14  
    Enable in CPU, 44  
    Functions, 42  
    S5/S7 addressing mode, 18  
FETCH/WRITE connections, 21  
Firewall, 18

## Firmware

Version, 3

## FTP

Enable in CPU, 44  
Response if the reference to the FTP job block is missing, 112  
FTP (FTP client), 20  
FTP client  
    Configuration limits, 23  
FTP server  
    Configuration limits, 23  
FTP\_CMD, 103, 104  
    Block execution time, 23  
FTPS, 19  
FTPS - Security, 63

## G

Gateway (VPN), 57  
Gigabit specification, 27  
Glossary, 8

## H

Hardware version, 3  
HMI communication, 14

## I

Instructions (OUC), 99  
IP address  
    Via DHCP, 45  
IP address - program-controlled change, 103  
IP configuration  
    IPv4 / IPv6, 17  
IP routing, 46  
IPv6 address  
    Use, 17  
ISO transport connections, 21  
ISO-on-TCP (RFC 1006), 13  
ISO-on-TCP connections, 21  
ISO-Transport (RFC 8073), 13

## L

Logging, 19  
Logging server, 60

**M**

MAC address, 17  
MIB, 122  
Multicast (UDP), 13

**N**

NTP, 16  
NTP (secure), 19, 52  
NTP server - program-controlled change, 103

**O**

Online diagnostics, 119  
Online functions, 120  
OP connections  
    Quantity, 21  
Open User Communication (OUC), 13  
Operating mode of the CPU, 37  
OUC (Open User Communication), 99

**P**

Passive VPN connection establishment, 57  
PG communication, 14  
PG connections  
    Quantity, 21  
Port 8448, 120  
Power supply modules  
    Additional, 19  
Product name, 4  
Program blocks - max. Data length, 22  
Programmed communications connections, 47  
Programmed connections  
    Quantity, 21  
PUT/GET  
    Enable in CPU, 44

**Q**

QoS, 93  
QualityCode, 85  
Quantity  
    Communications modules, 19

**R**

Recycling, 7  
Replacement part, 24  
RUN → STOP, 37

**S**

S7 communication, 14  
S7 connections, 20  
    Number of freely usable, 21  
Safety notices, 29  
Security diagnostics, 120  
Service & Support, 8  
SIMATIC NET glossary, 8  
SMTPS, 19  
SNMP, 49, 122  
SNMPv3, 19  
STEP 7 - version, 24  
System data type  
    FTP\_..., 103  
    TCON\_..., 102  
    TMail\_..., 102

**T**

T\_CONFIG, 103  
TCON, 102  
TCP (RFC 793), 13  
TCP connections, 21  
TCP connections for FTP, 23  
TDISCON, 102  
Time-of-day synchronization, 16  
    Recommendations, 52  
Training, 8  
TRCV, 102  
TSEND, 102

**U**

UDP, 22  
UDP (RFC 768), 13  
UDP connections, 21

**V**

Virtual Private Network  
    Definition, 53  
VPN, (Virtual Private Network)  
    Areas of application, 54  
    Cell protection concept, 54

**W**

Web server, 17