

# SIEMENS

## SIMATIC NET

### S7-1200 - TeleControl CP 1243-7 LTE

#### Operating Instructions

#### Preface

Application and properties

**1**

LEDs and connectors

**2**

Installation, connecting up,  
commissioning

**3**

Configuration and operation

**4**

Programming the  
program blocks

**5**

Diagnostics and upkeep

**6**

Technical specifications

**7**

Dimension drawings

**A**

Approvals

**B**

Accessories

**C**

Documentation references

**D**

CP 1243-7 LTE-EU




01/2015

C79000-G8976-C381-01

## Legal information

### Warning notice system

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

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


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

### Qualified Personnel

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

### Proper use of Siemens products

Note the following:

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

### Trademarks

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

### Disclaimer of Liability

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

# Preface

## Validity of this manual

This document contains information on the following product:

- CP1243-7 LTE-EU  
Article number 6GK7 243-7KX30-0XE0  
Hardware product version 1  
Firmware version V2.1

The device is the communications processor for connecting the SIMATIC S7-1200 via LTE, UMTS or GSM mobile wireless networks.



Figure 1 CP 1243-7 LTE

Behind the top hinged cover of the module housing, next to the article number you will see the hardware product version printed as a placeholder "X" (for example X 2 3 4). In this case, "X" would be the placeholder for hardware product version 1.

You will find the firmware version of the CP as supplied behind the top hinged cover of the housing to the left below the LED field.

You will find the IMEI under the lower hinged cover of the housing.

### TCSB:

Unless explicitly stated differently in the text, the way in which telecontrol communication works relates to a telecontrol server with the application "TeleControl Server Basic V3".

## Abbreviations/acronyms

- **CP**

Simplified designation of the product CP 1243-7 LTE-EU

- **TCSB**

TeleControl Server Basic V3, OPC server for telecontrol communication

- **Mobile wireless network**

The mobile wireless network(s) that support or use the relevant CP.

The precise standards and frequency bands which the two CPs support can be found in the sections Connecting the S7-1200 to a mobile wireless network (Page 11) and Technical specifications (Page 113).

## Purpose of the manual

This manual describes the properties of these modules and supports you when installing and commissioning the device.

The necessary configuration steps are described in the form of an overview.

You will also find instructions for operation and information about the diagnostics options of the device.

## New in this issue

First issue

## Replaced manual issue

None

## Current manual release on the Internet

You will also find the current version of this manual on the Internet pages of Siemens Industry Online Support under the following entry ID:

102255422 (<http://support.automation.siemens.com/WW/view/en/102255422>)

> > Entry list > Entry type "Manuals"

## Required experience

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

- Automation engineering
- Setting up the SIMATIC S7-1200
- SIMATIC STEP 7 Basic / Professional
- Data transfer via mobile wireless networks and Internet

## Sources of information and other documentation

You will find an overview of further reading and references in the Appendix of this manual.

## SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD  
The DVD ships with certain SIMATIC NET products.
- On the Internet under the following entry ID:  
50305045 (<http://support.automation.siemens.com/WW/view/en/50305045>)

## License conditions

---

### Note

#### Open source software

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

---

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

- DOC\_OSS-S7CMCP\_74.pdf
- DOC\_OSS-CP124x-7\_76.pdf

## Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit <http://www.siemens.com/industrialsecurity>.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit <http://support.automation.siemens.com>.

## **Firmware**

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

## **Training, Service & Support**

You will find information on Training, Service & Support in the multi--language document "DC\_support\_99.pdf" on the data medium supplied with the documentation.

## **Trademarks**

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SIMATIC, SIMATIC NET, SIMATIC STEP 7, SCALANCE, TeleControl Server Basic,  
MODEM MD720

# Table of contents

|          |   |           |
|----------|---|-----------|
|          | <b>Preface .....</b>  | <b>3</b>  |
| <b>1</b> | <b>Application and properties .....</b>                               | <b>11</b> |
| 1.1      | Connecting the S7-1200 to a mobile wireless network.....              | 11        |
| 1.2      | Communications services .....   | 13        |
| 1.3      | Other services and properties.....                                    | 14        |
| 1.4      | Performance data and configuration limits .....                       | 17        |
| 1.5      | Requirements for operation .....                                      | 19        |
| 1.6      | Configuration examples .....  | 21        |
| <b>2</b> | <b>LEDs and connectors .....</b>                                      | <b>27</b> |
| 2.1      | Opening the housing .....   | 27        |
| 2.2      | LEDs .....  | 28        |
| 2.3      | Electrical connectors .....   | 31        |
| 2.3.1    | Power supply .....  | 31        |
| 2.3.2    | Wireless interface .....  | 32        |
| <b>3</b> | <b>Installation, connecting up, commissioning .....</b>               | <b>33</b> |
| 3.1      | Important notes on using the device .....                             | 33        |
| 3.1.1    | Notices on use in hazardous areas .....                               | 34        |
| 3.1.2    | General notices on use in hazardous areas according to ATEX .....     | 35        |
| 3.1.3    | Notices regarding use in hazardous areas according to UL HazLoc ..... | 35        |
| 3.2      | Installing the CP and commissioning .....                             | 36        |
| <b>4</b> | <b>Configuration and operation .....</b>                              | <b>41</b> |
| 4.1      | Notes on operation.....   | 41        |
| 4.2      | Configuration in STEP 7 .....   | 41        |
| 4.3      | Information required for configuration.....                           | 42        |
| 4.4      | Configuration of the TeleService access .....                         | 45        |
| 4.5      | Configuring data points and messages .....                            | 47        |
| 4.6      | Datapoint types .....   | 48        |
| 4.7      | CPU scan cycle.....   | 50        |
| 4.8      | Process image, type of transmission, event classes, triggers .....    | 51        |
| 4.9      | Status IDs of data points.....  | 54        |
| 4.10     | Connection establishment .....  | 54        |
| 4.11     | Acknowledgment.....   | 55        |
| 4.12     | Calling a TeleService connection .....                                | 55        |

|          |   |            |
|----------|---|------------|
| 4.13     | Security functions.....   | 58         |
| 4.13.1   | VPN.....  | 58         |
| 4.13.1.1 | VPN (Virtual Private Network).....  | 58         |
| 4.13.1.2 | Addressing the CP when using VPN.....                                     | 59         |
| 4.13.1.3 | Creating a VPN tunnel for S7 communication between stations.....          | 59         |
| 4.13.1.4 | VPN communication with SOFTNET Security Client (engineering station)..... | 62         |
| 4.13.1.5 | Connection to the telecontrol server.....                                 | 62         |
| 4.13.1.6 | CP as passive subscriber of VPN connections.....                          | 63         |
| 4.13.2   | Firewall.....   | 63         |
| 4.13.2.1 | Firewall sequence when checking incoming and outgoing frames.....         | 63         |
| 4.13.2.2 | Notation for the source IP address (advanced firewall mode).....          | 63         |
| 4.13.2.3 | Firewall settings for S7 connections via a VPN tunnel.....                | 63         |
| 4.13.3   | Filtering of the system events.....                                       | 64         |
| 4.14     | Time-of-day synchronization.....  | 64         |
| 4.15     | STEP 7 configuration of individual parameters.....                        | 66         |
| 4.15.1   | Communication types.....  | 66         |
| 4.15.2   | Mobile wireless communications settings.....                              | 67         |
| 4.15.3   | Ethernet interface (X1).....  | 67         |
| 4.15.4   | Partner stations.....   | 70         |
| 4.15.4.1 | Partner stations > Telecontrol server.....                                | 70         |
| 4.15.4.2 | Partner for inter-station communication.....                              | 72         |
| 4.15.5   | Communication with the CPU.....   | 74         |
| 4.15.6   | E-mail configuration.....   | 75         |
| 4.15.7   | Data point configuration.....   | 76         |
| 4.15.7.1 | Data point name and data point index.....                                 | 76         |
| 4.15.7.2 | Threshold value trigger and Analog value preprocessing.....               | 77         |
| 4.15.7.3 | Threshold value trigger.....  | 78         |
| 4.15.7.4 | Analog value preprocessing.....   | 79         |
| 4.15.7.5 | Partner stations: Configuring the inter-station communication.....        | 85         |
| 4.15.8   | Messages.....   | 86         |
| 4.16     | Access to the Web server.....   | 89         |
| <b>5</b> | <b>Programming the program blocks.....</b>                                | <b>91</b>  |
| 5.1      | Program blocks for OUC.....   | 91         |
| 5.2      | Programming SMS messages via OUC.....                                     | 93         |
| 5.3      | TC_CONFIG for changing configuration data of the CP.....                  | 96         |
| 5.4      | IF_CONF: SDT for the configuration data of the CP.....                    | 99         |
| <b>6</b> | <b>Diagnostics and upkeep.....</b>  | <b>105</b> |
| 6.1      | Diagnostics options.....  | 105        |
| 6.2      | Downloading firmware.....   | 108        |
| 6.3      | Module replacement.....   | 111        |
| <b>7</b> | <b>Technical specifications.....</b>                                      | <b>113</b> |
| 7.1      | General technical specifications.....                                     | 113        |
| 7.2      | Technical specifications - wireless interface (CP 1243-7 LTE-EU).....     | 115        |
| 7.3      | Pin assignment of the socket for the external power supply.....           | 116        |



|          |                                       |            |
|----------|---------------------------------------|------------|
| <b>A</b> | <b>Dimension drawings</b> .....       | <b>117</b> |
| <b>B</b> | <b>Approvals</b> .....                | <b>119</b> |
| <b>C</b> | <b>Accessories</b> .....              | <b>125</b> |
|          | C.1        Antenna.....               | 125        |
|          | C.2        TS Gateway .....           | 125        |
| <b>D</b> | <b>Documentation references</b> ..... | <b>129</b> |
|          | <b>Index</b> .....                    | <b>131</b> |



# Application and properties

## 1.1 Connecting the S7-1200 to a mobile wireless network

The CP is intended for use in industrial environments.

### Type of communication, mobile wireless standards, frequency bands

Using the CP, the S7-1200 SIMATIC controller can be connected to mobile wireless networks of the following standards:

- **CP 1243-7 LTE-EU**

The CP supports the following mobile wireless standards:

- LTE 800 (B20) / 1800 (B3) / 2600 (B7)
- UMTS 900 (B8) / 2100 (B1)
- GSM 850 / 900, DCS 1800, PCS 1900

You will also find the supported frequency bands in the section General technical specifications (Page 113).

### Changing the mobile wireless standard if the network is not available

If the establishment of a connection via a mobile wireless network with the LTE standard fails, the CP attempts to dial in to an available network with the next lower mobile wireless standard. Fallback response of the CP 1243-7 LTE-EU: LTE → UMTS → GSM.

This is only possible if the corresponding mobile wireless standard is enabled in the configuration of the CP.

The CP allows the following types of WAN communication:

- Communication from remote stations to the telecontrol server (TCSB) in the master station (telecontrol communication)
- Inter-station communication  
Communication between stations and the master station (telecontrol communication)
- Direct communication  
Direct communication between stations (Open User Communication)

### National approvals

In countries in which the CP is approved, you will find this on the Internet on the pages of Siemens Industry Online Support under the following entry ID:

102255422 (<http://support.automation.siemens.com/WW/view/en/102255422>)

On the Internet page, select the "Entry list" tab and the "Certificates" entry type.

Refer also to the appendix "Approvals (Page 119)" of the manual.

## **IP-based WAN communication via mobile wireless networks**

The CP allows WAN communication from remote stations with a master station, communication between stations via a master station (inter-station communication) and direct communication between stations.

The CP supports the following services for communication via the mobile wireless network or via the mobile wireless network and the Internet:

- **Data services**

Transfer of process data via mobile wireless networks with the following standards:

- GPRS (General Packet Radio Service) / EDGE

The packet-oriented services for data transmission GPRS/EDGE are handled via the GSM network.

**Note:** The CP is not suitable for GSM networks in which the code multiplex method "Code Division Multiple Access" (CDMA) is used.

- UMTS (Universal Mobile Telecommunications System) / HSPA (High Speed Packet Access)

UMTS allows significantly higher transmission speeds than GSM.

HSPA is a further development of UMTS and once again allows higher transmission speeds.

- LTE (Long Term Evolution)

Mobile wireless specification with a higher transmission speed than UMTS.

- **SMS (Short Message Service)**

The CP can send and receive SMS messages.

- **E-mail**

The CP can send e-mails via mobile wireless and the Internet.

## 1.2 Communications services

The CP is intended for use in an industrial environment. The following applications are supported by the CP:

### Telecontrol communication

The following applications are possible if telecontrol communication is enabled in the configuration of the CP.

- Communication with a control center  
Remote S7-1200 stations communicate via the mobile wireless network and the Internet with a telecontrol server in the master station. The telecontrol server communicates with a higher-level control system using the integrated OPC server function.
- Event-driven sending of messages using SMS or e-mail  
Via the mobile wireless network, the CP sends SMS messages to mobile phones or e-mails to PCs with an Internet connection.  
Both types of messages are configured in telecontrol communication in STEP 7. The use of program blocks is not necessary.  
For information on the configuration, refer to sections E-mail configuration (Page 75) and Messages (Page 86).
- Inter-station communication between S7-1200 stations via the telecontrol server  
In this application, the CP establishes a connection to the telecontrol server via the mobile wireless network. The telecontrol server forwards the messages to the destination station.

For this communications service, the CP and TCSB use their own protocol on OSI layer 7 that among other things supports certain security functions, see section Other services and properties (Page 14).

### Direct communication via Open User Communication (OUC)

The program blocks of Open User Communication provide the CP with the following communication options:

- Communication between S7-1200 stations via the mobile wireless network  
For this, the CP must be assigned a fixed IP address, see section Other services and properties (Page 14).
- SMS and e-mail messages via the mobile wireless network
  - Sending and receiving SMS messages on mobile phones or S7 stations
  - Sending e-mails to PCs with an Internet connection

In contrast to the two corresponding services of telecontrol communication (see above), to transfer SMS messages/e-mails via OUC, program blocks need to be used, see section Program blocks for OUC (Page 91).

You will find examples of applications in the section Configuration examples (Page 21).

## S7 communication

Reading / writing data from / to a CPU via the mobile wireless network is possible if S7 communication is enabled in the configuration of the CP.

The following instructions are supported:

- PUT / GET

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

For S7 communication, the CP requires a fixed IP address, see section Other services and properties (Page 14).

## TeleService via the mobile wireless network

TeleService is possible if the online functions are enabled in the configuration of the CP.

A TeleService connection can be established between an engineering station (PC with STEP 7) and a remote S7-1200 station via the mobile wireless network and the Internet.

You can use the TeleService connection for the following purposes:

- Downloading project or program data from the STEP 7 project to the station
- Querying diagnostics data on the station

You will find application examples of the structure in the section Configuration examples (Page 21).

For more detailed information, refer to section Calling a TeleService connection (Page 55).

# 1.3 Other services and properties

## Other services and properties

- **Data point configuration**

Due to the data point configuration in STEP 7, programming program blocks in order to transfer the process data is unnecessary. The individual data points are processed one-to-one in the control system.

- **IP configuration**

The CP is assigned a dynamic or a fixed IP address by the mobile wireless network provider:

- Dynamic IP address

When using telecontrol communication, the mobile wireless network provider generally assigns the CP a dynamic IP address. You set this in STEP 7 in the parameter group "Ethernet interface > Ethernet addresses".

- Fixed IP address

To use S7 communication or to receive data via Open User Communication, the CPU must be reachable via a fixed IP address. In this case, enter the fixed IP address assigned by the mobile wireless network provider in the same parameter group.

- **Time-of-day synchronization**

- When telecontrol communication is enabled, the CP obtains its local time of day as UTC time from the partner (TCSB). The time of day can be read from the CPU. The mechanisms are described in the STEP 7 information system.

For information on the format of the time stamp, refer to the section Datapoint types (Page 48).

If telecontrol communication is disabled, the time of day can be obtained from an NTP server.

- If the security functions are enabled, the secure method NTP (secure) can be used.

For more information, refer to the section Time-of-day synchronization (Page 64).

- **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 the station.

- **Data buffering: Storage of event data**

If a connection fails, the CP can buffer the data of events of different classes and transfer them bundled to the telecontrol server.

- **Data transfer is on request or triggered**

The telecontrol communication with TCSB is triggered in two ways:

- After a request by TCSB or an OPC client connected to TCSB
- Triggered by various selectable criteria

**Logging status data and its transfer to the telecontrol server**

For example:

- Data volumes transferred
  - ID of the wireless cell in the area of the station
  - GSM signal strength
  - Communication status
- etc.

- **Analog value processing**

Analog values can be preprocessed on the CP according to various methods.

- **Diagnostics SMS message**

At the request of a mobile phone, the CP sends an SMS message with diagnostics data to this mobile phone.

## Security functions of the telecontrol protocol

The CP supports the following Security functions:

- **Encrypted telecontrol communication**

You configure the interval of the key exchange between the CPU and telecontrol server in STEP 7 in the parameter group "Ethernet interface (X1) > Advanced options > Transfer settings".

- **Configuring authorized phone numbers on the CP**

To authorize nodes allowed to establish a connection to the CP during telecontrol communication.

- **Telecontrol password**

To authenticate the CP with the telecontrol server

- **STARTTLS / SMTPS**

For the secure transfer of e-mails

- **NTP (secure)**

For secure transfer during time-of-day synchronization (with telecontrol communication disabled)

- **HTTPS**

For secure access to the Web server of the CPU

---

### Note

#### Plants with security requirements - recommendation

Use the following option:

- If you have systems with high security requirements, use the secure protocols NTP (secure) and HTTPS.
  - 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 limitation" of the firewall, you can restrict the possibility of flooding and DoS attacks.
- 

## Industrial Ethernet Security - Security functions of the CP

The following Security functions can be used independently of telecontrol communication.

With Industrial Ethernet Security, individual devices, automation cells or network segments of an IP-based network can be protected. The data transfer via the CP can be protected from the following attacks by a combination of different security measures:

- Data espionage
- Data manipulation
- Unauthorized access



Secure underlying networks can be operated via additional Ethernet/PROFINET interfaces of the CPU.

As a result of using the CP, as a Security module, the following additional Security functions are accessible to the S7-1200 station on the interface to the external network:

- **Firewall**

- IP firewall with stateful packet inspection (layer 3 and 4)
- Firewall also for "non-IP" Ethernet frames according to IEEE 802.3 (layer 2)
- Limitation of the transmission speed ("Bandwidth limitation")
- Global firewall rules

- **Communication made secure by IPsec tunnels (VPN)**

VPN tunnel communication allows the establishment of a secure IPsec tunnel for communication with a Security module.

The CP can be put together with other modules to form VPN groups during configuration. IPsec tunnels are created between all Security modules of a VPN group. All internal nodes of these Security modules can communicate securely with each other through these tunnels.

- **Logging**

To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a Syslog server.

For information on configuring the Security functions, refer to the section Security functions (Page 58).

You will find further information on the functionality and configuration of the Security functions in the information system of STEP 7 and in the manual /5/ (Page 130).

## 1.4 Performance data and configuration limits

### Number of simultaneous connections for telecontrol communication

- 1 reserved connection for user data exchange with the telecontrol server

### Number of possible partners for inter-station communication

- Max. 13 CPs as partners for inter-station communication
  - Of which:
    - Max. 3 sending partners
    - Max. 10 receiving partners
- Partners can be S7-1200 mobile wireless CPs with a data point configuration.

### Number of simultaneous TeleService connections

- Max. 1 TeleService connection

### Number of simultaneous connections for S7 communication and Open User Communication

A maximum total of 14 connection resources for S7 communication and Open User Communication

The maximum number can be divided up as required into:

- S7 connections (PUT/GET)
- TCP connections
- ISO-on-TCP connections
- UDP connections

### Number of connections to NTP servers

- Max. 1 connection to an NTP server

### User data

With the connection types listed below, the user data of a frame represent a consistent data area in terms of the time of transfer.

User data per frame with the various connection types:

- For TCP connections: Max. 8192 bytes
- For ISO-on-TCP connections: Max. 1452 bytes
- For UDP connections: Max. 1472 bytes

With frames of telecontrol communication, the individual values of the data points are time stamped.

### Number of PLC tags for data point configuration

The maximum number of PLC tags that can be used for data point configuration is 100.

### Frame memory (send buffer)

The CP has a frame memory (send buffer) for data points configured as an event.

The send buffer has a maximum size of 64 000 events divided into equal parts for all configured communications partners. The size of the frame memory can be set in STEP 7. See also section Process image, type of transmission, event classes, triggers (Page 51).

## **Messages: E-mail / SMS**

Up to 10 messages can be configured in STEP 7 and sent as e-mails or SMS messages.

Maximum number of characters that can be transferred per SMS message: 160 ASCII characters including any value sent at the same time

Maximum number of characters that can be transferred per e-mail: 256 ASCII characters including any value sent at the same time

## **IPsec tunnel (VPN)**

An IPsec tunnel can be established for secure communication with another Security module.

## **Firewall rules**

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

The firewall rules are divided up as follows:

- Maximum 226 rules with individual addresses
- Maximum 30 rules with address ranges or network addresses (e.g. 140.90.120.1 - 140.90.120.20 or 140.90.120.0/16)
- Maximum 128 rules with limitation of the transmission speed ("Bandwidth limitation")

# **1.5 Requirements for operation**

## **Hardware requirements**

Apart from the CP in the remote S7-1200, the following hardware is also required:

- A CPU with firmware version as of V4.1
- An external antenna for the CP

Use only antennas from the accessories program for the CP, refer to the appendix Antenna (Page 125).

- For telecontrol communication, a PC with an Internet connection is required for the telecontrol server in the master station.
- If you intend to use TeleService via mobile wireless, a TeleService gateway with Internet access is required for configurations without a telecontrol server. This is a PC on which the "TS Gateway" software is installed, see appendix TS Gateway (Page 125).

## Configuration software

To configure the module, the following configuration tool is required:

STEP 7 Basic V13 + SP1

## Program blocks for Open User Communication and S7 communication

For Open User Communication and S7 communication, program blocks are required, see section Communications services (Page 13).

## Software for telecontrol communication and TeleService

The CP is configured in "Telecontrol" mode.

- For the telecontrol communication

The telecontrol server requires the "TCSB" software in the master station.

- For TeleService

For TeleService a switching station is required between the CP and the engineering station (with STEP 7 in the version specified above).

This is either the telecontrol server or a TeleService gateway:

- When using telecontrol communication, the telecontrol server is the switching station.
- To use TeleService without a telecontrol server, the "TS Gateway" software is required for the TeleService gateway.

The software and the manual describing it are on the DVD that ships with the CP.

For the documentation of the application, see /4/ (Page 130) or /3/ (Page 130) in the References.

## Requirements for using mobile wireless services

- A contract with a suitable mobile wireless network provider

The contract must allow the transfer of data.

IP address:

- For communication with the telecontrol server, a private (fixed) or public (dynamic) IP address assigned by the mobile wireless network provider can be used.
- For direct communication between S7 stations (S7 communication and Open User Communication via T blocks) the mobile wireless network provider must assign a fixed IP address to the CP and forward the frames to the destination nodes.

- The SIM card and PIN belonging to the mobile wireless contract

The SIM card is inserted in the CP.

With mobile wireless contracts in which the network provider does not assign a PIN, no PIN is necessary for the configuration of the CP.

- Local availability of a mobile wireless network in the range of the station.

## 1.6 Configuration examples

Below, you will find configuration examples for stations with a CP 1243-7 LTE.

### SMS messages and e-mails

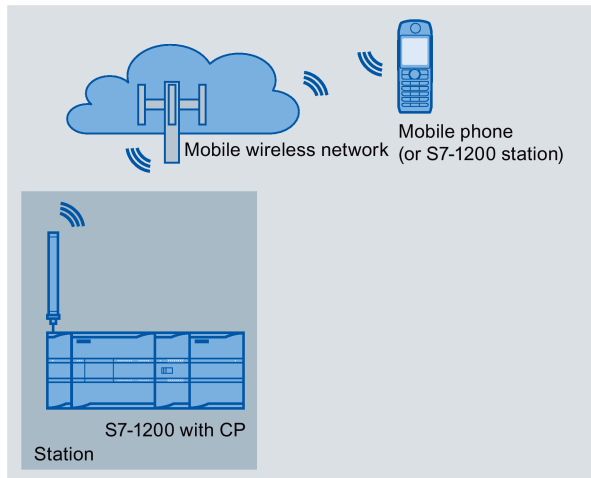


Figure 1-1 Sending messages by SMS from an S7-1200 station

### SMS

The CP can send SMS messages to a mobile phone or a configured S7-1200 station and receive from these nodes. The mechanisms for this are as follows:

- SMS messages generated and sent as the result of an event.  
For a description of the configuration, refer to the sections Configuring data points and messages (Page 47) and Messages (Page 86).
- SMS messages that are sent or received due to calling the corresponding program blocks of Open User Communication.  
You will find information on the blocks in the section Program blocks for OUC (Page 91), you will find the description of the programming in the STEP 7 information system.
- Using a mobile phone, a diagnostics SMS can be requested, see section Diagnostics options (Page 105).

For all mobile phones that send SMS messages to the CP, the authorize phone number must be specified in the STEP 7 configuration of the CP (parameter group "Security > Authorized phone number").

### E-mails

The CP can send e-mails to a PC with an Internet connection or a mobile phone. The mechanisms for this are as follows:

- E-mails generated and sent as the result of an event.

For a description of the configuration, refer to the sections Configuring data points and messages (Page 47), Messages (Page 86) and E-mail configuration (Page 75).

- E-mails sent as a result of calling the program block TMAIL\_C.

You will find information on the blocks in the section Program blocks for OUC (Page 91), you will find the description of the programming in the STEP 7 information system.

### Telecontrol by a control center

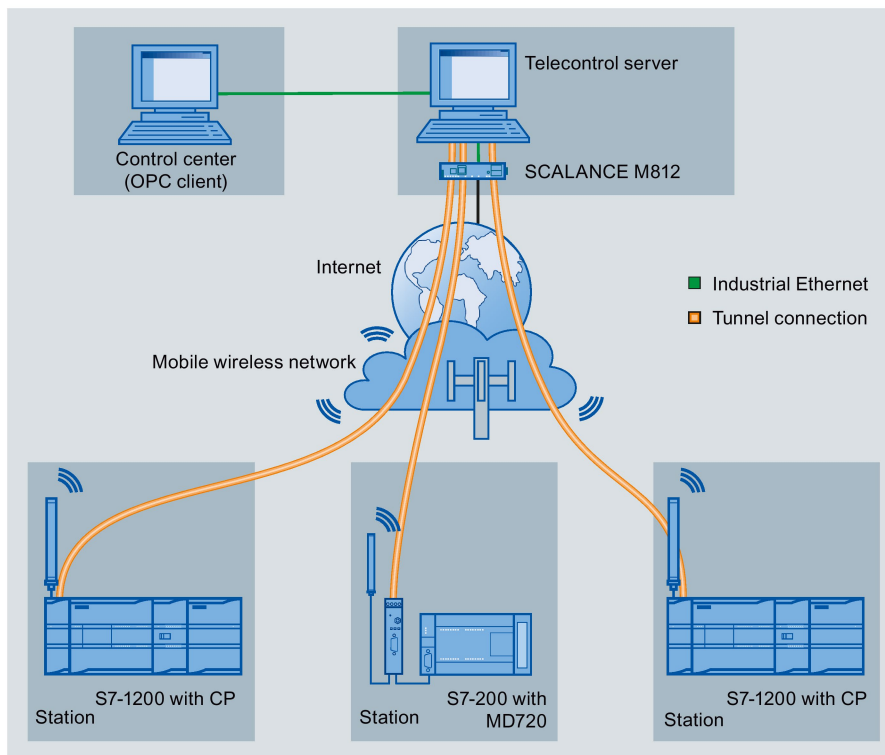


Figure 1-2 Communication between S7-1200 stations and a control center

In the telecontrol applications, the CP communicates with a telecontrol server with an Internet connection via the mobile wireless network. The "TeleControl Server Basic V3" (TCSB) application is installed on the telecontrol server in the master station. This results in the following use cases:

- Communication between a station and a control room with OPC client

The station communicates with the telecontrol server. Using its integrated OPC server, the telecontrol server exchanges data with the OPC client of the control room.

The OPC client and telecontrol server can be located on a single computer, for example when TCSB is installed on a control center computer with WinCC.

- Inter-station communication via a control center

Inter-station communication is possible with S7 stations equipped with a suitable telecontrol CP: CP 1243-1, CP 1242-7 GPRS V2, CP 1243-7 LTE

To allow inter-station communication, the telecontrol server forwards the messages of the sending station to the receiving station.

## Direct communication between stations

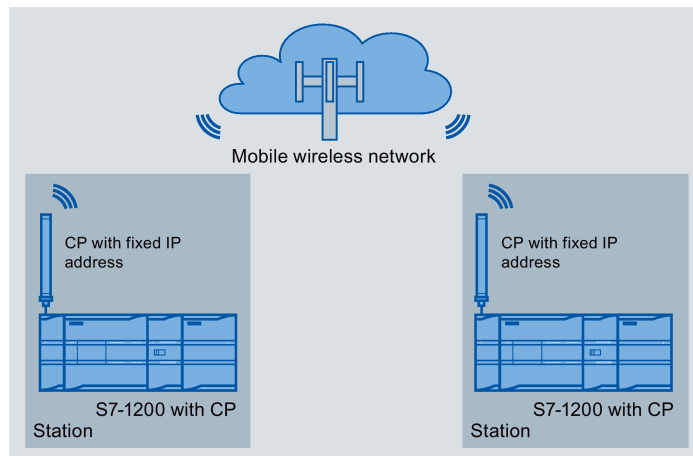


Figure 1-3 Direct communication between two S7-1200 stations

In this configuration, two SIMATIC S7-1200 stations communicate directly with each other using the CP via the mobile wireless network. Each CP has a fixed IP address. The relevant service of the network provider must allow this.

## TeleService via the mobile wireless network

In TeleService via the mobile wireless network, an engineering station on which STEP 7 is installed communicates via the mobile wireless network and the Internet with the CP in the S7-1200.

Since the firewall of the network provider is normally closed for connection requests from the outside, a switching station between the remote station and the engineering station is required. This switching station can be a telecontrol server or, if there is no telecontrol server in the configuration, a TeleService gateway.

### TeleService with telecontrol server

The connection runs via the telecontrol server.

- The engineering station and telecontrol server are connected via the Intranet (LAN) or Internet.
- The telecontrol server and remote station are connected via the Internet and via the mobile wireless network.

The engineering station and telecontrol server can also be the same computer; in other words, STEP 7 and TCSB are installed on the same computer.

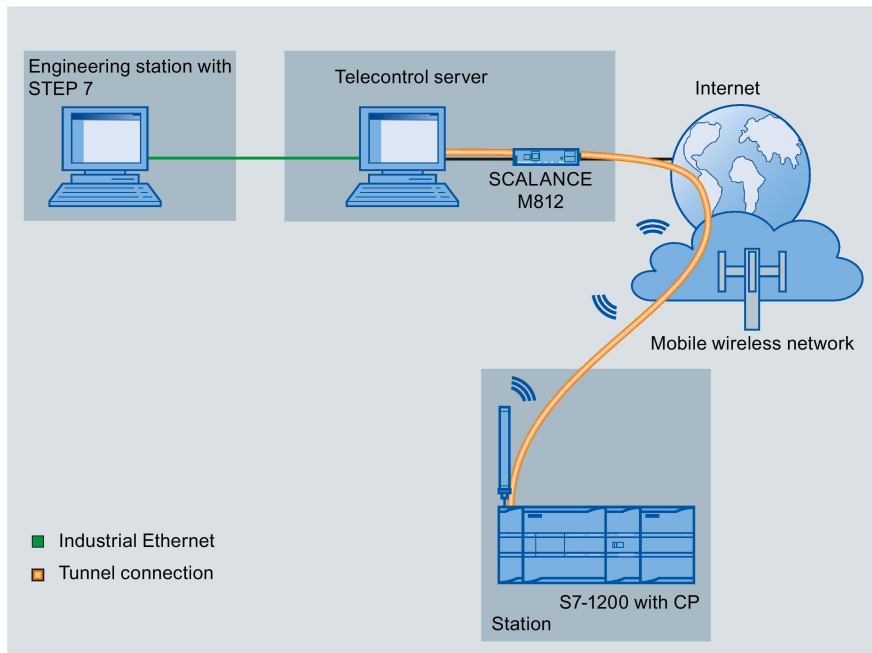


Figure 1-4 TeleService via the mobile wireless network in a configuration with telecontrol server



### TeleService with TeleService gateway (via LAN)

The connection between the engineering station and S7 station is via the TeleService gateway.

The engineering station is connected to the TeleService gateway via LAN.

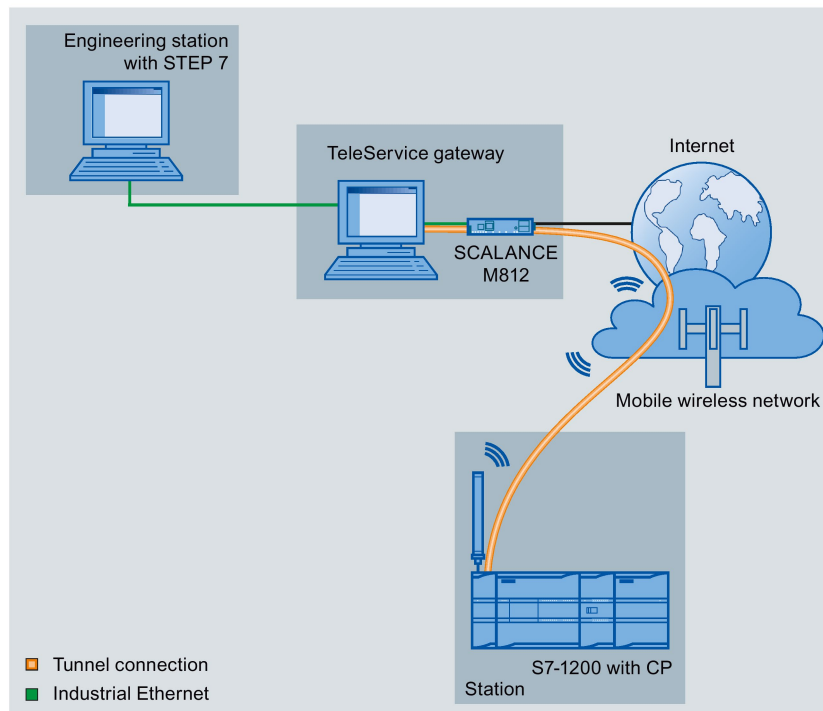


Figure 1-5 TeleService via the mobile wireless network with TeleService gateway - connection via LAN

### TeleService with TeleService gateway (via the Internet)

The connection between the engineering station and S7 station is via the TeleService gateway.

The engineering station is connected to the TeleService gateway via the Internet.

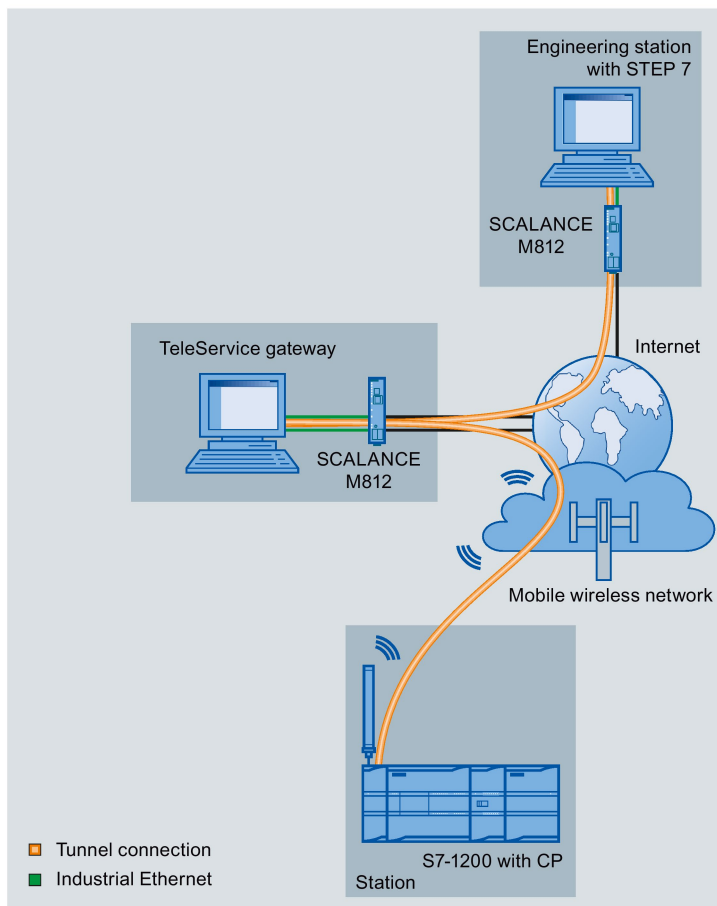


Figure 1-6 TeleService via the mobile wireless network with TeleService gateway - connection via the Internet

## LEDs and connectors

### 2.1 Opening the housing

#### Location of the display elements and the electrical connectors

The LEDs for the detailed display of the module statuses are located behind the upper cover of the module housing.

The socket for the power supply is located on the top of the module.

The connector for the external antenna is located on the bottom of the module.

The compartment for inserting the SIM card is located behind the upper hinged cover of the module.

#### Opening the housing

Open the upper or lower cover of the housing by pulling it down or up as shown in the illustration. The covers extend beyond the housing to give you a grip.

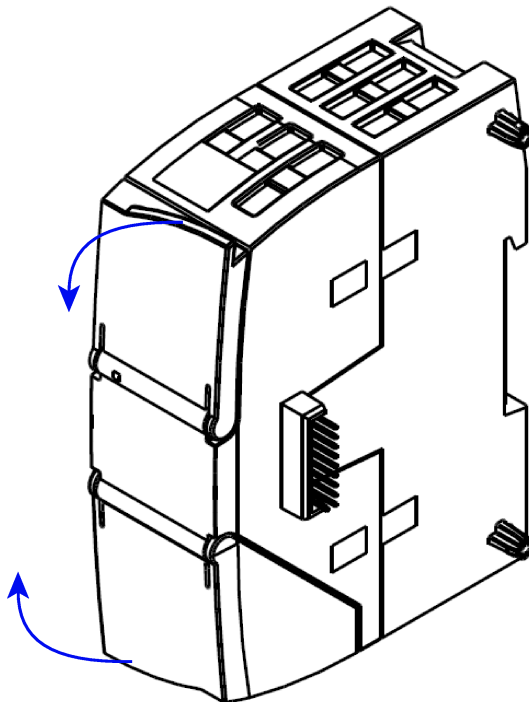


Figure 2-1 Opening the housing

## 2.2 LEDs

### LEDs of the module

The CP has the following LEDs for displaying the status:

- "DIAG" LED on the front panel  
The "DIAG" LED that is always visible shows the basic statuses of the module.
- LEDs below the upper cover of the housing  
These LEDs provide further details on the module status.

Table 2- 1 LED on the front panel






| LED / colors   | Name | Meaning                    |
|--|------|----------------------------|
| <br>red/green | DIAG | Basic status of the module |

Table 2- 2 LEDs below the upper cover of the housing

| LED / colors  | Name           | Meaning   |
|---|----------------|---|
| <br>red/green        | NETWORK        | Status of the connection to the mobile wireless network |
| <br>green          | CONNECT        | Status of the connection to the master station          |
| <br>yellow / green | SIGNAL QUALITY | Signal quality of the mobile wireless network           |
| <br>green          | VPN            | Status of the VPN connection                            |

#### Note

##### LED colors when the module starts up

When the module starts up, all its LEDs are lit for a short time. Multicolored LEDs display a color mixture. At this point in time, the color of the LEDs is not clear.









### Display of the operating and communication status

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

Table 2- 3 Meaning of the LED symbols

| Symbol     |  |  |  | -            |
|------------|---|---|---|--------------|
| LED status | OFF   | ON (steady light)   | Flashing  | Not relevant |

The LEDs indicate the operating and communications status of the module according to the following scheme:

| DIAG<br>(red / green)   | NETWORK<br>(red / green)  | CONNECT<br>(green)  | SIGNAL<br>QUALITY<br>(yellow / green)   | VPN<br>(green)  | Meaning  |
|---|---|---|---|---|--|
| <b>Display of the basic statuses of the module</b>  |   |   |   |   |  |
|                      |    |    |  |  | Power OFF  |
| <br>red              |    |    |  |  | Startup  |
| <br>flashing red     | -   |    | -   | -   | Errors: <ul style="list-style-type: none"> <li>Invalid CP configuration or</li> <li>CP type does not match the configuration data on the CPU.</li> </ul> |
| <br>green            | -   | -   | -   | -   | Running (RUN) without error  |
| <br>flashing red     | -   |    | -   | -   | Backplane bus error  |
| <br>flashing red    |   | -   | -   | -   | Missing SIM card   |
| <br>flashing red   |  | -   | -   | -   | Missing or incorrect PIN   |
| <b>Connection to the mobile wireless network</b>  |   |   |   |   |  |
| -   |  | -   | -   | -   | Existing connection to the service in the mobile wireless network  |
| -   |  | -   | -   | -   | No connection to the service in the mobile wireless network  |
| <b>Connection to communications partners</b>  |   |   |   |   |  |
| <br>green          |  |  | -   | -   | Connection established to at least one partner, CPU in RUN   |
| <br>green          |  |  | -   | -   | Connection established to at least one partner, CPU in STOP  |
| <br>flashing green |  |  | -   | -   | No partner reachable, CPU in RUN   |
| <br>flashing green |  |  | -   | -   | No partner reachable, CPU in STOP  |
| <br>flashing green |  |  | -   | -   | Telecontrol configuration exists, partner not reachable, CPU in RUN mode   |
| <br>flashing green |  |  | -   | -   | Telecontrol configuration exists, partner not reachable, CPU in STOP mode  |

2.2 LEDs

| DIAG<br>(red / green)                            | NETWORK<br>(red / green) | CONNECT<br>(green) | SIGNAL<br>QUALITY<br>(yellow / green) | VPN<br>(green) | Meaning   |
|--|--------------------------|--------------------|---------------------------------------|----------------|---|
| <b>Quality of the mobile wireless connection</b> |                          |                    |                                       |                |   |
| -  | -                        | -                  |                                       | -              | Good network (-73 ... ≥ -51 dBm)  |
| -  | -                        | -                  |                                       | -              | Medium strength network (-89 ... -74 dBm)   |
| -  | -                        | -                  |                                       | -              | Weak network (-109 ... -90 dBm)   |
| -  | -                        | -                  |                                       | -              | No network (≤ -110 dBm)   |
| <br>flashing red                                 | -                        | -                  |                                       | -              | Missing external power supply   |
| <b>VPN connections</b>                           |                          |                    |                                       |                |   |
| -  |                          | -                  | -                                     |                | VPN connection established  |
| -  |                          | -                  | -                                     |                | No VPN connection established   |
| -  | -                        | -                  | -                                     |                | No VPN connection configured on the CP  |
| <b>Loading firmware</b>                          |                          |                    |                                       |                |   |
|  |                          |                    |                                       |                | Loading firmware.<br>The "DIAG" LED flashes alternating red and green.  |
| <br>flashing green                               |                          |                    |                                       |                | Firmware was successfully loaded.   |
| <br>flashing red                                 |                          |                    |                                       |                | <ul style="list-style-type: none"> <li>• Error loading firmware or</li> <li>• Internal error of the CP; remedy: Power OFF → ON</li> </ul> |

## 2.3 Electrical connectors

### 2.3.1 Power supply

#### Power supply

The 3-pin socket for the external 24 V DC power supply is located on the top of the module. The matching plug ships with the product.

You will find the pin assignment of the socket in section Pin assignment of the socket for the external power supply (Page 116).

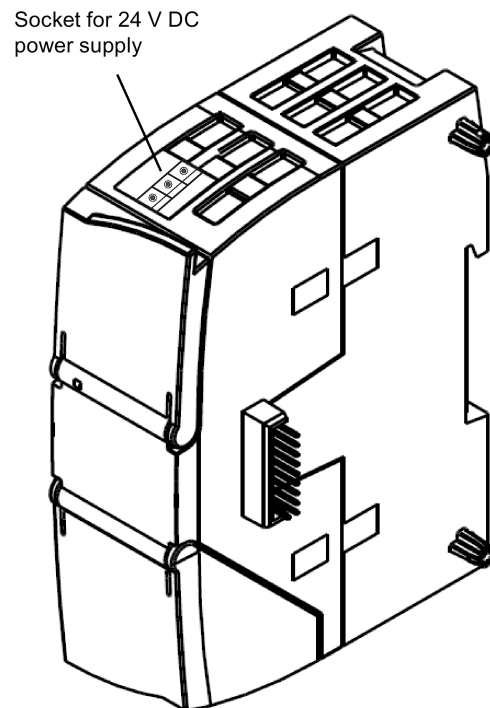


Figure 2-2 Socket for the 24 V DC power supply

## **2.3.2 Wireless interface**

### **Wireless interface for the mobile wireless network**

An extra antenna is required for communication in the mobile wireless network. This is connected via the SMA socket of the CP. The SMA socket is located behind the lower front cover of the CP.

You will find a suitable antenna for indoor and outdoor use in the section Accessories (Page 125).

### **More detailed information on the electrical connections**

For technical information on the electrical connections, refer to the section Technical specifications (Page 113).



# Installation, connecting up, commissioning

## 3.1 Important notes on using the device


### Safety notices on the use of the device


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


### Overvoltage protection


|   |
|---|
| <b>NOTICE</b>   |
| <b>Protection of the external power supply</b>  |
| If power is supplied to the module or station over longer power cables or networks, the coupling in of strong electromagnetic pulses onto the power supply cables is possible. This can be caused, for example by lightning strikes or switching of higher loads.   |
| The connector of the external power supply is not protected from strong electromagnetic pulses. To protect it, an external overvoltage protection module is necessary. The requirements of EN61000-4-5, surge immunity tests on power supply lines, are met only when a suitable protective element is used. A suitable device is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element. |
| Manufacturer:<br>DEHN+SOEHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt,<br>Germany  |


### 3.1.1 Notices on use in hazardous areas

|  |
|--|
|  <b>WARNING</b> |
| <b>EXPLOSION HAZARD</b>  |
| DO NOT OPEN WHEN ENERGIZED.  |


|   |
|---|
|  <b>WARNING</b>  |
| The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS).   |
| This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the equipment power supply must comply with NEC Class 2, as described by 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.   |


|   |
|---|
|  <b>WARNING</b> |
| <b>EXPLOSION HAZARD</b>   |
| DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.     |


|  |
|--|
|  <b>WARNING</b> |
| <b>EXPLOSION HAZARD</b>  |
| SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.               |

|   |
|---|
|  <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. |


### 3.1.2 General notices on use in hazardous areas according to ATEX

|   |
|---|
|  <b>WARNING</b>  |
| <b>Requirements for the cabinet/enclosure</b><br>To comply with EU Directive 94/9 (ATEX95), the enclosure or cabinet must meet the requirements of at least IP54 in compliance with EN 60529. |

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

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

### 3.1.3 Notices regarding use in hazardous areas according to UL HazLoc


|  |
|--|
|  <b>WARNING</b>           |
| <b>EXPLOSION HAZARD</b><br>DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS. |

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

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

## 3.2 Installing the CP and commissioning

### Prior to installation and commissioning

|  |
|--|
|  <b>WARNING</b>   |
| <b>Read the system manual "S7-1200 Programmable Controller"</b>  |
| Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller", refer to the documentation in the Appendix. |
| When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".  |

### Configuration

One requirement for the commissioning of the CP is the completeness of the STEP 7 project data (see below). You should also read the section "Configuration and operation (Page 41)".

### Inserting the SIM card

---

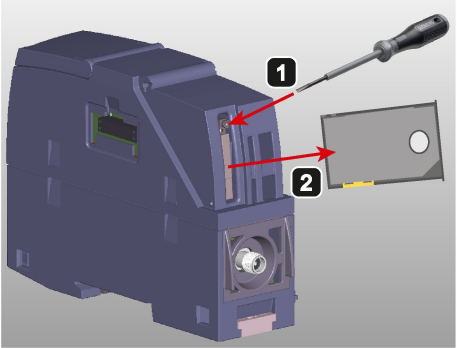
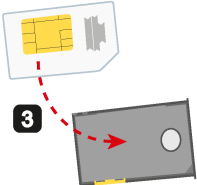
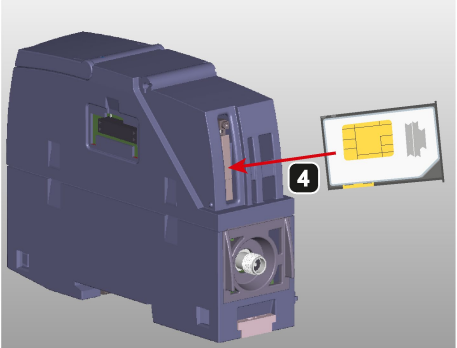
#### Note

#### Inserting and removing the SIM card

Do not insert or remove the SIM card while the CP is operating.

---

Prior to installation, insert the SIM card in the CP.

| Step | Execution   | Notes and explanations  |
|------|---|---|
| 1    | Turn off the power supply to the station.   |   |
| 2    | Release the slide for the SIM card on the bottom of the CP behind the lower cover by gently pressing the release pin. |   |
| 3    | Remove the slide from the housing.  |   |
| 4    | Insert the SIM card in the slide as illustrated.  |  |
| 5    | Push the slide back into the housing, where it locks gently in place.   |  |
| 6    | Turn on the power supply to the station.  |   |

**Dimensions for installation**

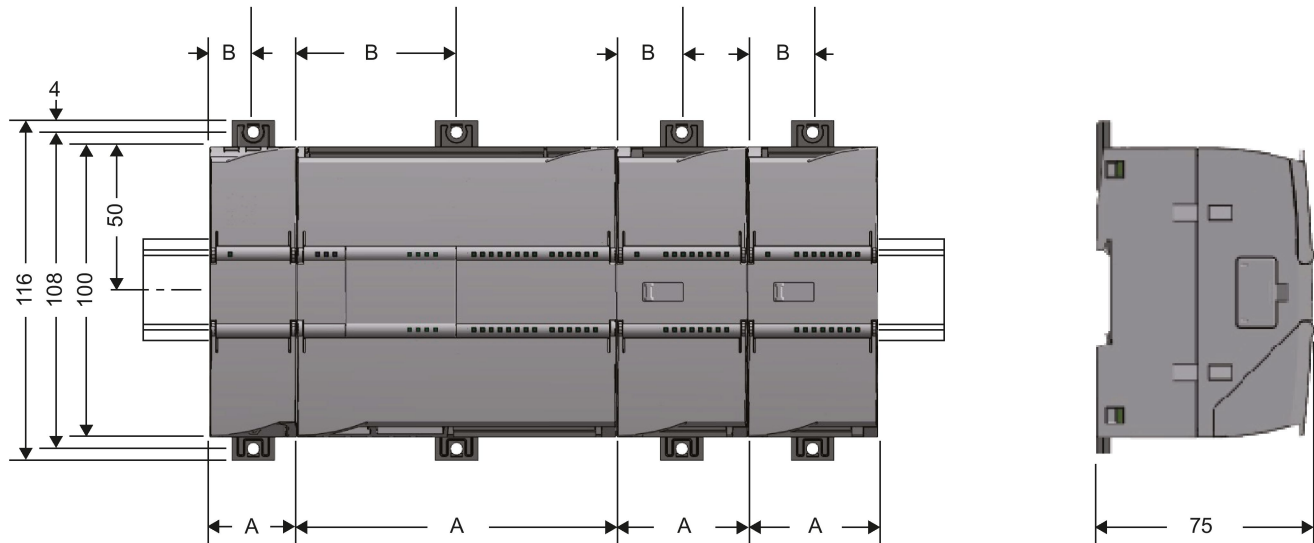


Figure 3-1 Dimensions for installation of the S7-1200

Table 3- 1 Dimensions for installation (mm)

| S7-1200 devices                              |   | Width A | Width B * |
|--|---|---------|-----------|
| CPU<br>(Examples)                            | CPU 1211C, CPU 1212C  | 90 mm   | 45 mm     |
|  | CPU 1214C   | 110 mm  | 55 mm     |
| Signal modules<br>(Examples)                 | 8 or 16 digital I/Os<br>2, 4 or 8 analog I/Os<br>Thermocouple, 4 or 8 I/Os<br>RTD, 4 I/Os | 45 mm   | 22.5 mm   |
|  | 16 analog I/Os<br>RTD, 8 I/Os   | 70 mm   | 35 mm     |
| Communications inter-<br>faces<br>(Examples) | CM 1241 RS232 / CM 1241 RS485   | 30 mm   | 15 mm     |
|  | CM 1243-5 (PROFIBUS master)<br>CM 1242-5 (PROFIBUS slave)                                 | 30 mm   | 15 mm     |
|  | CP 124x-7   | 30 mm   | 15 mm     |

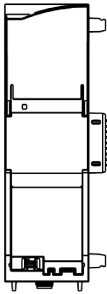
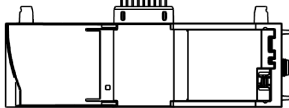
\* Width B: The distance between the edge of the housing and the center of the hole in the DIN rail mounting clip

**DIN rail mounting clips**

All CPUs, SMs, CMs and CPs can be installed on the DIN rail in the cabinet. Use the pull-out DIN rail mounting clips to secure the device to the rail. These mounting clips also lock into place when they are extended to allow the device to be installed in a switching panel. The inner dimension of the hole for the DIN rail mounting clips is 4.3 mm.

**Procedure for installation and commissioning**

|  |
|--|
| <b>NOTICE</b>  |
| <p><b>Installation location</b></p> <p>The module must be installed so that its upper and lower ventilation slits are not covered, allowing adequate ventilation. Above and below the device, there must be a clearance of 25 mm to allow air to circulate and prevent overheating.</p> <p>Remember that the permitted temperature ranges depend on the position of the installed device. You will find the permitted temperature ranges in the section General technical specifications (Page 113).</p> |

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

**Note**

**Connection with power off**

Only wire up the S7-1200 with the power turned off.

**Note**

**Power supply from the power outputs of the CPU**

The external power supply of the CP must be supplied via the power outputs of the CPU.

Keep within the maximum load of the power outputs of the CPU.

You will find data relating to the current consumption and power loss of the CP in the section General technical specifications (Page 113).

**Note**

**Turning off the station when plugging/pulling the CP**

Do not only turn off the power supply to the CP. Always turn off the power supply for the entire station.


Table 3- 2 Procedure for installation and connecting up

| Step | Execution  | Notes and explanations  |
|------|--|---|
| 1    | Mount the CP on the DIN rail and connect it to the module to its right.  | Use a 35 mm DIN rail.<br>The slots to the left of the CPU are permitted.  |
| 2    | Secure the DIN rail.   |   |
| 3    | Secure the power supply wires to the power output of the CPU.  |   |
| 4    | Secure the wires of the power supply to the plug supplied with the CP and insert the plug in the socket on the top of the CP.  | The pinning is shown beside the socket on the top of the housing. You will also find this in the section Pin assignment of the socket for the external power supply (Page 116).   |
| 5    | Connect the antenna to the SMA socket of the CP.   | Lower surface of the CP   |
|      | <p><b>Notice</b></p> <ul style="list-style-type: none"> <li>• Protect the antenna connector using suitable overvoltage protection equipment if the antenna cable is longer than 30 m.</li> <li>• Protect the antenna connector with suitable lightning protection if you install the antenna outdoors.</li> <li>• If you install several CPUs close to each other, keep to a minimum clearance of 50 cm between the antennas.</li> </ul> |   |
| 6    | Turn on the power supply.  |   |
| 7    | Close the front covers of the module and keep them closed during operation.  |   |
| 8    | The remaining steps in commissioning involve downloading the STEP 7 project data.  | <p>The STEP 7 project data of the CP is transferred when you load to the station. To load the station, connect the engineering station on which the project data is located to the Ethernet interface of the CPU.</p> <p>You will find more detailed information on loading in the following sections of the STEP 7 online help:</p> <ul style="list-style-type: none"> <li>• "Loading project data"</li> <li>• "Using online and diagnostics functions"</li> </ul> |



# Configuration and operation

## 4.1 Notes on operation

|   |
|---|
|  <b>CAUTION</b>  |
| <b>Minimum clearance to the device</b><br>The device may only be operated when the distance between the device (or antenna) and user is at least 20 cm. |
| <b>NOTICE</b>   |
| <b>Closing the front panels</b><br>To ensure interference-free operation, keep the front panels of the module closed during operation.                  |

## 4.2 Configuration in STEP 7

### Configuration in STEP 7

You configure the modules, networks and connections in an engineering station in SIMATIC STEP 7. You will find the required version in the section Requirements for operation (Page 19).

You can configure a maximum of three CMs/CPs per station. If you insert several CPs in an S7-1200, you can, for example, establish redundant communications paths.

### Configuring communication with the CPU (data point configuration)

CP communication is not programmed using program blocks but configured using data points.

One requirement for data point configuration is the programming of the assigned CPU and the input and output data of the station. To assign the user data to be transferred (input/output data) to the data points, you need to create PLC tags.

## Overview of the configuration steps in STEP 7

Notes:

- No Ethernet network needs to be created for the communication via the mobile wireless network.
- A telecontrol server or a TeleService- gateway cannot be configured in STEP 7.

Follow the steps below when configuring:

1. Create a STEP 7 project.
2. Insert the required SIMATIC stations.
3. Program the CPUs and the relevant inputs and outputs.
4. Create PLC tags for the input and output data to be transferred in the CPUs.
5. Insert the CPs in the relevant stations.
6. Configure the CPs including the data points and any messages (e-mail / SMS).

---

### Note

#### Changing the project number or station number for the entire STEP 7 project

If you change the project number or the station number in the "CP identification" parameter group for a telecontrol CP, these parameters are changed for all CPs in the STEP 7 project.

---

7. If required, program the program blocks for S7 communication and Open User Communication.
8. Save and compile the project.
9. Download the project data to the stations.

Using the "Download to device" function, the STEP 7 project data including the configuration data of the CPs is downloaded to the relevant CPU.

You will find further information on the individual steps in the following sections and in the help system of STEP 7.

## 4.3 Information required for configuration

To configure and commission the CP and the connected telecontrol system, the following information is required:

## General information

The following information is required for the STEP 7 configuration of the CP:

- Own phone number of the CP (required for TeleService)
- Authorized phone numbers  
Phone numbers of the nodes that are allowed to send an SMS to the CP.
- APN  
Name of the access point (APN) from the mobile wireless network to the Internet  
(information from the mobile wireless network provider)
- APN user name  
User name for the access point of the mobile wireless network provider
- APN password  
Password for the access point of the mobile wireless network provider
- Node number of the SMS master station (SMSC) when using SMS
- PIN of the SIM card

---

### Note

#### **Configured PIN and PIN on the SIM card must match.**

If you enter the PIN of the SIM card of the CP incorrectly during STEP 7 configuration and download the station, the CP stores the wrong PIN. An incorrectly entered PIN is transferred by the CP only once so that the SIM card is not locked.

If you change the PIN of the SIM card externally to the incorrectly configured PIN (new PIN of the SIM card = incorrectly entered PIN in STEP 7), the CP rejects this PIN again without checking it.

---

### Note

#### **Solution after entering an incorrect PIN:**

To avoid the PIN being rejected by the CP again, use a PIN that is different from the incorrectly entered PIN. Procedure:

- If the PIN of the SIM card was not changed:
    - Configure the PIN in STEP 7 with the PIN of the SIM card.
    - Reload the station.
  - If the original PIN of the SIM card was changed externally to the PIN that was previously incorrectly entered in STEP 7:
    - Change the PIN of the SIM card externally to a new PIN that has not yet been incorrectly configured in STEP 7.
    - Change the configured PIN in STEP 7 to the newly assigned PIN of the SIM card.
    - Reload the station.
-

### Information required for telecontrol communication

The following information is required for the STEP 7 configuration of the CP:

- Address of the telecontrol server
  - IP address
  - or
  - Name of the telecontrol server that can be resolved by DNS
  - IPT listener port (55097)
    - IPT listener port of the telecontrol server. Default setting: 55097

If only connections with TCSB are used (no direct communication), a dynamic IP address can be assigned to the CP by the Internet service provider.

For addressing a redundant TCSB system, refer to the section Partner stations > Telecontrol server (Page 70).

- DNS server address(es)

You require the DNS server address if you address the telecontrol server using a name that can be resolved by DNS and the DNS is not operated by the network provider. You configure DNS in the parameter group "DNS configuration":

  - If you do not specify an address, the DNS server address is obtained automatically from the network provider (recommended procedure).
  - If you want to use a different DNS server, enter its IP address. In this case, DNS servers of the network provider are not taken into account.

### CP parameter for configuring the telecontrol server

The following parameters from the STEP 7 configuration of the CP are also required for the configuration of the telecontrol server:

- Address and port of the telecontrol server
- Project number
- Station number
- Slot of the CP
- Telecontrol password
- Authorized phone numbers

## Address and authentication information for communication with TCSB

The following information is required for the STEP 7 configuration of the CP for communication with TCSB:

- Parameters in the "Partner stations" parameter group
  - Partner IP address  
Fixed IP address of the DSL router via which the telecontrol server is connected to the Internet.
  - Partner port (port number of the listener port of TCSB)
- Parameters in the "CP identification" parameter group ("Security" parameter group)
  - Project number
  - Station number
  - Password (for authentication)

## 4.4 Configuration of the TeleService access

### Configuration for using TeleService

To meet the requirements for using the TeleService functions for the CP, you need to make the necessary settings at the following points in STEP 7.

#### "Communication types" parameter group of the CP

Select the following options:

- Enable telecontrol communication
- Activate online functions

#### "Mobile wireless communications settings" of the CP

You configure the following information in the parameter group "Mobile wireless communications settings" of the CP:

- Address of the TeleService server  
IP address or name of the telecontrol server that can be resolved by DNS or of the TeleService gateway
- Port  
Port number of the telecontrol server or the TeleService gateway

### Global Security settings of the project

1. Open the following page in the project tree:

Global security settings > User management

2. Role

Open the "Roles" tab

The two tables "Roles" and "Rights of the role" become visible.

If necessary open the "Roles view" if this is hidden by the "Rights of the role" table.

In the "Roles" table (at the top) create a new user-defined role for TeleService.

3. In the "User" tab create a user that will later be allowed to execute the TeleService functions for the CP.

Configure the following parameters:

- User name

Assign the name of the user that will have TeleService rights.

You require the user name at the start of a TeleService session.

- Authentication method

Select the authentication method "Password" for this user.

- Password

Assign the password.

You require the password at the start of a TeleService session.

Note:

You specify the password properties of the security functions in the "Password policies" tab.

You enter the password on the engineering station when starting a TeleService session.

- Maximum time of the session

The time that can be configured here is only required for access to SCALANCE S modules. If the user is set up only for TeleService sessions, you can leave the default value unchanged.

4. Click on the "Roles" tab.
5. Select the CP in the lower list "Rights of the role" under the "Module rights" group.
6. The available rights are displayed in the "List of rights" table.  
The right "Use TeleService" is displayed.
7. Enable the "Use TeleService" right for the module.
8. Following this, set the S7 protocol to "allow" in Firewall.

## 4.5 Configuring data points and messages

### Data point-related communication with the CPU

No program blocks need to be programmed for the CP to transfer user data between the station and communications partner. The data areas in the memory of the CPU intended for communication with the partner are configured data point-related on the CP. Each data point is linked to a PLC tag or a data block on the CPU.

### Requirement: Created PLC tags and/or data blocks (DBs)

PLC tags or DBs must first be created in the CPU program to allow configuration of the data points.

The PLC tags for data point configuration can be created in the standard tag table or in a user-defined tag table. All PLC tags intended to be used for data point configuration must have the attribute "Visible in HMI".

Address areas of the PLC tags are input, output or bit memory areas on the CPU.

---

#### Note

##### Number of PLC tags

Remember the maximum possible number of PLC tags that can be used for data point configuration in the section Performance data and configuration limits (Page 17).

---

The formats and S7 data types of the PLC tags that are compatible with the protocol-specific data point types of the CP can be found in the section Datapoint types (Page 48).

### Access to the memory areas of the CPU

The values of the PLC tags or DBs referenced by the data points are read and transferred to the communications partner by the CP.

Data received from the communications partner is written by the CP to the CPU via the PLC tags or DBs.

### Configuring the data points and messages in STEP 7

You configure the data points in STEP 7 in the editor for the data point and message configuration. You can find this using the project tree:

Project > directory of the relevant station > Local modules > CP 1200

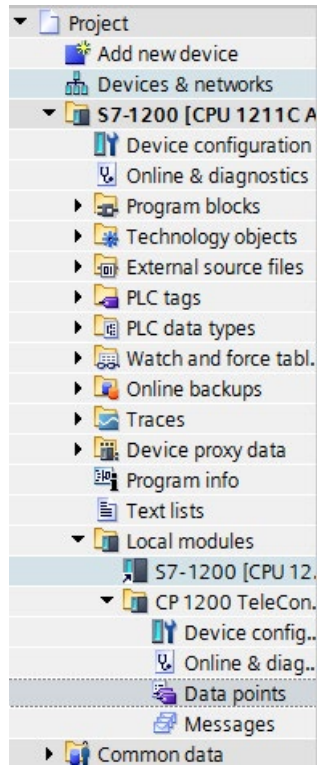


Figure 4-1 Configuring data points and messages

You will find more information on configuration in the following sections and in the STEP 7 information system.

## 4.6 Datapoint types

During the configuration of the user data to be transferred by the CP, each data point is assigned a protocol-specific data point type. The data point types supported by the CP along with the compatible S7 data types are listed below. They are grouped according to format (memory requirements).



## Supported data point types of the CP

Table 4- 1 Supported data point types and compatible S7 data types

| Format (memory requirements)                     | Data point type | S7 data types       | Address area |
|--|-----------------|---------------------|--------------|
| <b>Bit</b>                                       | Digital input   | BOOL                | I, Q, M, DB  |
|  | Digital output  | BOOL                | I, Q, M, DB  |
| <b>Byte</b>                                      | Digital input   | BYTE, CHAR          | I, Q, M, DB  |
|  | Digital output  | BYTE, CHAR          | I, Q, M, DB  |
| <b>Integer with sign (16 bits)</b>               | Analog input    | INT                 | I, Q, M, DB  |
|  | Analog output   | INT                 | I, Q, M, DB  |
| <b>Counter (16 bits)</b>                         | Counter input   | WORD                | I, Q, M, DB  |
| <b>Integer with sign (32 bits)</b>               | Analog input    | DINT                | I, Q, M, DB  |
|  | Analog output   | DINT                | I, Q, M, DB  |
| <b>Counter (32 bits)</b>                         | Counter input   | DWORD, UDINT        | I, Q, M, DB  |
| <b>Floating-point number with sign (32 bits)</b> | Analog input    | REAL                | Q, M, DB     |
|  | Analog output   | REAL                | Q, M, DB     |
| <b>Floating-point number with sign (64 bits)</b> | Analog input    | LREAL               | Q, M, DB     |
|  | Analog output   | LREAL               | Q, M, DB     |
| <b>Block of data (1 .. 64 bytes)</b>             | Data            | ARRAY <sup>1)</sup> | DB           |
|  | Data            | ARRAY <sup>1)</sup> | DB           |

<sup>1)</sup> For the possible formats of the ARRAY data type, refer to the following section.

### Block of data (ARRAY)

With the ARRAY data type, contiguous memory areas up to a size of 64 bytes can be transferred.

Compatible components of ARRAY are the following uniform S7 data types with a size between 1 and 32 bytes:

- BYTE, CHAR (in total up to 64 times per block of data)
- INT (in total up to 32 times per block of data)
- DINT, UDINT (in total up to 16 times per block of data)

If the array is modified later, the data point must be recreated.

### Time stamp in UTC format

Time stamps are transferred in UTC format (48 bits) and contain the time difference in milliseconds since 01.01.1970.

## 4.7 CPU scan cycle

### Priority in the scan cycle

The cyclic updating of the values of input data points of the CP by reading the current values of the assigned PLC tags on the CPU can be prioritized.

Less important input data points do not need to be read in every CPU scan cycle. Important input data points, on the other hand, can be prioritized for updating in every CPU scan cycle.

You can prioritize the data points in STEP 7 in the data point configuration in the "General" tab with the "Priority in the scan cycle" parameter. There you will find the two following options for input data points:

- High priority
- Low priority

The data points are read according to the method described below.

### Structure of the CPU scan cycle

The cycle (including the pause) with which the CP scans the memory area of the CPU is made up of the following phases:

- **High-priority read jobs**

The values of input data points with the scan priority "High-priority" are read in every scan cycle.

- **Low priority read jobs**

Some of the values of input data points with the scan priority "Low-priority" are read in every scan cycle.

The number of values read per cycle is specified for the CP in the "Communication with the CPU" parameter group with the "Max. number of read jobs" parameter. The values that exceed this value and can therefore not be read in one cycle are then read in the next or one of the following cycles.

- **Write jobs**

In every cycle, the values of a certain number of unsolicited write jobs are written to the CPU. The number of values written per cycle is specified for the CP in the "Communication with the CPU" parameter group with the "Max. number of write jobs" parameter. The values whose number exceeds this value are then written in the next or one of the following cycles.

- **Cycle pause time**

This is the waiting time between two scan cycles. It is used to reserve adequate time for other processes that access the CPU via the backplane bus of the station.

### Duration of the CPU scan cycle

Since no fixed time can be configured for the cycle and since the individual phases cannot be assigned a fixed number of objects, the duration of the scan cycle is variable and can change dynamically.

## 4.8 Process image, type of transmission, event classes, triggers

### The image memory, the process image of the CP

The image memory is the process image of the CP. All the current values of the configured data points are stored in the image memory. New values of a data point overwrite the last stored value in the image memory.

The values are sent after querying the communications partner, see "Transfer after call" in the section "Types of transmission" below.

### The send buffer (frame memory)

The send buffer of the CP is the memory for the individual values of data points that are configured as an event. The maximum size of the send buffer can be found in the section Performance data and configuration limits (Page 17).

The configured number of events is divided equally among all configured and enabled communications partners. For information on the configuration, refer to the parameter "Frame memory size" in the section Communication with the CPU (Page 74).

If the connection to a communications partner is interrupted, the individual values of the events are stored in the RAM of the CP. When the connection returns, the buffered values are sent. The frame memory operates chronologically; in other words, the oldest frames are sent first (FIFO principle).

If a frame was transferred to the communications partner, the transferred values are deleted from the send buffer.

If frames cannot be transferred for a longer period of time and the send buffer is threatening to overflow, the response is as follows:

#### The forced image mode

If the send buffer reaches a fill level of 80%, the CP changes to the forced image mode. New values of events are no longer added to the send buffer but rather they overwrite older existing values in the image memory. When the connection to the communications partner returns, the CP changes back to the send buffer mode if the fill level of the send buffer has fallen below 50%.

### Configuration of data points as events

Data points are configured as a static value or as an event using the "Type of transmission" parameter (see below):

- **No event (static value)**

The values of data points that are not configured as an event ("Transfer after call") are entered in the image memory of the CP and transferred to the communications partner when it requests this value.

- **Event**

The values of data points configured as an event are entered in the image memory and also in the send buffer of the CP.

The values of events are saved in the following situations:

- The configured trigger conditions are fulfilled (data point configuration > "Trigger" tab, see below)
- The value of a status bit of the status identifiers changes.

### Status identifiers: Generating an event on a status change

With data points that are configured as an event, the change to the status bit leads to an event being generated, refer also to the section Status IDs of data points (Page 54).

Example: When the value of a data point configured as an event is updated during startup of the station by reading the CPU data for the first time, the status "RESTART" of this data point changes (bit status change 1 → 0). This leads to generation of an event.

### Type of transmission / event classes

The following types of transmission are available:

- **Transfer after call**

The current value of the data point is entered in the image memory of the CP. New values of a data point overwrite the last stored value in the image memory.

The current value at the time is transferred only after being called by the communications partner.

- **Every value triggered**

The data point is configured as an event.

Each value change is entered in the send buffer in chronological order.

- **Current value triggered**

The data point is configured as an event.

Only the last current value is entered in the send buffer. It overwrites the value stored there previously.

## Trigger

Various trigger types are available for starting event-driven transfer:

- **Threshold value trigger**

The value of the data point is transferred when this reaches a certain threshold. The threshold is calculated as the difference compared with the last stored value, refer to the section Threshold value trigger (Page 78).

- **Time trigger**

The value of the data point is transferred at configurable intervals or at a specific time of day.

- **Event trigger**

The value of the data point is transferred when a configurable trigger signal is fired. For the trigger signal, the edge change (0 → 1) of a trigger tag is evaluated that is set by the user program. When necessary, a separate trigger tag can be configured for each data point.

**Resetting the trigger tag in the bit memory area / DB:**

If the memory area of the trigger tag is in the bit memory or in a data block, the trigger tag is reset to zero when the data point value is transferred.

You specify whether the value of a data point is transferred to the communications partner immediately after the trigger fires or after a delay in the "Transmission mode" parameter.

## Transmission mode

The transmission mode of a frame is set in the "Trigger" tab of the data point. With the two options, you specify whether frames of events are sent immediately or following a delay:

- **Unsolicited**

The value is transferred immediately.

- **Conditional spontaneous**

The value is transferred only when one of the two following conditions is fulfilled:

- The communications partner queries the station.
- The value of another event with the transmission mode "Unsolicited" is transferred.

## 4.9 Status IDs of data points

### Status IDs of data points

The status identifiers of the data points listed in the following tables are transferred along with the value in each frame to the communications partner. They can be evaluated by the communications partner.

The status identifiers are transferred in 2 bytes. Byte 1 is not used.

The meaning relates to the bit status in the last row of each table.

Table 4- 2 Byte assignment of the status byte for data points

| Bit        | 7                 | 6   | 5                | 4                      | 3   | 2                                  | 1                             | 0                |
|------------|-------------------|---|------------------|------------------------|---|------------------------------------|-------------------------------|------------------|
| Flag name  | -                 | NON_ EXISTENT                                       | SB Substituted   | LOCAL_ FORCED          | CY CARRY  | OVER_ RANGE                        | RESTART                       | ONLINE           |
| Meaning    | -                 | Data point does not exist or S7 address unreachable | Substitute value | Local operator control | Counted value overflow before reading the value | Analog value: Value range exceeded | Value not updated after start | Value is invalid |
| Bit status | <i>(always 0)</i> | 1   | 1                | 1                      | 1   | 1                                  | 1                             | 1                |

## 4.10 Connection establishment

### Connection establishment

- Connection to the telecontrol server

The connection to the telecontrol server is always established by the CP.

If a connection established by the CP is interrupted, the CP automatically attempts to re-establish the connection. Note the settings for re-establishing the connection in STEP 7, refer to the section Ethernet interface (X1) (Page 67).

---

#### Note

##### Connection interrupted by the mobile wireless network provider

When using mobile wireless services, remember that existing connections can be interrupted by mobile wireless network providers for maintenance purposes.

---

- Connections with direct communication (Open User Communication) and S7 communication

Connections are established as soon as the corresponding program blocks are called on the CPU.

This also applies to the situation when a different S7 station sends data. In this case, the corresponding receive blocks are called by the receiving station.

## 4.11 Acknowledgment

### Acknowledgment of frames

The receipt of a frame is monitored and acknowledged in different ways. The mechanisms differ depending on the type of communication:

- **Telecontrol communication**

Frames received from TCSB are acknowledged immediately by the CP.

Frames sent by the CP are acknowledged by TCSB.

- **Inter-station communication**

Received frames are acknowledged immediately by the CP. The acknowledgment frame is forwarded by the telecontrol server to the destination CP.

For sent frames, this applies in the opposite direction.

- **Direct communication (Open User Communication)**

The successful sending and receipt of frames is indicated by status displays of the program blocks.

With TCP segments, the protocol-specific acknowledgement mechanisms are used.

## 4.12 Calling a TeleService connection

### Requirement for the engineering station and the STEP 7 project

- The STEP 7 project with the CP is stored on the engineering station.
- The required configuration steps have been performed, see section Configuration of the TeleService access (Page 45).

### Requirement for connection establishment

The request for connection establishment is triggered by the engineering station. The connection is established by the CP.

With TeleService via the mobile wireless network, a switching station is required between the remote station and engineering Station, see section Requirements for operation (Page 19).

This switching station can be a telecontrol server or, if there is no telecontrol server in the configuration, a TeleService gateway.

For documentation of the two systems, refer to Documentation references (Page 129).

### Settings for establishing a TeleService connection

In the dialog "Establish mobile wireless remote connection", enter the previously configured data under the following headings:

- **Telecontrol server / TeleService gateway...**
- Selection whether the TeleService switching station is located on the PC of the engineering station or in the network or can be reached via the Internet.
  - In the latter case, enter the address of the TeleService server.

IP address or name and port number of the telecontrol server that can be resolved by DNS or of the TeleService gateway
  - Server password

If the option is enabled and the server password is configured in TCSB, enter the password to authenticate the CP with the telecontrol server.

The server password is not required for TeleService via a TeleService gateway.
- **Authentication ...**
  - User name and password
  - Here, enter the data for the TeleService user that you configured in STEP 7 in the global Security settings, see also section Configuration of the TeleService access (Page 45).

### Requirements in the security configuration of the CP

For the remote station, TeleService can only be used if the engineering station (with CP 1628 or via SCALANCE S) and the CP are configured in a common VPN group.

For TeleService, you need to enable the option "Allow S7 protocol" in the IP rules of the firewall configuration.

### Procedure for connection establishment for TeleService

---

#### Note

#### No TeleService connection establishment using "Online" > "Go online"

If you attempt to establish a TeleService connection by selecting the CPU and then selecting the menu or shortcut menu command "Online" > "Connect online", STEP 7 will automatically attempt to connect via Ethernet. Reason: In STEP 7, the last connection path used to download the project data is stored.

---

#### Note

#### TeleService to 1 station only from 1 TIA Portal instance

You can operate TeleService with an S7 station only from 1 engineering station (1 TIA Portal instance; 1 STEP 7 project). TeleService by more than one engineering station at the same time with 1 station is not possible.

---



**Note**


**Canceling a TeleService connection when calling online dialogs**

An existing TeleService connection is canceled when you attempt to access an additional station or a node.

When there is an existing TeleService connection, do not select any of the menu commands "Go online", "Online & Diagnostics", "Load to device", "Extended download to device" or "Accessible nodes".

---

Follow the steps below to establish a TeleService connection to the remote station via the mobile wireless network from the engineering station:

1. Select the CPU of the remote station in the STEP 7 project.
2. Select the "Online" > "Online & Diagnostics" menu.  
The "Online access" dialog opens.
3. Choose the entry "TeleService via mobile wireless" in the "Type of interface" drop-down list.
4. Choose the entry "Mobile wireless TeleService board" in the "PG/PC interface" drop-down list.
5. Click on the  icon next to the "PG/PC interface" drop-down list.  
The "Establish remote connection" dialog box opens.
6. Make the necessary entries in this dialog.  
You will find information on the necessary entries in the tooltips of the STEP 7 online help.

**Terminating a TeleService connection**

On completion of the TeleService session, terminate the TeleService connection again using the "Go offline" button. The connection is terminated after approximately 5 minutes.

**User data connections and TeleService**

Connections between a CP and telecontrol server for transferring user data are not interrupted by a TeleService connection.

## 4.13 Security functions

Note the range and application of the security functions of the CP, refer to the section Other services and properties (Page 14).

### 4.13.1 VPN

#### 4.13.1.1 VPN (Virtual Private Network)

##### VPN tunnel

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 features of the VPN tunnel is that it forwards all frames even from protocols of higher layers (HTTP, FTP telecontrol protocols of the application layer etc.).

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 or intermediate 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 frames and therefore operates independent of the rest of this network.
- VPN allows communication of the VPN partners in the subnet with the assigned network.
- VPN is based on tunnel technology and can be individually configured.
- 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 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/PG to automation devices or networks protected by security modules via public networks.

## Cell protection concept

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

- Access to individual devices and network segments 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

### 4.13.1.2 Addressing the CP when using VPN

#### IP addresses and VPN ports

In normal mobile wireless networks it is not possible to reach a dynamic IP address assigned to the CP by the mobile wireless network provider from the Internet. For this reason, for incoming connections make sure that the CP is assigned a fixed public IP address by the mobile wireless network provider.

You must also make sure that apart from this IP address, the ports required for VPN are reachable from the Internet.

### 4.13.1.3 Creating a VPN tunnel for S7 communication between stations

#### Requirements

To allow a VPN tunnel to be created for S7 communication between two S7 stations or between an S7 station and an engineering station with a security CP (for example CP 1628), the following requirements must be met:

- The two stations have been configured.
- The CPs in both stations must support the security functions.
- The Ethernet interfaces of the two stations are located in the same subnet.
- All receiving stations require a fixed IP address to be reachable via the public networks. For this, a special mobile wireless contract is normally necessary for the mobile wireless CP.

---

#### Note

##### Communication also possible via an IP router

Communication between the two 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. Creating 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. Creating the VPN group and assigning security modules
4. Configure the properties of the VPN group
5. Configure local VPN properties of the two CPs

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

### Creating a security user

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

1. In the local security settings of the CP, click the "User login" button.
  - Result: A new window opens.
2. Enter the user name, password and confirmation of the password.
3. Click the "Logon" button.

You have created a new security user. The security functions are now available to you.

With all further logons, log on as user.

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

After logging on, you need to select the "Activate security features" check box in the configuration of both CPs.

You now have the security functions available for both CPs.

### Creating the VPN group and assigning security modules

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.

**Note****Current date and current time on the CP for VPN connections**

Normally, to establish a VPN connection and the associated recognition of the certificates to be exchanged, the current date and the current time are required on both stations.

The establishment of a VPN connection to an engineering station that is also the telecontrol server at the same time (TCSB installed), runs as follows along with the time of day synchronization of the CP:

On the engineering station (with TCSB), you want the CP to establish a VPN connection. The VPN connection is established even if the CP does not yet have the current time. Otherwise the certificates used are evaluated as valid and the secure communication will work.

Following connection establishment, the CP synchronizes its time of day with the PC because the telecontrol server is the time master if telecontrol communication is enabled.

---

**Configure the properties of the VPN group**

1. Double-click on the newly created VPN group.

Result: The properties of the VPN group are displayed under "Authentication".

2. Enter a name for the VPN group. Configure the settings of the VPN group in the properties.

These properties define the default settings of the VPN group that you can change at any time.

---

**Note****Specifying the VPN properties of the CPs**

You specify the VPN properties of the CPs in the "Security" > "Firewall" > "VPN" parameter group of the relevant module.

---

**Result**

You have created a VPN tunnel. The firewalls of the CPs are activated automatically: The "Activate firewall" check box is selected as default when you create a VPN group. You cannot deselect the check box.

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

#### 4.13.1.4 VPN communication with SOFTNET Security Client (engineering station)

Setting up VPN tunnel communication between the SOFTNET Security Client and CP has essentially same requirements and procedure as described in the section Creating a VPN tunnel for S7 communication between stations (Page 59).

##### 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. Disable the option "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. Select "Delete Entry" in the shortcut menu.

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

#### 4.13.1.5 Connection to the telecontrol server

##### No VPN connection between CP and TCSB

For secure communication via a VPN tunnel, the communications partners are assigned to a common VPN group. The configuration of a VPN connection between CP and TCSB is not possible because the telecontrol server cannot be configured in STEP 7.

Thanks to the encrypted telecontrol protocol, the connection between the CP and telecontrol server is already protected.

### 4.13.1.6 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 "VPN" tab.
4. For each VPN connection with the CP as a passive VPN subscriber, change the default setting "Initiator/Responder" to the setting "Responder".

## 4.13.2 Firewall

### 4.13.2.1 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 will not be checked by the IP firewall (layer 3). This means that with suitable MAC firewall rules, IP communication can be restricted or blocked.

### 4.13.2.2 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.

### 4.13.2.3 Firewall settings for S7 connections via a VPN tunnel

#### IP rules in advanced firewall mode

If you set up S7 connections with a VPN tunnel between the CP and a communications partner, you will need to adapt the local firewall settings of the CP:

Select the "Allow\*" action for S7 connections in advanced firewall mode ("Security > Firewall > IP rules") for both communications directions of the VPN tunnel.

### 4.13.3 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.

## 4.14 Time-of-day synchronization

### Procedure for time-of-day synchronization

With applications that require time-of-day synchronization (e.g. telecontrol), you need to synchronize the time of day of the CP regularly. If you do not synchronize the time of day of the CP regularly, there may be deviations of several seconds per day in the time information of the CP.

The CP supports the two methods of time-of-day synchronization:

- **Time from partner**

The time of the CP is synchronized by a telecontrol server.

Only with communication type "Telecontrol" activated.

- **NTP / NTP (secure)**

Only with communication type "Telecontrol" deactivated.

The method NTP (secure) can only be selected if the security functions are enabled.

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.



## Configuration

Depending on the configured communication types and security functions, time-of-day synchronization is configured differently:

- Telecontrol communication enabled

With telecontrol communication enabled, the time of day of the CP is synchronized automatically by the TCSB computer.

- Security functions enabled:

The time-of-day synchronization is configured in the "Security" parameter group.

- Telecontrol communication not enabled

The time of day of the CP can only be synchronized with NTP mechanisms:

- Security functions enabled:

The time-of-day synchronization is configured in the "Security" parameter group. NTP and NTP (secure) are available as the synchronization methods.

- Security functions not enabled:

The time-of-day synchronization is configured in the "Ethernet interface > Time synchronization" parameter group. Only NTP is available as the synchronization method.

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

### **NTP (secure) with security functions enabled**

If you use Security functions, a valid time of day is extremely important. It is recommended to use the NTP (secure) method.

The secure method NTP (secure) uses authentication with symmetrical keys according to the hash algorithms MD5 or SHA-1.

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

### **"Accept time from non-synchronized NTP servers" option**

If the option is enabled, the CP also accepts the time-of-day from non-synchronized NTP servers with stratum 16.

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

### **Time-of-day synchronization of the CPU**

In the parameter group "Communication with the CPU", you can set whether or not the current time of day of the CP will be made available to the CPU via a PLC tag.

## 4.15 STEP 7 configuration of individual parameters

Below, you will find information on the configuration of individual functions grouped according to parameter groups in STEP 7.

---

### Note

#### Information in STEP 7 and in the manual

If there are discrepancies between the following descriptions and the information in STEP 7 / Professional V13, the information in this document is valid.

---

### 4.15.1 Communication types

In this parameter group, you enable the communication type of the CP.

To minimize the risk of unauthorized access to the station via mobile wireless, you need to enable the communications services that the CP will execute individually. You can enable all options but at least one option should be enabled.

#### "Communication types" parameter group

- **Enable telecontrol communication**

Enables communication with a Telecontrol server on the CP.

Note:

To enable telecontrol communication, the Security functions must also be enabled.

- **Activate online functions**

Enables access to the CPU for the online functions via the CP (diagnostics, loading project data etc.). If the function is enabled, the engineering station can access the CPU via the CP.

If the option is disabled, you have no access to the CPU via the CP with the online functions. Online diagnostics of the CPU with a direct connection to the interface of the CPU however remains possible.

- **Enabling S7 communication**

Enables the functions of S7 communication with a SIMATIC S7 on the CP.

If you configure S7 connections to the relevant station, and these run via the CP, you will need to enable this option on the CP.

Open User Communication does not need to be enabled since you then need to create the relevant program blocks. Unintended access to the CP is therefore not possible.

## 4.15.2 Mobile wireless communications settings

### "Services and settings" parameter group

In this parameter group, you configure the phone number of the CP, the PIN and the SMSC.

You continue to enable the required mobile wireless services. You can enable individual mobile wireless services or all of them. If you do not enable a mobile wireless service, the CP behaves as if all mobile wireless services were enabled and the choice of the mobile wireless service used is made based on the data on the SIM card.

### "APN settings" parameter group

In this parameter group, you configure the APN data.

### "List of preferred networks" parameter group

In this parameter group, you specify the dial-in behavior of the CP into various mobile wireless networks.

### "Teleservice settings" parameter group

In this parameter group, you specify the connection parameters for the TeleService server(s).

## 4.15.3 Ethernet interface (X1)

### The Ethernet interface

The CP does not have a physical Ethernet interface.

In STEP 7, the Ethernet interface is used as a placeholder for the configuration of various address and monitoring parameters.

### Ethernet interface (X1) > Ethernet addresses > IP protocol

Enter you configure IP address of the CP.

- **Dynamic IP address**

Enable this option if the CP is assigned the IP address dynamically by the network provider.

- **Fixed IP address from the mobile wireless network provider**

Enable this option if you have a mobile wireless contract with which the network provider assigns the CP a fixed IP address.

This is necessary when using S7 communication and Open User Communication.

## Ethernet interface (X1) > Advanced options > TCP connection monitoring

The settings made here apply globally to all configured TCP connections of the CP. If telecontrol communication is enabled, this is the connection to the telecontrol server.

Note the option of overwriting the general value configured here for individual communications partners, refer to the section Partner stations (Page 70).

(Note: The settings made here do not apply to connections programmed for Open User Communication with the program blocks.)

### TCP connection monitoring time

Function: If there is no data traffic within the connection monitoring time, the CP sends a keepalive to the communications partner.

The monitoring time is configured for the Ethernet interface as the default for all TCP connections. The default value can be adapted individually for each connection in "Partner stations".

### TCP keepalive monitoring time

After sending a keepalive, the CP expects a reply from the communications partner within the keepalive monitoring time. If the CP does not receive a reply within the configured time, it terminates the connection.

The monitoring time is configured for the Ethernet interface as the default for all TCP connections. The default value can be adapted individually for each connection in "Partner stations".

## Ethernet interface(X1) > Advanced options > Transfer settings

### Reconnection delay

The settings made here apply to the connection to the telecontrol server.

The reconnection delay is the waiting time between repeated attempts to establish the connection by the CP when the telecontrol server is not reachable or the connection has aborted.

This waiting time avoids continuous connection establishment attempts at short intervals if there are connection problems.

A basic value is configured for the waiting time before the next connection establishment attempt. Starting at the basic value, the current waiting time is doubled after every 3 unsuccessful retries up to a maximum value of 900 s.

Range of values for the basic value: 10 to 600 s.

Example: The basic value 20 results in the following intervals (waiting times) between the attempts to re-establish a connection:

- three times 20 s
- three times 40 s
- three times 80 s
- etc. up to max. 900 s

---

**Note**

If the partner cannot be reached, connection establishment via the mobile wireless network can take several minutes. This may depend on the particular network and current network load.

Depending on your contract, costs may result from each connection establishment attempt.

---

**Send timeout**

Time for the arrival of the acknowledgment from the telecontrol server after sending unsolicited frames. The time is started after sending an unsolicited frame. If no acknowledgement has been received from the partner when the connection monitoring time elapses, the frame is repeated up to three times. After three unsuccessful attempts, the connection is terminated and re-established.

**Watchdog cycle**

Interval at which a watchdog frame is sent to the telecontrol server if there is no productive data exchange.

**Watchdog monitoring time**

After sending a watchdog frame, an answer is expected from the Telecontrol server within the watchdog monitoring time (timeout). If the CP does not receive a reply from the Telecontrol server within the monitoring time, it terminates and re-establishes the connection.

**Key exchange interval**

Here, you enter the interval in hours after which the key is exchanged again between the CP and the telecontrol server. The key is a security function of the telecontrol protocol used by the CP and TCSB V3.

## 4.15.4 Partner stations

### 4.15.4.1 Partner stations > Telecontrol server

#### Partner stations > "Telecontrol server"

- **Partner number**

The partner number for the telecontrol server is assigned automatically by the system if telecontrol communication is enabled.
- **Station address**

The station address of the telecontrol server is assigned automatically by the system if telecontrol communication is enabled.

#### Partner stations > "Telecontrol server > "Connection to partner"

- **Partner IP address**

IP address of the telecontrol server

If the CP is connected to a TCSB redundancy group (TCSB V3), here configure the public IP address of the DSL router via which the telecontrol server can be reached from the Internet. Set the port forwarding on the DSL router so that the public IP address (external network) is led to the virtual IP address of the TCSB server PCs (internal network). The station does not therefore receive any information telling it which of the two computers of the redundancy group it is connected to.
- **Connection monitoring**

When the function is enabled, the connection to the communications partner (telecontrol server) is monitored by sending keepalive frames.

The TCP connection monitoring time is set for all TCP connections of the CP in the parameter group of the Ethernet interface. The setting applies to all TCP connections of the CP.

Here in the parameter group "Partner stations > Telecontrol server", the globally set TCP connection monitoring time can be set separately for the telecontrol server. The value set here overwrites the global value for the telecontrol server that was set in the "Ethernet interface (X1) > Advanced options > TCP connection monitoring" parameter group.

- **TCP connection monitoring time**

The monitoring time is specified at a higher level for the Ethernet interface as the default for all configured TCP connections, see also section Ethernet interface (X1) (Page 67).

The default value for the Ethernet interface can be adapted for the connection to the telecontrol server individually in the "Partner stations" parameter group. If the monitoring time in the "Partner stations" parameter group has a different value from the monitoring time in the Ethernet interface parameter group, the monitoring time of the "Partner stations" parameter group is used.

Function: If there is no data traffic within the connection monitoring time, the CP sends a keepalive to the telecontrol server.

Permitted range: 0 to 65535 s. Default: 180 s.

If you enter 0 (zero), the function is disabled.

- **TCP keepalive monitoring time**

If the value configured here differs from the value configured in the Ethernet interface parameter group, the monitoring time of the "Partner stations" parameter group is used.

After sending a keepalive, the CP expects a reply from the communications partner within the keepalive monitoring time. If the CP does not receive a reply within the configured time, it terminates the connection. Permitted range: 0 to 65535 s. Default: 1 s. If you enter 0 (zero), the function is deactivated. The monitoring time is configured for the Ethernet interface as the default for all TCP connections. The default value can be adapted individually for each connection in "Partner stations".

- **Connection establishment**

Specifies the communications partner that establishes the connection (always the CP).

- **Partner port**

Number of the listener port of the telecontrol server.

## Partner stations > "Telecontrol server" > "Advanced settings"

- **Report partner status**

If the "Report partner status" function is enabled, the CP signals the status of the communication to the remote partner.

- Bit 0 of "PLC tag for partner status" (data type WORD) is set to 1 if the partner can be reached.
- Bit 1 is set to 1 if all the paths to the remote partner are OK (useful with redundant paths).
- Bits 2-3 indicate the status of the send buffer (frame memory).  
The following values are possible:
  - 0: send buffer OK
  - 1: send buffer threatening to overflow (more than 80 % full).
  - 3: send buffer has overflowed (fill level 100 % reached).

As soon as the fill level drops below 50%, bits 2 and 3 are reset to 0.

Bits 4 to 15 of the PLC tags are not used and do not need to be evaluated in the program.

### 4.15.4.2 Partner for inter-station communication

#### Inter-station communication

In this table, you specify the communications partners of the CP for inter-station communication. The communications partner is a CP in the partner S7 station.

Connections for inter-station communication run via the telecontrol server.

Note the special features when configuring the data points for inter-station communication in the section Partner stations: Configuring the inter-station communication (Page 85).

#### Partner

The partner number is assigned by the system. It is required during data point configuration to assign data points to their communications partners.

You specify the partner CP for inter-station communication with the parameters "Project", "Station" and "Slot".

#### Project

Here, enter the project number of the CP in the partner station.

You will find the parameter in the parameter group "Security > CP identification" on the partner CP.

#### Station number

Here, enter the station number of the CP in the partner station.

You will find the parameter in the parameter group "Security > CP identification" on the partner CP.



## Slot

Here, enter the slot number of the CP in the partner station.

You will find the parameter in the parameter group "General" on the partner CP.

## Send buffer

When enabled, the frames are stored in the send buffer (frame memory) of the CP if the connection is disturbed. Note that the capacity of the frame memory is shared by all communications partners.

If the option is disabled, even frames for events are only stored in the image memory of the CP; in other words if there are problems on the connection older values are overwritten by new values.

## Access ID

The access ID of the partner CP is displayed here.

The Access ID (DWORD) is formed from the hexadecimal values of project number, station number and slot:

Bits 0 to 7: Slot

Bits 8 to 20: Station number

Bits 21 to 31: Project number

## 4.15.5 Communication with the CPU

The parameter group is displayed as soon as telecontrol communication is enabled.

### Communication with the CPU

- **Frame memory size**

Here, you set the size of the send buffer for events.

A maximum of 64000 events divided up equally among the communications partners can be buffered.

You will find a description of the send buffer and the functions involved in the section Process image, type of transmission, event classes, triggers (Page 51).

### CP diagnostics

In the parameter group "CP diagnostics", you have the option of reading out advanced diagnostics data from the CP using PLC tags.

- **Diagnostics trigger tag**

If you want to use advanced CP diagnostics, you need to configure the "Diagnostics trigger tag".

If the user program of the CPU sets the PLC tag "Diagnostics trigger tag" (BOOL) to 1, the CP updates the values of the configured PLC tags for advanced diagnostics. After writing the current values to the PLC tags for advanced diagnostics, the CP sets the "Diagnostics trigger tag" to 0 signaling the CPU that the updated values can be read from the PLC tags.

Reading out the following diagnostics data can be enabled selectively:

- **Send buffer overflow**

PLC tag (data type byte) for the send buffer overflow pre-warning. Bit 0 is set to 1 when 80% of the fill level of the send buffer is reached.

- **Send buffer level**

PLC tag (data type DWord) for the occupation of the send buffer. The number of saved frames is displayed.

- **Current IP address**

PLC tag (data type String) for the current IP address of the CP.

- **Mobile wireless signal quality (LED)**

PLC tag (data type UInt) for the signal quality of the local mobile wireless network as this is displayed by the "SIGNAL QUALITY" LED.

- **Mobile wireless signal quality (dBm)**

PLC tag (data type INT) for the signal quality of the local mobile wireless network as a dBm value.

- **'NETWORK' LED**  
PLC tag (data type UInt) for the status of the connection for the data service in the mobile wireless network.
- **Date of last successful logon to network**  
PLC tag (data type DTL) for the date on which the CP last logged in to the mobile wireless network.
- **Date of last unsuccessful logon to network**  
PLC tag (data type DTL) for the date on which the CP was last unable to log in to the mobile wireless network.
- **Date of last successful logon to TCSB**  
PLC tag (data type DTL) for the date on which the CP last logged in to the telecontrol server.
- **Date of last unsuccessful logon to TCSB**  
PLC tag (data type DTL) for the date on which the CP was last unable to log in to the telecontrol server.

## 4.15.6 E-mail configuration

### Configuring e-mails in STEP 7

In the "E-mail configuration" entry, you configure the protocol to be used and the data for access to the e-mail server in STEP 7.

In the message editor ("Messages" entry in STEP 7), you configure the individual e-mails, see section Messages (Page 86).

### E-mail configuration

With the default setting of the SMTP port 25, the CP transfers unencrypted e-mails.

If your e-mail service provider only supports encrypted transfer, use one of the following options:

- Port no. 587  
By using STARTTLS, the CP sends encrypted e-mails to the SMTP server of your e-mail service provider.  
Recommendation: If your e-mail provider offers both options (STARTTLS / SSL/TLS), you should use STARTTLS with port 587.
- Port no. 465  
By using SSL/TLS (SMTPS), the CP sends encrypted e-mails to the SMTP server of your e-mail service provider.

Ask your e-mail service provider which option is supported.

### Importing the certificate with encrypted transfer

To be able to use encrypted transfer, you need to load the certificate of your e-mail account in the certificate manager of STEP 7. You obtain the certificate from your e-mail service provider.

To import the certificate, follow these steps:

1. Save the certificate from your e-mail service provider in the file system of the engineering station.
2. In STEP 7, select the entry "Global security settings > Certificate manager" in the "Project tree".
3. Change to the "Trusted certificates and root certification authorities" tab.
4. Select any row in the table "Trusted certificates and root certification authorities".
5. Select the "Import" entry in the shortcut menu.
6. In the dialog that follows, select the required certificate.

## 4.15.7 Data point configuration

### 4.15.7.1 Data point name and data point index

#### Character set for data point names

When a data point is created, the name of the PLC tag is initially adopted. In the "General" tab of the data point you can change the name of the data point.

When assigning the name, only the following ASCII characters can be used: ASCII characters 0x20 ... 0x7e with the exception of the characters listed below.

The following characters are forbidden since they do not adhere to the syntax rules of TCSB for OPC items:

- 0x27 (apostrophe)
- 0x2e (period)
- 0x2f (slash)
- 0x5b and 0x5d (square brackets)
- 0x5c (backslash)
- 0x7c (pipe)

### Configuration of the data point index

Within a CP, the indexes of the data point classes must comply with the following rules:

- Input

The index of a data point of the type input must be unique throughout all data point types (digital inputs, analog inputs etc.).
- Output
  - A data point of the type output can have the same index as a data point of the type input.
  - Several data points of the type output can have the same index.

---

**Note****Data points for the inter-station communication with a CP in another S7 station**

Note that for inter-station communication, the indexes of the two corresponding data points (data point pair) must be identical for the sending and receiving CP, see also section Partner stations: Configuring the inter-station communication (Page 85).

---

#### 4.15.7.2 Threshold value trigger and Analog value preprocessing

##### Sequence of processing Threshold value trigger and Analog value preprocessing

---

**Note****Threshold value trigger: Calculation only after "Analog value preprocessing"**

Note that the analog value preprocessing is performed before the check for a configured threshold value.

This affects the value that is configured for the threshold value trigger, refer to the section Threshold value trigger (Page 78).

---

**Note****Restricted preprocessing and no Threshold value trigger if Mean value generation is configured**

If you configure mean value generation for an analog value event, the following preprocessing options are not available:

- Unipolar transfer
- Error suppression time
- Smoothing

If mean value generation is configured, no threshold value trigger can be configured for the analog value event involved.

---

#### 4.15 STEP 7 configuration of individual parameters

Analog inputs that are configured as an event are processed on the CP in the following sequence:

##### Sequence of analog value processing

1. Reading the data from the input area of the CPU
2. Analog value preprocessing (part 1)  
Processing involves the following steps:
  - Mean value generation
    - if configured: Calculation and then continue at point 4.
    - if not configured: Continue with "Unipolar transfer".
  - Unipolar transfer (if configured)
  - Error suppression time (if configured)
  - Smoothing (if configured)
3. Threshold value calculation (if Threshold value trigger is configured)
4. Analog value preprocessing (part 2)
  - Set limit value 'low' / Set limit value 'high' (if configured)
5. Storage of the value in the send buffer  
Transfer of the value to the partner if trigger and threshold value conditions are met.

#### 4.15.7.3 Threshold value trigger

The CP calculates the value for the threshold value trigger after the analog value preprocessing, refer to the section Analog value preprocessing (Page 79).

##### Threshold value trigger: How the integration calculation works

To calculate the threshold value trigger, the integration method is used.

In the integration threshold value calculation, it is not the absolute value of the deviation of the process value from the last stored value that is evaluated but rather the amount of the integrated deviation.

##### The calculation cycle

The integration threshold value calculation works with a cyclic comparison of the integrated current value with the last stored value. The calculation cycle in which the two values are compared is 500 milliseconds.

(Note: The calculation cycle must not be confused with the scan cycle of the CPU memory areas).

The deviations of the current process value are totaled in each calculation cycle. The trigger is set only when the totaled value reaches the configured value of the threshold value trigger and a new process value is entered in the send buffer.

The method is explained based on the following example in which a threshold value of 2.0 is configured.

Table 4- 3 Example of the integration calculation of a threshold value configured with 2.0

| Time [s]<br>(calculation cycle) | Process value<br>stored in the<br>send buffer | Current process<br>value | Absolute deviation<br>from the stored<br>value | Integrated<br>deviation |
|---------------------------------|---|--------------------------|--|-------------------------|
| 0                               | <b>20.0</b>                                   | <b>20.0</b>              | 0  | 0                       |
| 0.5                             |   | 20.3                     | +0.3   | 0.3                     |
| 1.0                             |   | 19.8                     | -0.2   | 0.1                     |
| 1.5                             |   | 20.2                     | +0.2   | 0.3                     |
| 2.0                             |   | 20.5                     | +0.5   | 0.8                     |
| 2.5                             |   | 20.3                     | +0.3   | 1.1                     |
| 3.0                             |   | 20.4                     | +0.4   | 1.5                     |
| 3.5                             | <b>20.5</b>                                   | <b>20.5</b>              | +0.5   | <b>2.0</b>              |
| 4.0                             |   | 20.4                     | -0.1   | -0.1                    |
| 4.5                             |   | 20.1                     | -0.4   | -0.5                    |
| 5.0                             |   | 19.9                     | -0.6   | -1.1                    |
| 5.5                             |   | 20.1                     | -0.4   | -1.5                    |
| 6.0                             | <b>19.9</b>                                   | <b>19.9</b>              | -0.6   | <b>-2.1</b>             |

In this example, a value of 2.0 was configured for the threshold value trigger.

With the changes in the process value shown in the example, the threshold value trigger fires twice, if the value 2.0 is reached:

- At the time 3.5 s: The value of the integrated deviation is at 2.0. The new process value stored in the send buffer is 20.5.
- At the time 6.0 s: The value of the integrated deviation is at 2.1. The new process value stored in the send buffer is 19.9.

In this example, if a deviation of the process value of approximately 0.5 should fire the trigger, then with the behavior of the process value shown here a threshold value of approximately 1.5 ... 2.5 would need to be configured.

#### 4.15.7.4 Analog value preprocessing

CPs with data point configuration support analog value preprocessing with some or all of the functions described below.

## Sequence of processing Threshold value trigger and Analog value preprocessing

---

### Note

#### Threshold value trigger: Calculation only after "Analog value preprocessing"

Note that the analog value preprocessing is performed before the check for a configured threshold value.

This affects the value that is configured for the threshold value trigger.

#### Restricted preprocessing options if mean value generation is configured

If you configure mean value generation for an analog value event, the following preprocessing options are not available:

- Unipolar transfer
- Fault suppression time
- Smoothing

#### No Threshold value trigger if Mean value generation is configured

If mean value generation is configured, no threshold value trigger can be configured for the analog value event involved.

---

Analog inputs that are configured as an event are processed on the CP in the following sequence:

### Sequence of analog value processing

1. Reading the data from the input area of the CPU
2. Analog value preprocessing (part 1)  
Processing involves the following steps:
  - Mean value generation
    - Mean value generation configured: Calculation and then continued at point 4.
    - No mean value generation configured: Continue with "Unipolar transfer".
  - Unipolar transfer (if configured)
  - Fault suppression time (if configured)
  - Smoothing (if configured)
3. Threshold value calculation (if Threshold value trigger is configured)
4. Analog value preprocessing (part 2)
  - Set limit value 'low' / Set limit value 'high' (if configured)
5. Storage of the value in the send buffer  
Transfer of the value to the partner if trigger and threshold value conditions are met.



## Unipolar transfer

With unipolar transfer, negative values are corrected to zero. This can be desirable if values from the underrange should not be transferred as real measured values.

Exception: The value -32768 / 8000<sub>h</sub> for wire break of live zero inputs is transferred.

Unipolar transfer cannot be configured at the same time as mean value generation.

## Mean value generation

With this parameter, acquired analog values are transferred as mean values.

The current values of an analog data point are acquired cyclically and totaled. The number of acquired values per time unit depends on the read cycle of the CPU and the CPU scan cycle of the CP. The mean value is calculated from the accumulated values as soon as the transfer is triggered by a time trigger. Following this, the accumulation starts again so that the next mean value can be calculated.

The mean value can also be calculated if the transmission of the analog value message is triggered by a request from the communications partner. The duration of the mean value calculation period is then the time from the last transmission (for example triggered by the trigger) to the time of the request. Once again, the accumulation restarts so that the next mean value can be calculated.

### Overflow range / underflow range

Acquisition of a value in the overflow or underflow range results in the mean calculation being stopped immediately. The value 32767 / 7FFF<sub>h</sub> or -32768 / 8000<sub>h</sub> is saved as an invalid mean value for the current mean value calculation period and sent when the next analog value message is triggered. The calculation of a new mean value is then started. If the analog value remains in the overflow or underflow range, this new value is again saved immediately as an invalid mean value and sent when the next frame is triggered.

---

### Note

#### Fault suppression time > 0 configured

If you have configured an error suppression time and then enable mean value generation, the value of the error suppression time is grayed out but no longer used. If mean value generation is enabled, the error suppression time is set to 0 (zero) internally.

---

## Smoothing factor

Analog values that fluctuate quickly can be evened out using the smoothing function.

The smoothing factors are calculated according to the following formula as with S7 analog input modules.

$$y_n = \frac{x_n + (k - 1)y_{n-1}}{k}$$

where

$y_n$  = smoothed value in the current cycle

$x_n$  = value acquired in the current cycle  $n$

$k$  = smoothing factor

The following values can be configured for the module as the smoothing factor.

- 1 = No smoothing
- 4 = Weak smoothing
- 32 = Medium smoothing
- 64 = Strong smoothing

The smoothing factor cannot be configured at the same time as mean value generation.

## Fault suppression time

An analog value in the overflow range (32767 / 7FFF<sub>h</sub>) or underflow range (-32768 / 8000<sub>h</sub>) is not transferred for the duration of the fault suppression time. This also applies to live zero inputs. The value in the overflow/underflow range is only sent after the fault suppression time has elapsed, if it is still pending.

If the value returns to the measuring range before the fault suppression time elapses, the current value is transferred immediately.

A typical use case for this parameter is the suppression of peak current values when starting up powerful motors that would otherwise be signaled to the control center as a disruption.

The suppression is adjusted to analog values that are acquired by the S7 analog input modules as raw values. These modules return the specified values for the overflow or underflow range for all input ranges (also for live zero inputs).

The fault suppression time cannot be configured at the same time as mean value generation.

### Recommendation for finished values that were preprocessed by the CPU:

If the CPU makes preprocessed finished values available in bit memory or in a data block, suppression is only possible or useful if these finished values also adopt the values listed above 32767 / 7FFF<sub>h</sub> or -32768 / 8000<sub>h</sub> in the overflow or underflow range. If this is not the case, the parameter should not be enabled for preprocessed values.

### Set limit value 'low' / Set limit value 'high'

In these two input boxes, you can set a limit value in the direction of the start of the measuring range or in the direction of the end of the measuring range. You can also evaluate the limit values, for example as the start or end of the measuring range.

If the limit value is overshoot or undershot, the status identifier "OVER\_RANGE" of the data point is set. This status identifiers are described in the section Status IDs of data points (Page 54).

The "OVER\_RANGE" bit of the status identifier of the data point is set as follows when the relevant analog value is transferred:

- Limit value 'high':
  - If the limit value is exceeded: OVER\_RANGE = 1
  - If the value falls below the limit value: OVER\_RANGE = 0
- Limit value 'low':
  - If the value falls below the limit value : OVER\_RANGE = 1
  - If the value then exceeds the limit value: OVER\_RANGE = 0

#### Requirements for the function

- Configuration of the threshold trigger for this data point
- PLC tag in the bit memory operand area or data area

The analog value data point must be linked to a PLC tag in the bit memory or data area (data block). For hardware modules (input operand area) limit value configuration is not possible.

The configuration of limit values is pointless for measured values that have already been preprocessed on the CPU.

**Configuration of the limit value**

The value to be configured as a whole decimal number therefore depends on the value range of the PLC tags and the raw value of the analog module:

| Division                             | Raw value of the of PLC tags * |             |             | Module output [mA] |                     |                    | Measuring range [%] |
|--------------------------------------|--------------------------------|-------------|-------------|--------------------|---------------------|--------------------|---------------------|
|                                      | Decimal                        |             | Hexadecimal | 0 - 20 (unipolar)  | -20 - +20 (bipolar) | 4 - 20 (life zero) |                     |
|                                      | 16 bits                        | 32 bits     | 16 bits     |                    |                     |                    |                     |
| Overflow                             | 32767                          | 2147483647  | 7FFF        | > 23.515           | > 23.515            | > 22.810           | > 117.593           |
| Overrange                            | 32511                          | 2130769779  | 7EFF        | 23.515             | 23.515              | 22.810             | 117.593             |
|                                      | ...                            | ...         | ...         | ...                | ...                 | ...                | ...                 |
|                                      | 27649                          | 1812067105  | 6C01        | 20.001             | 20.001              | 20.001             | 100.004             |
| Nominal range (unipolar / life zero) | 27648                          | 1811994624  | 6C00        | 20                 |                     | 20                 | 100                 |
|                                      | ...                            | ...         | ...         | ...                |                     | ...                | ...                 |
|                                      | 0                              | 0           | 0000        | 0                  |                     | 4                  | 0                   |
| Nominal range (bipolar)              | 27648                          | 1811994624  | 6C00        |                    | 20                  |                    | 100                 |
|                                      | ...                            | ...         | ...         |                    | ...                 |                    | ...                 |
|                                      | 0                              | 0           | 0000        |                    | 0                   |                    | 0                   |
|                                      | ...                            | ...         | ...         |                    | ...                 |                    | ...                 |
|                                      | -27648                         | -1811994625 | 9400        |                    | -20                 |                    | -100                |
| Underrange (unipolar / life zero)    | -1                             | -1          | FFFF        | -0.001             |                     | 3.999              | -0.004              |
|                                      | ...                            | ...         | ...         | ...                |                     | ...                | ...                 |
|                                      | -4864                          | -318729855  | ED00        | -3.518             |                     | 1.185              | -17.59              |
| Underrange (bipolar)                 | -27649                         | -1812067105 | 93FF        |                    | -20.001             |                    | -100.004            |
|                                      | ...                            | ...         | ...         |                    | ...                 |                    | ...                 |
|                                      | -32512                         | -2130769779 | 8100        |                    | -23.516             |                    | -117.593            |
| Undershoot / wire break              | -32768                         | -2147483648 | 8000        | < -3.518           |                     | < 1.185            | < -17.593           |

\* The raw values of the measured values relate to the values of 16-bit or 32-bit PLC tags.

**Note**

**Evaluation of the value even when the option is disabled**

If you enable one or both options and configure a value and then disable the option later, the grayed out value is nevertheless evaluated.

To disable the two options, delete the previously configured values limit values from the input boxes and then disable the relevant option.

**Recommendation for quickly fluctuating analog values:**

If the analog value fluctuates quickly, it may be useful to smooth the analog value first if limit values are configured. If the analog value fluctuates close to a limit value for a longer period of time, with a smoothed value you avoid a status change each time the value exceeds/falls below the limit value and so triggers a transfer.

#### 4.15.7.5 Partner stations: Configuring the inter-station communication

##### Options for specifying the communications partner

##### Telecontrol server activated / Enable partner for inter-station communication

If no partner was enabled for inter-station communication, the "Telecontrol server activated" option is selected automatically. In this case, the telecontrol server is the only communications partner of the data point.

If instead a CP of an S7 station should be the communications partner of the data point, select the option "Activate partner for inter-station communication".

The telecontrol server and a CP in an S7 station cannot be selected as the partner at the same time.

##### Partner number for inter-station communication:

Specify the partner CP for inter-station communication for this data point by selecting the partner number from the drop-down list.

The partners you specified in the table of the "Partner stations" > "Partner for inter-station communication" can be selected. The access ID of the relevant partner is shown in brackets.

##### Data point index

Index of the corresponding data point on the communications partner.

##### Note:

- The data pair of the sending and receiving CP must have an identical data point index. A receiving data point of CP 2 corresponds to a sending data point of CP 1 with the same data point index.
- For the opposite communications direction, a second pair of data points must be created: A sending data point of CP 2 corresponds to the receiving data point of CP 1. Once again, both have an identical data point index.

## 4.15.8 Messages

### Configuring SMS messages

If important events occur, the CP can send SMS messages. The recipient can be a mobile phone or an S7-1200.

You configure the SMS message in STEP 7 in the data point and message configuration. You can find this using the project tree:

Project > directory of the relevant station > Local modules > CP

For the view in STEP 7, refer to the section *Configuring data points and messages* (Page 47).

You will find the character set supported for the text of the SMS message in the section *Programming SMS messages via OUC* (Page 93).

### Configuring e-mails

If important events occur, the CP can send e-mails. The recipient can be a PC with an Internet connection or an S7-1200.

You configure the e-mails in STEP 7 in the data point and message configuration. You can find this using the project tree:

Project > directory of the relevant station > Local modules > CP

For the view in STEP 7, refer to the section *Configuring data points and messages* (Page 47).

### Triggering sending of messages

One of the following events triggers sending of the message:

- CPU changes to STOP.
- CPU changes to RUN.
- The connection to the partner is interrupted.
- The connection to the partner is re-established.
- Connection establishment has failed.
- Weak mobile wireless network (signal quality)
- A trigger signal is fired.

For the trigger signal to send the message, the edge change (0 → 1) of a trigger bit is evaluated that is set by the user program. When necessary, a separate trigger bit can be configured for each message.

If the memory area of the trigger bit is in the bit memory or in a data block, the trigger bit is reset to zero when the message is sent.

## Requirements and necessary information

Remember the following requirements in the CP configuration for the transfer of messages:

- Enabling telecontrol communication ("Communication types") parameter group
- Activating security functions
- Additionally for e-mails: Configuring the "E-mail configuration" parameter group

To do this, you require the following information:

- Access data of the SMTP server: Address, port number, user name, password

When using STARTTLS or SSL/TLS: Certificate of the e-mail service provider

- Email address of the recipient

## Text of the message optionally with the value of a PLC tag

In the text of every message, you can not only transfer the configured text but also the value of a PLC tag. To do this enter "\$\$" as a placeholder for the value to be sent in the message text. For the configuration, refer to the next section "Include value".

## Enable status identifier / External status

If this option is enabled in STEP 7, a status is output on the CP that provides information about the processing status of the sent message. The status is written to a PLC tag of the type DWORD that is specified in the "External status" box.

The meaning of the statuses is as follows:

Table 4- 4 SMS: Meaning of the status ID output in hexadecimal format

| Status | Meaning   |
|--------|---|
| 0000   | Transfer completed free of errors   |
| 8001   | Error in the transfer, possible causes: <ul style="list-style-type: none"> <li>• SIM card invalid</li> <li>• No network</li> <li>• Wrong destination phone number (number not reachable)</li> </ul> |

4.15 STEP 7 configuration of individual parameters

Table 4- 5 E-mails: Meaning of the status ID output in hexadecimal format

| Status | Meaning  |
|--------|--|
| 0000   | Transfer completed free of errors  |
| 82xx   | Other error message from the e-mail server<br>Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.   |
| 8401   | No channel available<br>Possible cause: There is already an e-mail connection via the CP. A second connection cannot be set up at the same time.   |
| 8403   | No TCP/IP connection could be established to the SMTP server.  |
| 8405   | The SMTP server has denied the login request.  |
| 8406   | An internal SSL error or a problem with the structure of the certificate was detected by the SMTP client.  |
| 8407   | Request to use SSL was denied.   |
| 8408   | The client could not obtain a socket for creating a TCP/IP connection to the mail server.  |
| 8409   | It is not possible to write via the connection. Possible cause: The communications partner reset the connection or the connection aborted.   |
| 8410   | It is not possible to read via the connection. Possible cause: The communications partner terminated the connection or the connection was aborted.   |
| 8411   | Sending the e-mail failed. Cause: There was not enough memory space for sending.   |
| 8412   | The configured DNS server could not resolve specified domain name.   |
| 8413   | Due to an internal error in the DNS subsystem, the domain name could not be resolved.  |
| 8414   | An empty character string was specified as the domain name.  |
| 8415   | An internal error occurred in the cURL module. Execution was aborted.  |
| 8416   | An internal error occurred in the SMTP module. Execution was aborted.  |
| 8417   | Requests to SMTP on a channel already being used or invalid channel ID. Execution was aborted.   |
| 8418   | Sending the e-mail was aborted. Possible cause: Execution time exceeded.   |
| 8419   | The channel was interrupted and cannot be used before the connection is terminated.  |
| 8420   | Certificate chain from the server could not be verified with the root certificate of the CP.   |
| 8421   | Internal error occurred. Execution was stopped.  |
| 8450   | Action not executed: Mailbox not available / unreachable. Try again later.   |
| 84xx   | Other error message from the e-mail server<br>Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.   |
| 8500   | Syntax error: Command unknown.<br>This also includes the error of having a command chain that is too long. The cause may be that the e-mail server does not support the LOGIN authentication method.<br>Try sending e-mails without authentication (no user name). |
| 8501   | Syntax error. Check the following configuration data:<br>Message configuration > Message parameters: <ul style="list-style-type: none"> <li>Recipient address ("To" or "Cc").</li> </ul>   |



| Status | Meaning  |
|--------|--|
| 8502   | Syntax error. Check the following configuration data:<br>Message configuration > Message parameters: <ul style="list-style-type: none"><li>• Email address (sender)</li></ul>  |
| 8535   | SMTP authentication incomplete. Check the "User name" and "Password" parameters in the CP configuration.   |
| 8550   | SMTP server cannot be reached. You have no access rights. Check the following configuration data: <ul style="list-style-type: none"><li>• CP configuration &gt; E-mail configuration:<ul style="list-style-type: none"><li>– User name</li><li>– Password</li><li>– Email address (sender)</li></ul></li><li>• Message configuration &gt; Message parameters:<ul style="list-style-type: none"><li>– Recipient address ("To" or "Cc").</li></ul></li></ul> |
| 8554   | Transfer failed  |
| 85xx   | Other error message from the e-mail server<br>Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.   |

### Include value

If you enable the option "Include value", the CP sends a value for the placeholder \$\$ from the memory area of the CPU in the message. To do this, you configure a PLC tag whose value is integrated in the message.

The value is entered in the message text instead of the placeholder \$\$.

## 4.16 Access to the Web server

### Access to the Web server of the CPU

The Web server of the S7-1200 station is located in the CPU. Via the LAN interface of the CP, you have access to the Web server of the CPU.

Access using HTTPS: When there is secure access (HTTPS) to the Web server using the IP address of the CP, the SSL certificate of the CPU is displayed.



## Programming the program blocks

### 5.1 Program blocks for OUC

#### Using the program blocks for Open User Communication (OUC)

The instructions (program blocks) listed below are required for direct communication between S7 stations via the mobile wireless network.

In contrast to other communication types, Open User Communication does not need to be enabled in the configuration of the CP because corresponding program blocks need to be created for this. You will find details on the program blocks in the information system of STEP 7.

To use the Open User Communication, the CP requires a fixed IP address to be assigned by the mobile wireless network provider.

---

#### Note

##### Different program block versions

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

---

#### Supported program blocks for OUC

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

- TSEND\_C V3.0 / TRCV\_C V3.0  
Compact blocks for connection establishment/termination and sending / connection establishment/termination and receiving  
Transfer of data or SMS message  
or
- TCON V4.0 / TDISCON V2.1  
Connection establishment / connection termination
- TUSEND V4.0 / TURCV V4.0  
Sending and receiving data via UDP
- TSEND V4.0 / TRCV V4.0
  - Sending and receiving data via TCP or ISOonTCP
  - Sending and receiving SMS messages
- TMAIL\_C V4.0  
Sending e-mails

The program block can be found in STEP 7 in the "Instructions > Communication > Open User Communication" window.

## Connection descriptions in system data types (SDTs)

For the connection description, the blocks listed above use the parameter CONNECT (or MAIL\_ADDR\_PARAM with TMAIL\_C). The connection description is stored in a data block whose structure is specified by the system data type (SDT).

### Creating an SDT for the data blocks

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

### Using the SDT

- **TCON\_Param**

For transferring frames via TCP

- **TADDR\_Param**

For transferring frames via UDP

- **TCON\_IP\_RFC**

For transferring frames via ISO-on-TCP (direct communication between two S7-1200 stations)

- **TCON\_Phone**

For transferring SMS messages

- **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

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

You will find notes on programming SMS messages in the section Programming SMS messages via OUC (Page 93).

## Connection establishment and termination

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

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

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

---

### Note

#### Connection abort

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

---

## 5.2 Programming SMS messages via OUC

### Transferring e-mails / SMS messages via OUC or telecontrol communication

The event-driven sending of e-mails or SMS messages using telecontrol communication is configured in STEP 7 in the message editor, refer to the section Messages (Page 86). No program blocks are required for this.

You only require the program blocks and system data types (SDTs) described below to transfer SMS messages using Open User Communication.

### Programming SMS messages

#### **Sending SMS messages to one partner**

To do this, create the following blocks or system data types (alternatives):

- TCON + TDISCON + TSEND + TCON\_PHONE
- TSEND\_C + TCON\_PHONE

#### **Receiving SMS messages from one partner**

To do this, create the following blocks or system data types (alternatives):

- TCON + TDISCON + TRCV + TCON\_PHONE
- TRCV\_C + TCON\_PHONE

If you do not program a phone number in the "PhoneNumber" parameter of the TCON\_PHONE system data type, the CP cannot receive any SMS messages.

#### **Receiving SMS messages from several partners**

As an alternative, you can create a separate block set for each partner as described above for 1 partner or a single block set with the following special feature in the TCON\_PHONE block:

If you enter an asterisk (\*) after the phone number body in the "PhoneNumber" parameter of the TCON\_PHONE block, the asterisk acts as a placeholder for all authorized phone numbers with this phone number body.

You configure the phone numbers authorized for access to the CP in STEP 7 in the "Security" parameter group of the CP.

#### **Message text to be sent in the "DATA" parameter**

You enter the message text as a string in the "DATA" parameter of TSEND or TSEND\_C.

A message can contain up to 160 characters. If the message text contains more than 160 characters, the text is distributed over two or more SMS messages.

#### **Reading out the message text from the "DATA" parameter**

To receive an SMS message, program the message text to be read out in the TRCV / TRCV\_C in the "DATA" parameter via a data block of the data type "Struct".

When creating this structure (DB of the data type "Struct"), no optimized block access can be configured.

The structure should have a size of 194 bytes and the following structure to store the relevant data of the received SMS message:

- DTL  
12 bytes for the time stamp of the received SMS message (time stamp from the network)
- String[22]  
String of 22 bytes for the phone number of the sender
- String[160]  
String of 160 bytes for the message text  
The SMS message text can contain max. 160 characters.
- Byte  
Status of the SMS message:
  - 0 = Invalid
  - 1 = Unread
  - 2 = Read

#### Storing the last 10 received SMS messages

You can output up to 10 received SMS messages from the receive block by making the entry "SMSSTORE" for the "PhoneNumber" parameter of TCON\_PHONE.

In this case, you need to create an adequately large structure (1940 bytes) for the "DATA" parameter of the receiving block to save the received data of 10 SMS messages. The structure is then organized as follows:

- Received data SMS 1 (DTL, String[22], String[160], Byte)
- Received data SMS 2 (DTL, String[22], String[160], Byte)
- ... to
- Received data SMS 10 (DTL, String[22], String[160], Byte)

## Character set for the SMS text

The CP supports the following ASCII character set (hexadecimal value and character name) for SMS message texts:

- 0x0A  
LF (line feed)
- 0x0D  
CR (carriage return)
- 0x20  
Space
- 0x21 ... 0x5A  
!"#\$%&'()\*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN  
OPQRSTUVWXYZ
- 0x5F  
£
- 0x61 ... 0x7A  
abcdefghijklmnopqrstuvwxyz

## 5.3 TC\_CONFIG for changing configuration data of the CP

### Meaning

With the program block TC\_CONFIG , you can modify parameters of a the CP configured in STEP 7. The configured values are not overwritten retentively. The overwritten values remain valid until TC\_CONFIG is called again or until the station starts up again (cold restart after cycling power).

If the STEP 7 configuration data of the CP needs to be changed permanently, the block needs to be called again each time the station restarts (cold restart) or a modified project must be downloaded to the station.

The CONFIG parameter points to the memory area with the configuration data. The configuration data is stored in a data block (DB). The DB cannot be created with optimized block access. The structure of the DB is specified by the system data type (SDT) IF\_CONF.

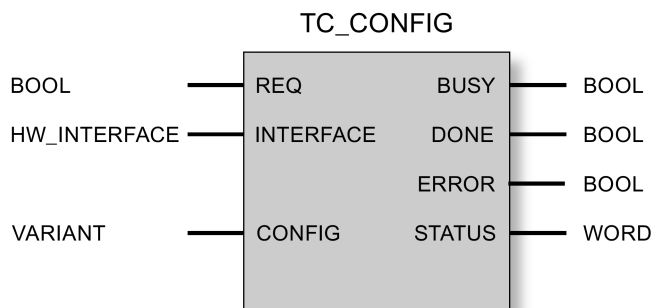
The configuration data to be modified on the CP is put together as necessary in blocks in IF\_CONF "IF\_CONF\_..." for the individual parameters.

Parameters that are not intended to change as a result of the block are not entered in IF\_CONF. They retain the value configured in STEP 7.

For detailed information on programming IF\_CONF, refer to the section IF\_CONF: SDT for the configuration data of the CP (Page 99).

The INTERFACE parameter references the name of the interface of the mobile wireless CP. You will find the name of the interface in the STEP 7 project in the standard tag table of the station in the "System constants" tab under the entry with the value of the "Hardware identifier" of the CP.

### Call interface in FBD representation





## Explanation of the formal parameters

The following table explains all the formal parameters for the TC\_CONFIG instruction

| Parameter | Declaration | Data type           | Possible values  | Description  |
|-----------|-------------|---------------------|--|--|
| REQ       | INPUT       | BOOL                | 0, 1   | The processing of the block is started and the status codes initialized on a rising edge.<br>Updating of the DONE, ERROR and STATUS status codes when there is no positive edge.   |
| INTERFACE | INPUT       | HW_Interface (WORD) |  | Reference to the interface of the local CP   |
| CONFIG    | INOUT       | VARIANT             | See also "IF_CONF: SDT for telecontrol configuration data  | Reference to the memory area with the collected configuration data to be modified  |
| ENO       | OUTPUT      | BOOL                | 0: Error<br>1: Error-free  | Enable output<br>If there is a runtime error with the instruction, ENO = 0 is set.   |
| BUSY      | OUTPUT      | BOOL                | 0: Execution of the instruction not yet started, completed or aborted<br>1: The instruction is executing | Condition code of the execution status of the block  |
| DONE      | OUTPUT      | BOOL                | 0: -<br>1: The instruction executed successfully   | This parameter indicates whether or not the job was completed without errors.<br>For the meaning in conjunction with the parameters ERROR and STATUS, refer to Codes of the block. |
| ERROR     | OUTPUT      | BOOL                | 0: -<br>1: Error   | Error code<br>For the meaning in conjunction with the parameters DONE and STATUS, refer to Codes of the block.   |
| STATUS    | OUTPUT      | WORD                |  | Status code<br>For the meaning in conjunction with the parameters DONE and ERROR, refer to Codes of the block.   |

### The codes BUSY, DONE and ERROR

The codes of DONE and ERROR are relevant only when BUSY = 0.

| BUSY | DONE | ERROR | Meaning               |
|------|------|-------|-----------------------|
| 0    | 0    | 0     | No job being executed |

You will find all other code combinations of DONE and ERROR in the following table.

### The codes DONE, ERROR and STATUS

The following table shows the condition codes formed based on DONE, ERROR and STATUS that must be evaluated by the user program.

| DONE | ERROR | STATUS | Meaning  |
|------|-------|--------|--|
| 1    | 0     | 0000H  | Job executed without errors  |
| 0    | 0     | 7000H  | No job processing active (first block call)  |
| 0    | 0     | 7001H  | Job processing started (first block call)  |
| 0    | 0     | 7002H  | Job processing already active (renewed block call when BUSY = 1)   |
| 0    | 1     | 80E6H  | No query in progress (block call not started)  |
| 0    | 1     | 80EBH  | Query temporarily rejected (the CP is currently being configured by STEP 7)  |
| 0    | 1     | 80F6H  | Format error of a parameter in the called data block (wrong length, wrong format or invalid value)<br>Check the "IF_CONF" SDT. |
| 0    | 1     | 80F7H  | Wrong ID in the parameter fields of the configuration data:<br>Check the "IF_CONF" SDT.  |

## 5.4 IF\_CONF: SDT for the configuration data of the CP

### Structure of the system data type IF\_CONF for the TC\_CONFIG program block

The CONFIG parameter of the TC\_CONFIG program block references the memory area containing the configuration data of the CP to be modified. The configuration data stored in a data block is described as a structure of the IF\_CONF system data type (SDT).

IF\_CONF is made up of a header followed by fields that correspond to the parameters or parameter areas of the CP in the device properties of the STEP 7 project.

The CP configuration data to be modified is collected together as IF\_CONF fields. Parameters that will not be modified are ignored in the IF\_CONF structure and remain as they were configured in the STEP 7 project.

### Creating the DB and the IF\_CONF structures

You can create the parameters of the CP within the IF\_CONF DB in one or more structures each with one or more fields.

You will need to type in the data types of the fields using the keyboard. They are not displayed in the selection list. The data types are not case-sensitive.

Follow the steps below to create IF\_CONF:

1. Create a data block of the type "global DB" with block access "Standard".
2. Create a structure (data type "Struct") in the table of the parameter configuration of the DB.

You can specify any name.

3. Under this structure add a header by assigning the name of the header and typing it in in the cell of the data type "IF\_CONF\_Header".

The header of the structure and its three parameters (see below) is created.

4. Create a field for the first parameter to be changed by typing in the required data type (for example "IF\_CONF\_APN") in the cell of the data type.
5. Repeat the last step for all parameters you want to change on the CP using the TC\_CONFIG instruction.
6. Finally, update the number of fields in the header in the "subfieldCnt" parameter.

### Header of IF\_CONF

Table 5- 1 IF\_CONF\_Header

| Byte    | Parameter   | Data type | Initial value | Description                                       |
|---------|-------------|-----------|---------------|---|
| 0 ... 1 | fieldType   | UINT      |               | Field type: Must always be 0.                     |
| 2 ... 3 | fieldId     | UINT      |               | Field ID: Must always be 0.                       |
| 4 ... 5 | subfieldCnt | UINT      |               | Total number of fields contained in the structure |

### General parameters of the parameter fields

Each field has the following general parameters:

- Id  
This parameter identifies the field and must not be modified.
- Length  
This parameter indicates the length of the field. The value serves as information.  
Fields with strings and / or arrays have a variable length. Due to hidden bytes, the actual length of fields can be greater than the sum of the displayed parameters.
- Mode  
The following values are permitted to these parameters:

Table 5- 2 Values of "Mode"

| Value | Meaning   |
|-------|---|
| 1     | Permanent validity of the configuration data<br>Not relevant for the CP   |
| 2     | Temporary validity of the configuration data, including deleting of existing permanent configuration data<br>The permanent configuration data is replaced by the parameter fields of IF_CONF. |

**"APN settings"**

In STEP 7, the corresponding data is located in the "Mobile wireless communications settings" parameter area.

Table 5- 3 IF\_CONF\_APN

| Parameter           | Data type   | Initial value | Description  |
|---------------------|-------------|---------------|--|
| Id                  | UINT        | 4             | ID of the parameter field  |
| Length              | UINT        |               | Length of the parameter field in bytes: 174                                    |
| Mode                | UINT        |               | Validity (1, 2) - see above (general parameters)                               |
| AccesspointGPRS     | STRING [98] |               | APN: Name of the access point from the mobile wireless network to the Internet |
| AccesspointUser     | STRING [42] |               | APN user name  |
| AccesspointPassword | STRING [22] |               | APN password   |

**"CP identification"**

In STEP 7, the corresponding data is located in the "Security" parameter area.

Table 5- 4 IF\_CONF\_Login

| Parameter     | Data type   | Initial value | Description  |
|---------------|-------------|---------------|--|
| Id            | UINT        | 5             | ID of the parameter field  |
| Length        | UINT        |               | Length of the parameter field in bytes: 54                           |
| Mode          | UINT        |               | Validity (1, 2) - see above (general parameters)                     |
| ModemName     | STRING [22] |               | Access ID  |
| ModemPassword | STRING [22] |               | Telecontrol password<br>The password cannot be changed with IF_CONF. |

**"Telecontrol server"**

In STEP 7, the corresponding data is located in the "Partner stations" parameter area."

This field is only used when the telecontrol server is addressed with a name that can be resolved by DNS or when the IP address is to stored as a string.

Table 5- 5 IF\_CONF\_TCS\_Name

| Parameter  | Data type    | Initial value | Description  |
|------------|--------------|---------------|--|
| Id         | UINT         | 6             | ID of the parameter field  |
| Length     | UINT         |               | Length of the parameter field in bytes: 266  |
| Mode       | UINT         |               | Validity (1, 2) - see above (general parameters)   |
| TcsName    | -            | -             | - reserved -   |
|            | STRING [254] |               | Name of the telecontrol server that can be resolved by DNS or IP address as string   |
| RemotePort | UINT         |               | Port of the telecontrol server   |
| Rank       | UINT         |               | Priority of the server [1, 2]<br>1 = first telecontrol server,<br>2 = second telecontrol server (second server not relevant) |

**"SMSC"**

In STEP 7, the corresponding data can be found in the parameter area "Mobile wireless communications settings" > "Services and settings".

Table 5- 6 IF\_CONF\_SMS\_Provider

| Parameter   | Data type   | Initial value | Description   |
|-------------|-------------|---------------|---|
| Id          | UINT        | 10            | ID of the parameter field   |
| Length      | UINT        |               | Length of the parameter field in bytes: 28  |
| Mode        | UINT        |               | Validity (1, 2) - see above (general parameters)  |
| SMSProvider | STRING [20] |               | Subscriber number of the SMS center (SMSC) of the mobile wireless network provider with which the mobile wireless contract was signed for this station. |

**"PIN"**

In STEP 7, the PIN can be found in the parameter area "Mobile wireless communications settings" > "Services and settings".

Table 5- 7 IF\_CONF\_PIN

| Parameter | Data type  | Initial value | Description   |
|-----------|------------|---------------|---|
| Id        | UINT       | 11            | ID of the parameter field   |
| Length    | UINT       |               | Length of the parameter field in bytes: 16  |
| Mode      | UINT       |               | Validity (1, 2) - see above (general parameters)  |
| Pin       | STRING [8] |               | PIN of the SIM card inserted in the SIM card<br>The parameter is not relevant if the PIN was correctly configured. If the PIN was incorrectly configured, the correct PIN can be entered. |

**"Authorized phone number"**

In STEP 7, the corresponding data is located in the "Security" parameter area.

Table 5- 8 IF\_CONF\_WakeupList

| Parameter            | Data type                        | Initial value | Description   |
|----------------------|----------------------------------|---------------|---|
| Id                   | UINT                             | 13            | ID of the parameter field   |
| Length               | UINT                             |               | Length of the parameter field in bytes: 246   |
| Mode                 | UINT                             |               | Validity (1, 2) - see above (general parameters)  |
| WakeupPhone [1...10] | ARRAY [1...10]<br>of STRING [22] |               | Phone number subscriber authorized to wake up<br>The asterisk (*) at the end of a call number is used a placeholder for direct dialing numbers. |

**"Preferred mobile wireless networks"**

In STEP 7, the corresponding data is located in the "Mobile wireless communications settings" parameter area.

Table 5- 9 IF\_CONF\_PrefProvider

| Parameter        | Data type                   | Initial value | Description   |
|------------------|-----------------------------|---------------|---|
| Id               | UINT                        | 14            | ID of the parameter field   |
| Length           | UINT                        |               | Length of the parameter field in bytes: 46  |
| Mode             | UINT                        |               | Validity (1, 2) - see above (general parameters)  |
| Provider [1...5] | ARRAY [1...5] of STRING [6] |               | Alternative mobile wireless networks with priority 1 to 5 into which the CP dials. Up to 5 networks can be configured. No. 1 with highest priority, no. 5 with lowest priority.<br>Entry of the Public Land Mobile Network (PLMN) of the network provider consisting of Mobile Country Code (MCC) and Mobile Network Code (MNC).<br>Example (test network of Siemens AG): 26276 |

**TeleService access (DNS name / IP address of the server)**

Access data of the TeleService server (switching station).

In STEP 7, the corresponding data is located in the "Mobile wireless communications settings" parameter area.

Table 5- 10 IF\_CONF\_TS\_Name

| Parameter  | Data type    | Initial value | Description  |
|------------|--------------|---------------|--|
| Id         | UINT         | 20            | ID of the parameter field  |
| Length     | UINT         |               | Length of the parameter field in bytes: 266  |
| Mode       | UINT         |               | Validity (1, 2) - see above (general parameters)   |
| ts_name    | String [254] |               | Name of the TeleService server that can be resolved by DNS or IP address as string   |
| RemotePort | UINT         |               | Port of the engineering station  |
| Rank       | UINT         |               | Priority of the server [1] or [2]: <ul style="list-style-type: none"> <li>• 1 = server 1</li> <li>• 2 = server 2 (not relevant)</li> </ul> |



## Diagnostics and upkeep

### 6.1 Diagnostics options

The following diagnostics options are available:

#### LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 28).

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

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

- Entries in the diagnostics buffer of the CPU
- Information on the online status of the module

#### STEP 7: Diagnostics functions via the "Online > Online and diagnostics" menu

On the diagnostics pages, you can obtain static information on the selected module:

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

- Industrial Remote Communication

Here, you obtain specific information on the mobile wireless interface and other parameters of the CP. The entry job has the following subentries:

- Partner

Information about the address settings of the partner, connection statistics, configuration data of the partner and other diagnostics information.

- Mobile wireless parameters

Diagnostics information on the network, statistical connection information, information on received/sent messages

- List of data points

Various information on the data points such as configuration data, value, connection status etc.

- Protocol diagnostics

Trace data of the transfer protocol

- Device-specific events

Information on CP-internal events

- Time

Information on the time on the device

### Diagnostics options via the Web server of the CPU

You will find details on the diagnostics options of the Web server in the S7-1200 system manual, see /1/ (Page 129).

### Diagnostics SMS message

The CP sends a diagnostics SMS message to a telephone with an authorized call number if it receives an SMS message with the following text from this telephone:

CPDIAG

The diagnostics SMS message that is then sent contains the following data of the S7 station:

- Firmware version of the CP
- Mode of the CPU (RUN / STOP)
- Status of the mobile wireless network connection
- Date and time of the last dial-in to the mobile wireless network

The data is specified in the ISO 8601 format ("Attach: YYYY-MM-DD hh:mm:ss").

If the time-of-day of the CP has not been synchronized at the time of the dial-in, the time of the measurement since the beginning of the default time-of-day of the CP (01.01.2009) is transferred.

If the last attempted dial-in to the mobile wireless network was not successful, "Attach: -" is sent.

- Name of the current mobile wireless network
- IP address of the CP
- Signal strength of the mobile wireless network
  - good: Good signal quality (-73 ... -51 dBm)
  - medium: Medium signal quality (-89 ... -74 dBm)
  - weak: Bad signal quality (-109 ... -90 dBm)
  - no signal: Signal too weak to be received ( $\leq$  -110 dBm)
- Received Signal Strength Indication (RSSI) - Received field strength at the station [0 ... 31]
- Status of the connection to the telecontrol server

If the data to be sent exceeds the default size of an SMS message, several SMS messages are sent.

### **Diagnostics options of the telecontrol server**

For telecontrol communication, TCSB provides several diagnostics options that you should use if problems occur during productive operation.

If there are connection problems between the station and telecontrol server, you can check the connection step-by-step using the following system tags:

- ConnectionState
- PLCConnected
- PLCCpuState

### **Failed mobile wireless transmission**

If mobile wireless transmission is not working but all other settings and connections are correct, check the external power supply of the CP.

## 6.2 Downloading firmware

### New firmware versions of the CP

If a new firmware version is available for the module, you will find this on the Internet pages of Siemens Industry Online Support under the following entry ID:

102255422 (<http://support.automation.siemens.com/WW/view/en/102255422>)

On the Internet page, select the "Entry list" tab and the "Download" entry type. There you will find the available firmware files.

There are three different ways of loading a new firmware file on the CP:

- Saving the firmware file on the memory card of the CPU  
You will find a description of the procedure for loading on the memory card of the CPU on the Internet page of Industry Online Support shown above.
- Loading the firmware with the online functions of STEP 7 via a WAN
- Downloading the firmware via the Web server of the CPU (as of CPU firmware version V4.0)

You can recognize that firmware is being loaded by the flashing LEDs of the CP, see section LEDs (Page 28).

The last two methods are described below.

### Loading the firmware with the online functions of STEP 7 via a WAN

#### Requirements:

- The CP can be reached using its IP address.
- The engineering station and the CP are located in the same subnet.
- The new firmware file is stored on your engineering station.

#### Procedure:

1. Connect the engineering station to the network.
2. Open the relevant STEP 7 project on the engineering station.
3. Select the CP or the CPU of the station whose CP you want to update with new firmware.
4. Enable the online functions using the "Connect online" icon.
5. In the "Connect online" dialog, select the Ethernet interface "PN/IE" in the "Type of PG/PC interface" list box.
6. Select the slot of the CP or the CPU.

Both methods are possible.

7. Connect using the "Connect" button.

The "Connect online" wizard guides you through the remaining steps in installation.

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

## Downloading the firmware via the Web server of the CPU

Follow the steps below to connect to the Web server of the CPU from the engineering station and to download the CP's new firmware file to the station.

### Requirements in the CPU configuration

1. Open the corresponding project on the engineering station.
2. Select the CPU of the station involved in STEP 7.
3. Select the "Web server" entry.
4. In the parameter group "General", select the "Enable Web server for this interface" option.
5. With a CPU version V4.0 or higher, create a user in the user management with the name "admin".

You need to assign the right to perform firmware updates in the access level.

The procedure for establishing a connection to the Web server depends on whether you have enabled or disabled the "Allow access only using HTTPS" option in the "General" parameter group:

- **Connection establishment with HTTP**

Procedure if the "Allow access only using HTTPS" option is disabled

- **Connection establishment with HTTPS**

Procedure if the "Allow access only using HTTPS" option is enabled

These two variants are described in the following sections.

Requirement: The new firmware file is stored on your engineering station.

You will find the requirements for access to the Web server of the CPU (permitted Web browser) and the description of the procedure in the STEP 7 information system under the keyword "Information about the Web server".

### Connection establishment with HTTP

1. Connect the PC on which the new firmware file is located to the CPU via the Ethernet interface.
2. Enter the address of the CPU in the address box of your Web browser: **http://<IP address>**
3. Press the Enter key.  
The start page of the Web server opens.
4. Click on the "Download certificate" entry at the top right of the window.  
The "Certificate" dialog opens.

5. Download the certificate to your PC by clicking the "Install certificate ..." button.

The certificate is loaded on your PC.

You will find information on downloading a certificate in the help of your Web browser and in the STEP 7 information system under the key words "HTTPS" or "Access for HTTPS (S7-1200)".

6. When the connection has changed to the secure mode HTTPS ("**https://<IP address>/...**" in the address box of the Web server), you can continue as described in the next section "Downloading firmware".

If you terminate the connection to the Web server, the next time you can log in with the Web server without downloading the certificate using HTTP.

#### **Connection establishment with HTTPS**


1. Connect the PC on which the new firmware file is located to the CPU via the Ethernet interface.
2. Enter the address of the CPU in the address box of your Web browser: **https://<IP address>**
3. Press the Enter key.  
The start page of the Web server opens.
4. Continue as described in the following section "Downloading firmware".

#### **Loading firmware**

1. Log in on the start page of the Web server as an administrator.
  - User name: admin
  - Password: No password necessary
2. After logging in, select the entry "Module status" in the navigation panel of the Web server.
3. Select the CP in the module list.
4. Select the "Firmware" tab lower down in the window.
5. Browse for the firmware file on your PC using the "Browse..." button and download the file to the station using the "Run update" button.

## 6.3 Module replacement

### Module replacement

|   |
|---|
|  <b>WARNING</b>  |
| <b>Read the system manual "S7-1200 Programmable Controller"</b>   |
| Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller" (refer to the documentation in the Appendix). |
| When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".   |
| Make sure that the power supply is turned off when installing/uninstalling the devices.   |

The STEP 7 project data of the CP is stored on the local CPU. If there is a fault on the device, this allows simple replacement of this communications module without needing to load the project data to the station again.

When the station starts up again, the new CP reads the project data from the CPU.

If you replace a module, remember to take the SIM card from the old module and insert it in the new CP.





# Technical specifications

## 7.1 General technical specifications

Table 7- 1 General technical specifications

| <b>Technical specifications</b>     |   |                                       |
|-------------------------------------|---|---------------------------------------|
| <b>Article number</b>               | Module name:<br>CP 1243-7 LTE-EU  | Article number: 6GK7 243-7KX30-0XE0   |
| <b>Antenna connector</b>            |   |                                       |
| Antenna connector                   | Quantity  | 1                                     |
|                                     | Design  | SMA socket                            |
|                                     | Nominal impedance   | 50 Ω                                  |
|                                     | Antenna cable, maximum permitted length                                     | ≤ 30 m                                |
| <b>Electrical data</b>              |   |                                       |
| External power supply               | Power supply  | 24 VDC                                |
|                                     | Permitted range   | 19,2 ... 28.8 V                       |
|                                     | Design  | Terminal block with plug, 3 terminals |
|                                     | Cable cross-section   |                                       |
|                                     | • Minimum   | • 0.14 mm <sup>2</sup> (AWG 25)       |
|                                     | • Maximum   | • 1.5 mm <sup>2</sup> (AWG 15)        |
|                                     | Max- tightening torque of the screw terminals                               | 0.45 Nm (4 lb-in)                     |
|                                     | Electrical isolation:<br>Power supply unit to internal circuit              | 710 VDC for 1 minute                  |
| Current consumption (typical)       | From 24 VDC (external)  | 75 mA                                 |
|                                     | From the S7-1200 backplane bus  | 100 mA                                |
| Effective power loss (typical)      | From 24 VDC (external)  | 1.8 W                                 |
|                                     | From the S7-1200 backplane bus  | 0.5 W                                 |
| <b>Permitted ambient conditions</b> |   |                                       |
| Ambient temperature                 | During operation with the rack installed horizontally (DIN rail horizontal) | -20 °C ... +70 °C                     |
|                                     | During operation with the rack installed vertically (DIN rail vertical)     | -20 °C ... +60 °C                     |
|                                     | During storage  | -40 °C ... +70 °C                     |
|                                     | During transportation   | -40 °C ... +70 °C                     |
| Relative humidity                   | During operation  | ≤ 95 % at 25 °C, no condensation      |

*Technical specifications*

---

*7.1 General technical specifications*

---

---

| <b>Technical specifications</b>      |   |
|--------------------------------------|---|
| <b>Design, dimensions and weight</b> |   |
| Module format                        | Compact module for S7-1200, single width  |
| Degree of protection                 | IP20  |
| Weight                               |   |
| • Net weight                         | • 133 g   |
| • Weight including packaging         | • 170 g   |
| Dimensions (W x H x D)               | 30 x 100 x 75 mm  |
| Installation options                 | <ul style="list-style-type: none"><li>• 35 mm DIN rail</li><li>• Switch panel</li></ul> |

---

You will find additional functions and performance data in the section Application and properties (Page 11).

## 7.2 Technical specifications - wireless interface (CP 1243-7 LTE-EU)

Table 7- 2 Technical specifications of the wireless interface

| <b>Technical specifications</b>            |                                |   |
|--|--------------------------------|---|
| <b>Article number</b>                      | 6GK7 243-7KX30-0XE0            |   |
| <b>Frequency bands</b>                     |                                |   |
| CP 1243-7 LTE-EU                           | LTE                            | B3 (1800 MHz)   |
|  |                                | B7 (2600 MHz)   |
|  |                                | B20 (800 MHz)   |
|  | UMTS                           | B1 (2100 MHz)   |
|  |                                | B8 (900 MHz)  |
|  | GSM                            | GSM (850/900 MHz)<br>DCS (1800 MHz)<br>PCS (1900 MHz)   |
| <b>Wireless interface</b>                  |                                |   |
| Maximum transmit power in the service used | LTE FDD (B3, B4, B7, B13, B20) | +23 dBm (Class 3)   |
|  | WCDMA FDD (B1, B2, B5, B8)     | +24 dBm (Class 3)   |
|  | EDGE 1800/1900 MHz             | +26 dBm (Class E2)  |
|  | EDGE 850/900 MHz               | +27 dBm (Class E2)  |
|  | DCS 1800, PCS 1900             | +30 dBm (Class 1)   |
|  | GSM 850/950                    | +33 dBm (Class 4)   |
| LTE  | Transmission speed (maximum)   | <ul style="list-style-type: none"> <li>Downlink: 100 Mbps</li> <li>Uplink: 50 Mbps</li> </ul>   |
| HSPA                                       | Transmission speed (maximum)   | <ul style="list-style-type: none"> <li>Downlink (HSDPA): 42 Mbps</li> <li>Uplink (HSUPA): 5.76 Mbps</li> </ul>                        |
| EDGE                                       | Properties                     | <ul style="list-style-type: none"> <li>Multislot class 10</li> <li>end device class B</li> <li>coding scheme 1 to 9 (GMSK)</li> </ul> |
|  | Transmission speed             | <ul style="list-style-type: none"> <li>Downlink: 236.8 kbps</li> <li>Uplink: 236.8 kbps</li> </ul>                                    |
| GPRS                                       | Properties                     | <ul style="list-style-type: none"> <li>Multislot class 10</li> <li>device class B</li> <li>coding scheme 1 to 4 (GMSK)</li> </ul>     |
|  | Transmission speed             | <ul style="list-style-type: none"> <li>Downlink: 85.6 kbps</li> <li>Uplink: 85.6 kbps</li> </ul>                                      |
| SMS  | Mode outgoing                  | MO  |
|  | Service                        | Point-to-point  |

### 7.3 Pin assignment of the socket for the external power supply

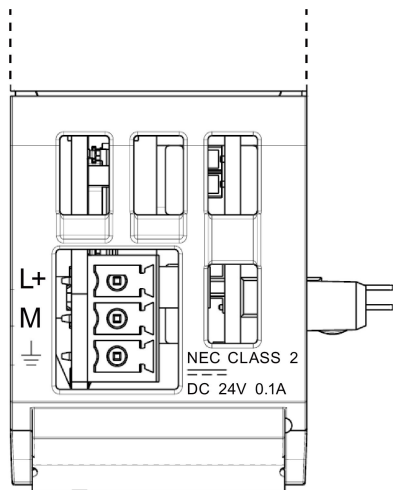



Figure 7-1 Socket for the external 24 VDC power supply (view from above)

Table 7-3 Pin assignment of the socket for the external power supply

| Pin | Labeling  | Function                      |
|-----|---|-------------------------------|
| 1   | L+  | + 24 VDC                      |
| 2   | M   | Ground reference for + 24 VDC |
| 3   |  | Ground connector              |

# Dimension drawings

# A

---

**Note**

All dimensions in the drawings of the CP are in millimeters.

---

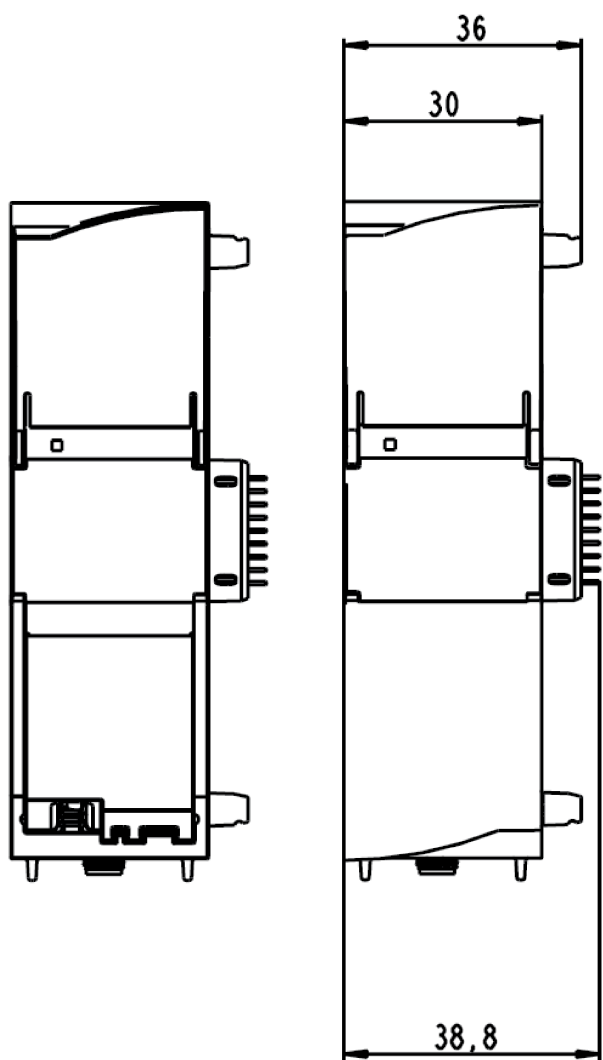


Figure A-1 Front view

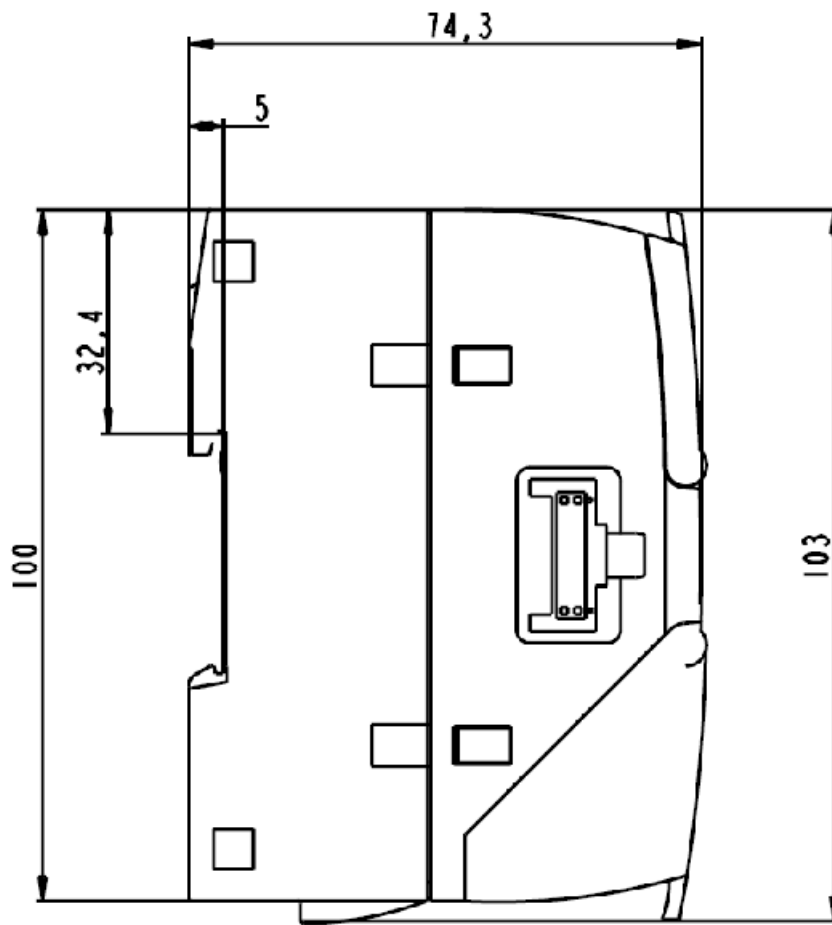


Figure A-2 Side view left

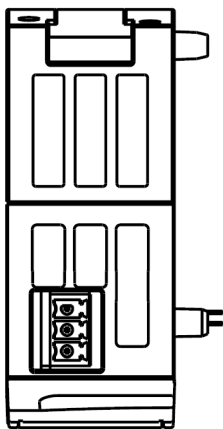


Figure A-3 From above

# Approvals

## Approvals issued

---

### Note

#### Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

---

## 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.

- **94/9/EC (ATEX explosion protection directive)**

Directive of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres

- **1999/5/EC (R&TTE)**

Directive of the European Parliament and of the Council of 9 March 1999 on Radio Equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity

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

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

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

Siemens Aktiengesellschaft  
Process Industries and Drives  
Process Automation  
DE-76181 Karlsruhe  
Germany

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

10805878 (<http://support.automation.siemens.com/WW/view/en/10805878>) → "Entry List" tab

Filter settings:  
Entry type: "Certificates"  
Certificate Type: "Declaration of Conformity"  
Search items(s): <name of the module>

### Use of the device in hazardous areas

The device shall only be used in an area with pollution degree 1 or 2, as defined in IEC 60664-1.

### IECEX

The CP meets the requirements of explosion protection according to IECEx.

IECEX classification: Ex nA IIC T4 Gc

The CP meets the requirements of the following standards:

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

### ATEX



The CP meets the requirements of the EC directive 94/9/EC "Equipment and Protective Devices for Use in Potentially Explosive Atmospheres".

Applied standards:

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

ATEX approval: II 3 G Ex nA II T4

Test number: KEMA 10 ATEX 0166X

Over and above this, the following conditions must be met for the safe deployment of the CP; see section General notices on use in hazardous areas according to ATEX (Page 35).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find on the supplied data medium with the documentation.

For information on the EU declaration of conformity see above.



## R&TTE

The CP meets the requirements of the EC directive 1999/5/EC "Radio equipment and telecommunications terminal equipment" according to the requirements of article 3 (1) a, 3 (1) b and 3 (2).

### Article 3 (1) a - Health and Safety

Harmonized standards:

- EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013  
Information technology equipment - Safety - Part 1: General requirements
- EN 62479:2010  
Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz ... 300 GHz)
- EN 62311:2008  
Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz ... 300 GHz)

### Art. 3 (1) b - EMC

Harmonized standards:

- ETSI EN 301 489-1 V1.9.2  
Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 1 : Common technical requirements
- ETSI EN 301 489-3 V1.6.1  
Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility (EMC) for radio equipment and services - Part 3 : Specific conditions for wireless devices with a low range (SRD) for use on frequencies between 9 kHz and 246 GHz
- ETSI EN 301 489-7 V1.3.1  
Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 7 : Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
- ETSI EN 301 489-24 V1.5.1  
Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 24 : Specific conditions for mobile and portable IMT-2000 CDMA Direct Spread (UTRA) radio and ancillary equipment
- EN 61000-6-1:2007  
Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments
- EN 61000-6-2:2005+AC:2005  
Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments

- EN 61000-6-3:2007+A1:2011+AC:2012  
Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments
- EN 61000-6-4:2007+A1:2011  
Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
- EN 55022:2010+AC:2011 Class A / B  
Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
- EN 55024:2010  
Information technology equipment - Immunity characteristics -Limits and characteristics - Limits and methods of measurement

### **Art. 3 (2) Measures of efficient use of the frequency spectrum**

Harmonized standards:

- ETSI EN 300 440-2 V1.4.1  
Electromagnetic compatibility and radio spectrum matters (ERM) - short range devices - radio equipment to be used in the 1 GHz to 40 GHz frequency range. Part 2: Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive.
- ETSI EN 301 511 V9.0.2  
Global system for mobile communication (GSM). Harmonized standard for mobile phones in the GSM 900 and GSM 1800 bands covering essential requirements of article 3.2 of the R&TTE directive.
- ETSI EN 301 908-1 V6.2.1  
IMT cellular networks - Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive. Part 1: Introduction and common requirements
- ETSI EN 301 908-2 V5.4.1  
IMT cellular networks. Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive. Part 2: CDMA Direct Spread (UTRA FDD) User Equipment (UE)

### **Maximum antenna gain**

Users and installers must be provided with antenna installation instructions and transmitter operating conditions that must be followed to avoid exceeding the permitted RF exposure.

Refer to the technical specifications of the antenna, refer to the appendix Antenna (Page 125).

## RoHS

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

Applied standard:

- EN 50581:2012

## cULus



Underwriters Laboratories Inc. meets

- Underwriters Laboratories, Inc.: UL 508 Listed (industrial control devices)
- Canadian Standards Association: CSA C22.2 No. 142 (process control equipment)

## cULus HAZ.LOC.



Underwriters Laboratories Inc. meets

- UL 1604 (Hazardous Location)
- CSA C22.2 No. 213 (Hazardous Location)

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4A; Ta = -20 °C...60 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...60 °C

## FM



Factory Mutual Research (FM)

Approval Standard Class number 3600 and 3611

Approved for use in:

Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C

Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

## C-Tick



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

## National approvals

You will find an overview of the country-specific wireless approvals of SIMATIC NET devices with GSM or UMTS services on the Internet pages of Siemens Automation Customer Support. You will find the link to the document on the following page:

[www.siemens.com/simatic-net/ik-info](http://www.siemens.com/simatic-net/ik-info)

## Other 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:

102255422 (<http://support.automation.siemens.com/WW/view/en/102255422>)

Under this entry, go to the relevant product and select the following settings: "Entry list" tab > entry type "Certificates".

## Overview of the approvals for SIMATIC NET products

You will find an overview of the approvals for SIMATIC NET products including approvals for shipbuilding on the Internet pages of Siemens Industry Online Support under the following entry ID:

57337426 (<http://support.automation.siemens.com/WW/view/en/57337426>)

## Accessories

### C.1 Antenna

The following antenna is available for use in mobile wireless networks and can be installed both indoors and outdoors. The antenna must be ordered separately.

#### Antenna ANT794-4MR



Figure C-1 Antenna ANT794-4MR

| Short name | Order no.      | Explanation   |
|------------|----------------|---|
| ANT794-4MR | 6NH9 860-1AA00 | Omnidirectional antenna for LTE networks (4G), GSM networks (2G) and UMTS networks (3G); weatherproof for indoor and outdoor areas; 5 m connecting cable connected permanently to the antenna, SMA connector, including installation bracket, screws, wall plugs. |

You will find detailed information in the documentation of the device. You will find this on the Internet on the pages of Siemens Industry Online Support under the following entry ID:

23119005 (<http://support.automation.siemens.com/WW/view/en/23119005>)

### C.2 TS Gateway

#### Use of TS Gateway

TS Gateway is an application used for TeleService connections via the mobile wireless network with remote SIMATIC stations of the type S7-1200.

### What is a TeleService gateway?

A TeleService gateway is a PC on which the "TS Gateway" software is installed.

A TeleService gateway is not configured in STEP 7.

### What functions does the TeleService gateway provide?

The TeleService gateway has the following functions:

- Switching station

The TeleService gateway is a PC in the network that serves as the intermediary between the engineering station and remote S7 station.

Since a firewall is normally closed for connection requests from the outside, a switching station between the remote station and the engineering station is required. This switching station can be a telecontrol server or, if there is no telecontrol server in the configuration, a TeleService gateway. The switching station directs the messages via a tunnel through the firewall. This allows access by the engineering station connected to a LAN to the S7-1200 via a router and via the APN of the network provider.

- Configuration of the SMS gateway provider

With the help of TS Gateway, SMS gateway providers are configured that are necessary for the sending of SMS messages to the remote S7 stations.

---

#### Note

##### TS Gateway only for TeleService

TS Gateway is used only for the "TeleService" function via the mobile wireless network. No connections to the remote stations can be monitored and no process data can be transferred.

---

### Configuration with TeleService gateway

A TeleService gateway is intended for the following telecontrol systems in which TeleService is used via a mobile wireless network:

- Configurations without a telecontrol server

In configurations without a telecontrol server, a TeleService gateway is required for TeleService via the mobile wireless network.

- Configurations with telecontrol server

In configurations in which a second path needs to be established for TeleService via the mobile wireless network alongside the telecontrol server, a TeleService gateway can be used.

This can, for example, be the case when certain people, groups or companies should not operate TeleService via the telecontrol server or when access to the stations for TeleService needs to be set up independent of the telecontrol server.

## Range of performance of a TS Gateway

Number of simultaneous TeleService connections: 1

If the requirements for availability are higher, you can install two TeleService gateways. If the connection cannot be established via one gateway, you can establish the TeleService connection via the second gateway. In terms of the range of functions the two systems are identical and are independent of each other.

Note that a station can only establish one TeleService connection.

## Requirements for TeleService with the TeleService gateway

The following requirements must be met for TeleService via a TeleService gateway:

- Engineering station connected to a LAN or with Internet access

TeleService using mobile wireless is possible on an engineering station with the STEP 7 project that contains the remote station with the mobile wireless CP.

STEP 7 version required for TeleService via the mobile wireless network: V13 + SP1.

- SIMATIC S7-1200
  - CPU with firmware version as of V4.1
  - Mobile wireless CP with firmware version as described in this manual.

PC for the TeleService gateway with:

- DVD drive
- Connection to LAN or Internet access for connecting to the engineering station
- Internet access for connecting to the remote S7 station
- Installation of the "TS Gateway" application

The software ships with the CP (see product DVD).

## Documentation

The manual on TS Gateway can be found on the Internet pages of Siemens Industry Online Support under the following entry ID:

89330723 (<http://support.automation.siemens.com/WW/view/en/89330723>)

See also /2/ (Page 130).





# Documentation references

## Where to find Siemens documentation

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

You can request the catalogs and additional information from your Siemens representative.

- You will find SIMATIC NET manuals on the Internet pages of Siemens Automation Customer Support:

Link to Customer Support (<http://support.automation.siemens.com/WW/view/en>)

Enter the entry ID of the relevant manual as the search item. The ID is listed below some of the reference entries in brackets.

As an alternative, you will find the SIMATIC NET documentation on the pages of Product Support:

10805878 (<http://support.automation.siemens.com/WW/view/en/10805878>)

Go to the required product group and make the following settings:

"Entry list" tab, Entry type "Manuals / Operating Instructions"

- You will find the documentation for the SIMATIC NET products relevant here on the data medium that ships with some products:
  - Product CD / product DVD or
  - SIMATIC NET Manual Collection

/1/

SIMATIC  
S7-1200 Programmable Controller  
System Manual  
Siemens AG  
Current issue under the following entry ID:  
34612486 (<http://support.automation.siemens.com/WW/view/en/34612486>)

**/2/**

SIMATIC NET  
CP 1243-7 LTE  
Operating Instructions  
Siemens AG  
entry ID: 102255422 (<http://support.automation.siemens.com/WW/view/en/102255422>)

**/3/**

SIMATIC NET  
TS Gateway (Version V3)  
Operating Instructions  
Siemens AG  
entry ID: 107535103 (<http://support.automation.siemens.com/WW/view/en/107535103>)

**/4/**

SIMATIC NET  
TeleControl Server Basic (Version V3)  
Operating Instructions  
Siemens AG  
entry ID: 46635999 (<http://support.automation.siemens.com/WW/view/en/46635999>)

**/5/**

SIMATIC NET  
Industrial Ethernet Security  
Basics and Application  
configuration manual  
Siemens AG  
Entry ID: 18701555 (<http://support.automation.siemens.com/WW/view/en/18701555>)

# Index

## A

Article number, 3  
Authorized phone number, 21

## C

CDMA, 12  
Communication with the CPU, configuration, 47  
Conditional spontaneous, 53  
Connection interrupted, 54  
Consistent data area, 18

## D

Data buffering, 18  
Data point configuration, 47  
Direct communication, 13, 23  
DNS, 44

## E

E-mail  
    Configuration, 86  
    Number of messages, 19  
    Programming (OUC), 91  
Events, 52

## F

Firmware version, 3  
Forced image mode, 51  
Frame memory, 18, 51

## G

Gateway, 63  
Glossary, 5

## H

Hardware product version, 3

## I

Image memory, 51  
IMEI, 3  
Importing a certificate - e-mail, 76  
Inserting/removing a SIM card, 36  
Instructions (OUC), 91  
Inter-station communication, 13, 22  
Inter-station communication - configuration, 72  
IP address - fixed, 59  
IP configuration, 14

## M

Messages, 86

## N

NTP, 64  
NTP (secure), 65  
IPsec tunnel,

## O

Online functions, 66  
OPC, configuration example, 22  
OUC (Open User Communication), 91

## P

Passive VPN connection establishment, 63  
Phone number of CP, 43  
PIN  
    Configuration, 43  
    Incorrect entry, 43  
Priority in the scan cycle, 50  
Program blocks, 13  
PUT/GET, 18

## R

Replacing a module, 111

## S

- S7 connections, 18
  - Enable, 66
- S7 data types, 47
- Safety notices, 33
- Security, 16
- Send buffer, 18, 51
- Server password, 56
- Service & Support, 6
- SIMATIC NET glossary, 5
- SMS
  - Configuration (telecontrol communication), 86
  - Number of messages, 19
  - Programming (OUC), 91
- SMTPS, 75
- SSL/TLS, 75
- STARTTLS, 75
- Status IDs - data points, 52
- STEP 7 version, 20

## T

- TCSB, 4
- TeleService gateway, 19
- TeleService via mobile wireless, 14
- Threshold value trigger, 78
- Time stamp, 18, 49
- Time-of-day synchronization, 15
- Training, 6
- Transmission mode, 53
- Trigger tag - resetting, 53, 86
- TS Gateway, 19, 127

## U

- Unsolicited, 53
- User data, 18

## V

- VPN, 19, 58

## W

- Web server
  - Access, 89
  - Diagnostics data, 106