SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-7 LTE

Operating Instructions

CP 1243-7 LTE-EU
CP 1243-7 LTE-US

02/2018
C79000-G8976-C381-04

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C381-04
℗ 02/2018 Subject to change

Preface

Validity of this manual

This document contains information on the following product:

- CP 1243-7 LTE-EU
  Article number 6GK7 243-7KX30-0XE0
  Hardware product version 2
  Firmware version V3.1
  Communications processor for connection of the SIMATIC S7-1200 via LTE, UMTS or GSM mobile wireless networks, European standard
- CP 1243-7 LTE-US

  Article number 6GK7 243-7SX30-0XE0
  Hardware product version 2
  Firmware version V3.1
  Communications processor for connection of the SIMATIC S7-1200 via LTE or UMTS mobile wireless networks, North American standard (AT&T certified)

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.

Abbreviations/acronyms

- **CP / submodule / module**

  Simplified designation of the CP 1243-7 LTE-EU / CP 1243-7 LTE-USCP 1243-7 LTE-EU / CP 1243-7 LTE-US

- **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 141).

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

Connection to SINEMA Remote Connect of the above firmware version

Replaced manual issue

Edition 04/2017

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 at the following address:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/man)

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

Cross references

In this manual there are often cross references to other sections.

To be able to return to the initial page after jumping to a cross reference, some PDF readers support the command <Alt>+<left arrow>.

Sources of information and other documentation

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

License conditions

Note

Open source software

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

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

- OSS_CP124x7_99.pdf

Security information

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

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

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

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information on industrial security measures that may be implemented, please visit
Link: (http://www.siemens.com/industrialsecurity)

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

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

Firmware

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

Recycling and disposal

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

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

Keep to the local regulations.

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

SIMATIC NET glossary

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 address:

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

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.

Table of contents

Application and functions

1

1.1 Connecting the S7-1200 to a mobile wireless network

The CP is intended for use in industrial environments.

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

  – UMTS

  – GSM

- **CP 1243-7 LTE-US**

  The CP is certifies by AT&T supports the following mobile wireless standards:

  – LTE

  – UMTS

  – GSM

You will find the supported frequency bands in the section Technical specifications (Page 141).

Unless explicitly stated differently in the following manual , the telecontrol communication relates to connections to a telecontrol server with the application TCSB (TeleControl Server Basic V3).

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. The following fallback behavior applies:

- CP 1243-7 LTE-EU: LTE → UMTS → GSM
- CP 1243-7 LTE-US: LTE → UMTS → GSM (if network exists)

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

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. You will find the link in the section Approvals (Page 147).

Communication types

The CP allows the following types of WAN communication:

- **Telecontrol communication**

  WAN communication between S7-1200 stations and the telecontrol server (TCSB) in the master station

- **Inter-station communication**

  Communication between stations and the master station (telecontrol communication)

- **Direct communication**

  Direct inter-station communication between stations (Open User Communication) via program blocks

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 / EDGE**

    (General Packet Radio Service)

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

    Note
    No CDMA

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

  – **UMTS / HSPA**

    (Universal Mobile Telecommunications System) / (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 73) and Messages (Page 107).

- 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 Security functions (Page 17).

Communication via SINEMA Remote Connect

Supported as of firmware version V3.1. See section Connection to SINEMA RC (Page 15).

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 16).

- 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 113).

You will find examples of applications in the section Configuration examples (Page 23).

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 CP supports the following functions:

- PUT / GET

  The CP supports the function as client (program blocks) and server for data exchange with remote stations (S7-300/400/1200/1500).

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 16).

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 23).

For more detailed information, refer to section Establishment of a TeleService connection (Page 137).

1.3 Connection to SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

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

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

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

For the CP firmware version required for communication via SINEMA RC see section Communications services (Page 13).

The CP can also handle telecontrol communication via the SINEMA RC server.

Parameter groups

You configure communication via SINEMA RC and telecontrol communication via SINEMA RC in two parameter groups:

- Communication via SINEMA RC:

  > "Security > VPN"

- Telecontrol communication via SINEMA RC:

  > "Communication types"

  For information on the supported protocols and configuration, see section Telecontrol via SINEMA RC (Page 55).

Applications

The following application options of the CP result from the combination of the parameters for telecontrol communication and SINEMA RC:

- (1) No telecontrol and no SINEMA RC (CP for network separation only)
- (2) CP only for remote maintenance via SINEMA RC
- (3) CP for telecontrol communication only
- (4) CP uses telecontrol communication, but SINEMA RC only for remote maintenance.
- (5) CP uses SINEMA RC for telecontrol communication and remote maintenance.

The table provides an overview of the applications with the respective parameter settings.

- "On" means that the parameter is activated.
- "Off" means that the parameter is deactivated.

Table 1- 1 Use cases and parameters to be activated

Use case	Parameter settings (Parameters abbreviated) *		
	SRC	TC	TC-SRC
(1)	Off	Off	Off
(2)	On	Off	Off
(3)	Off	On	Off
(4)	On	On	Off
(5)	On	On	On

* Explanation of the parameter abbreviations:

SRC - Security > VPN (activated) > "VPN connection type":
"Automatic OpenVPN configuration via SINEMA Remote Connect Server"

TC - Communication types > Telecontrol communication enabled

TC-SRC - Communication types >
"Activate telecontrol communication via SINEMA Remote Connect"

1.4 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**

  The CP supports various methods of time-of-day synchronization. You will find information in the section Time-of-day synchronization (Page 52).

  For information on the format of the time stamp, refer to the section Datapoint types (Page 91).

- **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.

- **Send buffer**

  The CP saves the values of data points configured as an event in the send buffer.

  The data is not saved retentively. It is lost in case of a power outage.

- **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

  e. g.

  – 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.

1.5 Security functions

Security functions of the telecontrol protocol

The CP supports the following security functions:

- **TeleControl Basic**

  – **Encrypted telecontrol communication**

    As an integrated (unconfigurable) security function, the TeleControl Basic protocol encrypts the data for transfer.

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

  - **Authorized phone numbers**

    To authorize nodes allowed to establish a connection to the CP (e.g. mobile phones), an authorized phone number is configured for each subscriber.

  - **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 to restrict flooding and DoS attacks ("Define IP packet filter rules")
  - Global firewall rules
- **VPN**

  The following alternatives can be used:
  - Secured communication via IPsec tunnels

    VPN communication allows the establishment of secure IPsec tunnels for communication with one or more security modules. The CP can be grouped together with other modules to form VPN groups during configuration. IPsec tunnels are created between all security modules of a VPN group.
  - Remote maintenance via SINEMA Remote Connect

    It is not necessary and not possible to create a VPN group for communication via a SINEMA RC server. The SINEMA RC Server manages the communication between the devices and the security mechanisms (OpenVPN).
- **Logging**

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

For information on configuring the security functions, refer to the section Security (Page 69).

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 160).

1.6 Configuration limits and performance data

Number of simultaneous connections for telecontrol communication

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

Number of simultaneous TeleService connections

- Max. 1 TeleService connection

Number of simultaneous connections for S7 communication and Open User Communication

A maximum total of 22 connection resources for S7 communication and Open User Communication (OUC)Open User Communication (OUC)

The maximum number can be divided up as follows into:

- S7 connections: Maximum 8
  - (PUT/GET)
- OUC connections Maximum 8
  - TCP connections
  - ISO-on-TCP connections
  - UDP connections
- Additional free resources for S7 or OUC connections: Maximum 6

Number of connections to NTP servers

- Max. 1 connection to an NTP server

Number of possible partners for inter-station communication

- Max. 13 CPs as partners for inter-station communication

  Of which:

  - Sending

    Max. 3 partners

    Note: In total along with the telecontrol server it is possible to send to max. 4 partners. The send buffer would divide itself up proportionately with 4 partners, i.e. 16000 event messages for each partner.

  - Receiving

    Max. 10 partners
- Partners can be S7-1200 CPs with data point configuration and use of the protocol "TeleControl Basic".

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 data points for the data point configuration

The maximum number of configurable data points is 200.

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 (Page 95).

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")

1.7 Requirements for operation

Hardware requirements

Apart from the CP. the following hardware is required in the S7-1200:

- CP

  The requirement for the firmware version V3 of the CP is a CP with hardware product version 2.

- A CPU with firmware version as of V3

  The full functionality of the CP is only available with a CPU as of V4.2.

- An external antenna for the CP

  Use only the antenna from the accessories program for the CP, refer to the appendix Antennas (Page 155).

- 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 156).

Configuration software

To use the full range of functions the following configuration tool is required to configure the module:

STEP 7 Basic V15

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" (TeleControl Server V3) 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 160) or /3/ (Page 160) in the References.

Requirements for using mobile wireless services

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

- Access point (Access Point)

  For the transition between the mobile wireless network and Internet you require an access point. The name of the access point (APN) and the access data are configured for the CP in STEP 7.

  Generally the mobile wireless network providers make an access point available.

  Note the information on APNs in the section Mobile wireless communications settings (Page 57).

1.8 Configuration examples

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

SMS messages and e-mails

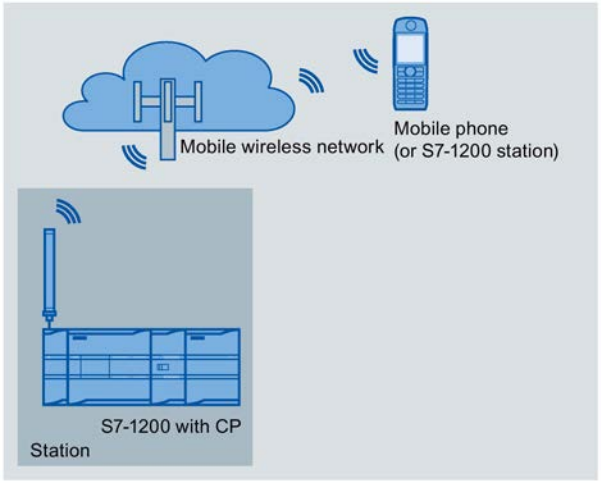


Figure 1-1 Sending messages by SMS from an S7-1200 station

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 Data point configuration (Page 84) and Messages (Page 107).

- 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 113), 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 127).

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 Data point configuration (Page 84), Messages (Page 107) and E-mail configuration (Page 73).

- 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 113), you will find the description of the programming in the STEP 7 information system.

If you want to use the secure transfer of e-mails, the CP must have the current time of day.

Telecontrol by a control center

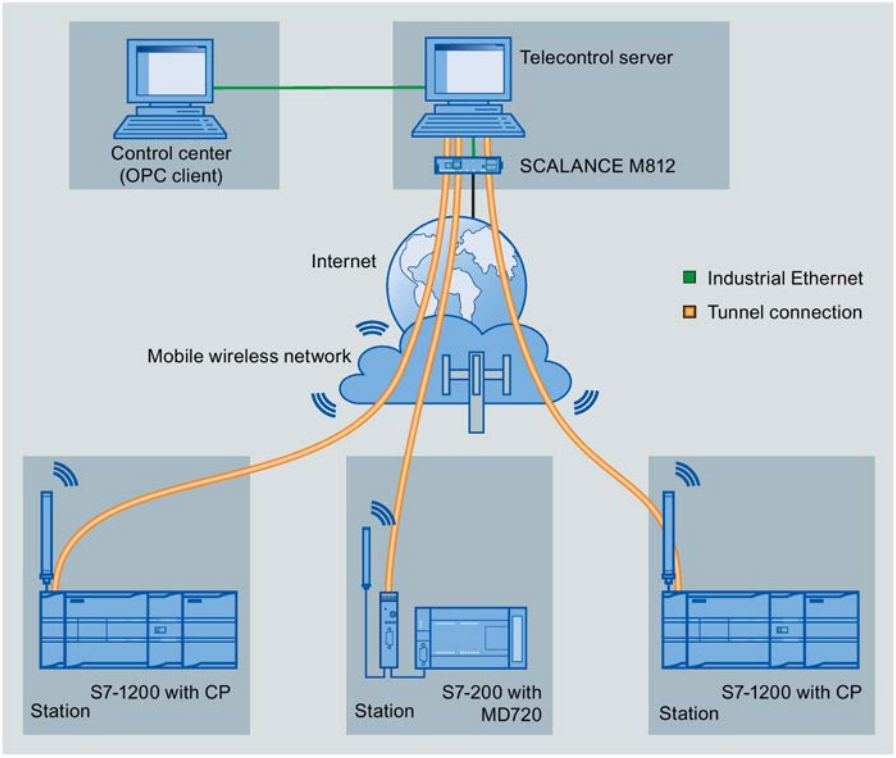


Figure 1-2 Communication between S7-1200 stations and a control center

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

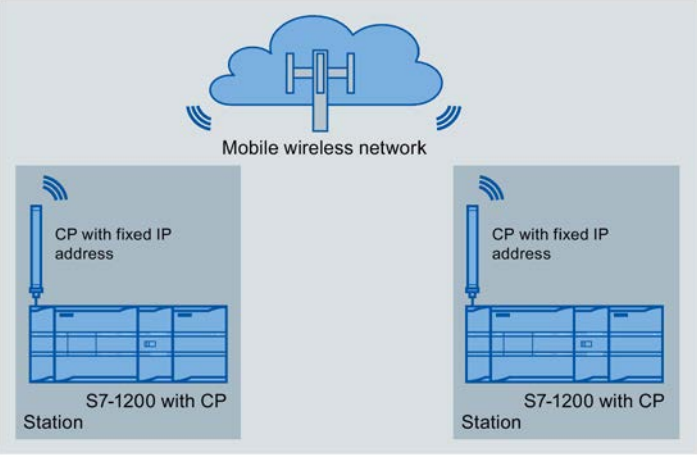


Figure 1-3 Direct communication between two S7-1200 stations

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.

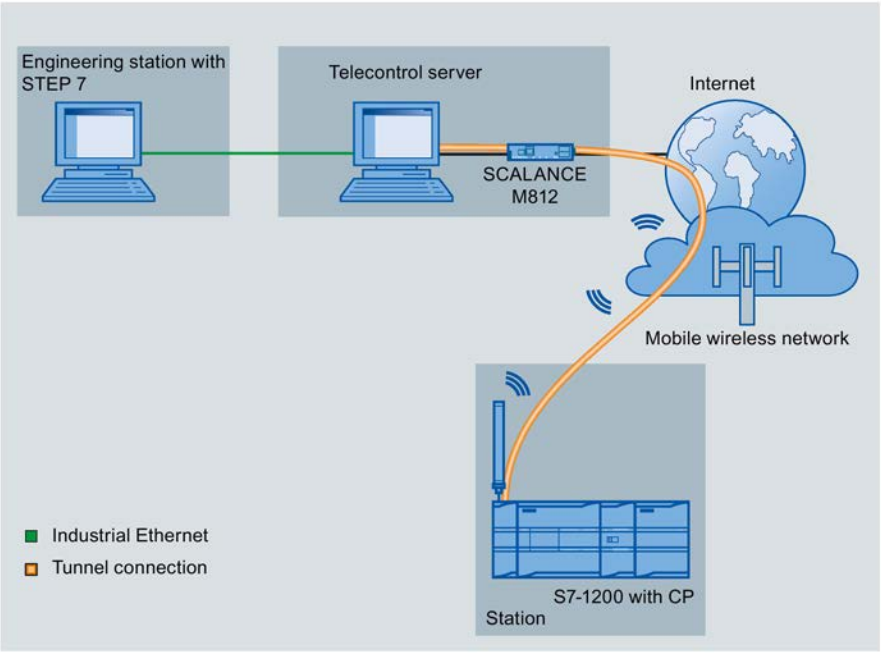


Figure 1-4 TeleService via the mobile wireless network in a configuration with telecontrol server

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.

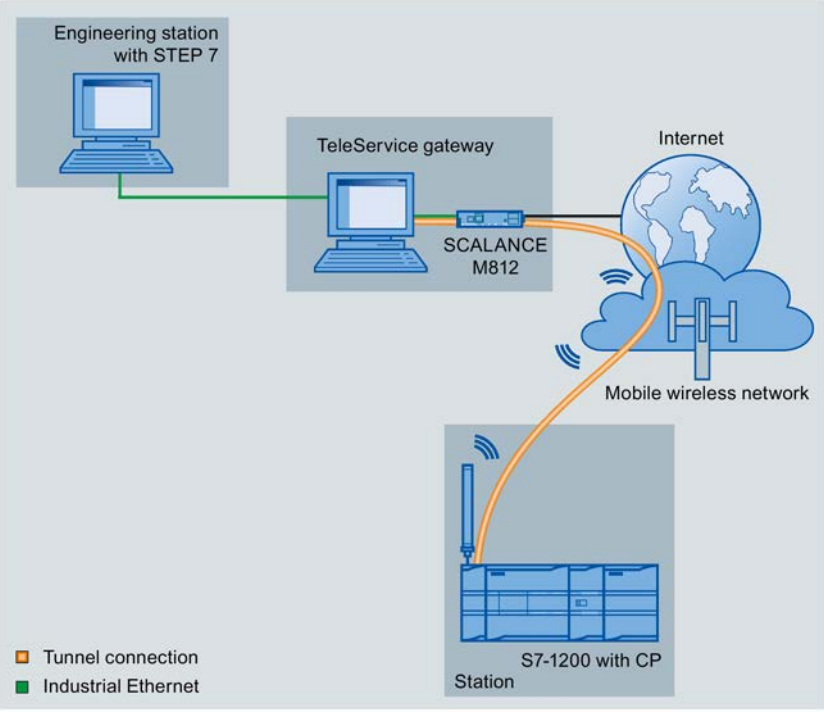


Figure 1-5 TeleService via the mobile wireless network with TeleService gateway - connection via LAN

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.

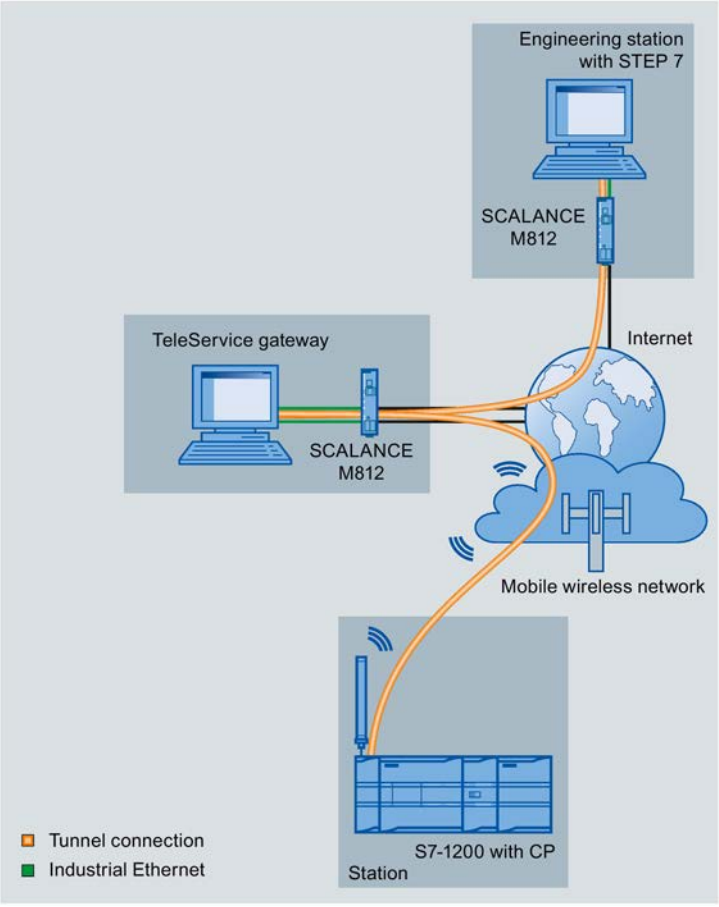


Figure 1-6 TeleService via the mobile wireless network with TeleService gateway - connection via the Internet

Remote maintenance with SINEMA RC

The following figure shows the connection of different stations with Security CP to an engineering station via SINEMA Remote Connect - Server.

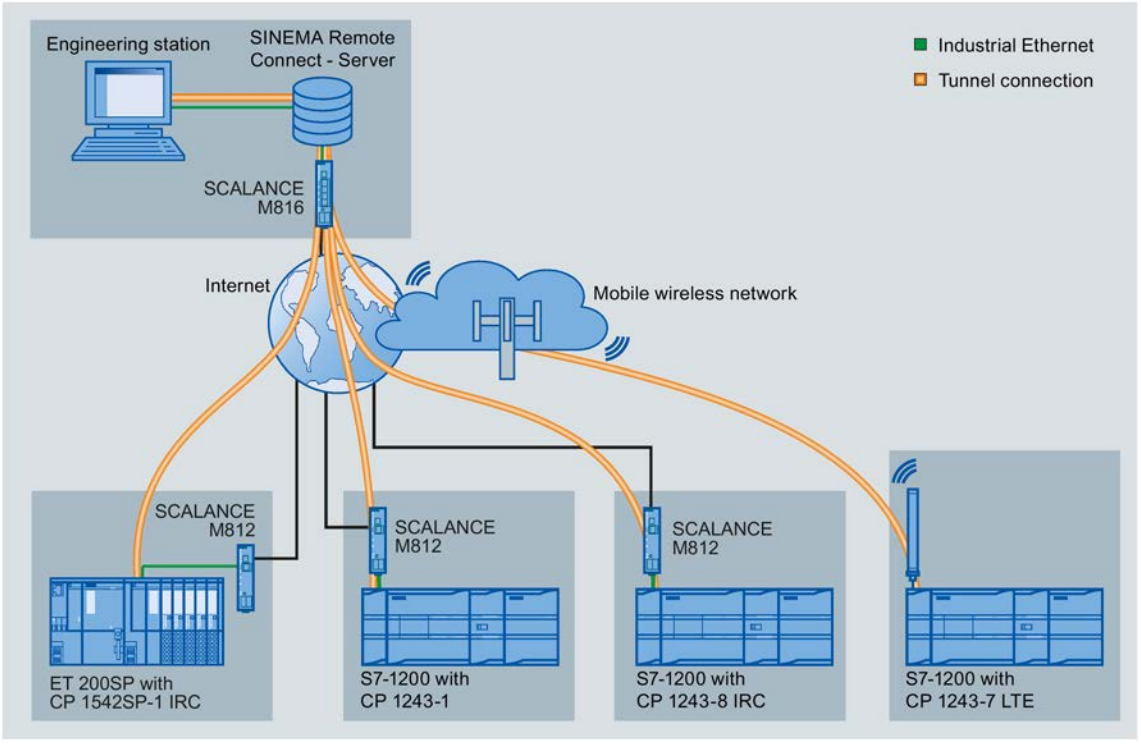


Figure 1-7 Connection of stations to engineering station via SINEMA RC

LEDs and connectors

2

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.

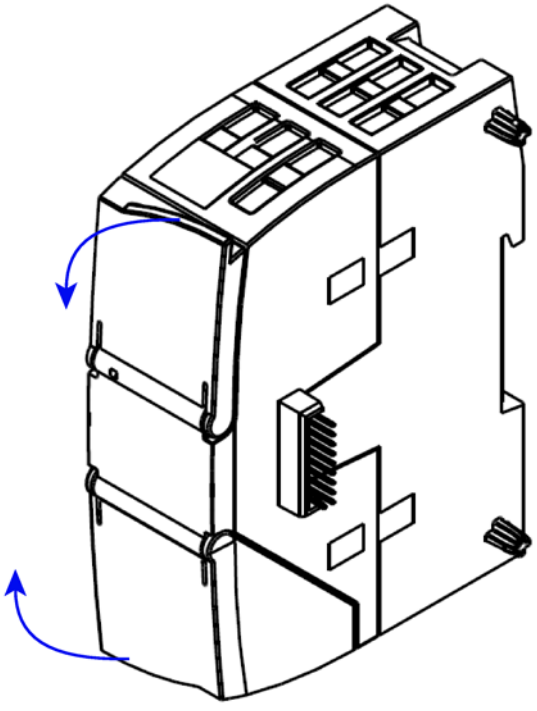


Figure 2-1 Opening the housing

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
red/green	DIAG	Basic status of the module

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

LED / colors	Name	Meaning
red/green	NETWORK	Status of the connection to the mobile wireless network
green	CONNECT	Status of the connection to the master station
yellow / green	SIGNAL QUALITY	Signal quality of the mobile wireless network
green	VPN	Status of the VPN or SINEMA Remote Connect configuration

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 (red / green)	**NETWORK** (red / green)	**CONNECT** (green)	**SIGNAL QUALITY** (yellow / green)	**VPN** (green)	**Meaning**
Display of the basic statuses of the module					
○	○	○	○	○	Power OFF
● red	●	●	●	●	Startup
☼ flashing red	-	○	-	-	Errors: • Invalid CP configuration or • CP type does not match the configuration data on the CPU.
● green	-	-	-	-	Running (RUN) without error
☼ flashing red	-	☼	-	-	Backplane bus error
☼ flashing red	●	-	-	-	Missing SIM card
☼ flashing red	☼	-	-	-	Missing or incorrect PIN
Connection to the mobile wireless network					
-	●	-	-	-	Existing connection to the service in the mobile wireless network
-	○	-	-	-	No connection to the service in the mobile wireless network
Connection to communications partners					
● green	●	●	-	-	Connection established to at least one partner, CPU in RUN
● green	●	☼	-	-	Connection established to at least one partner, CPU in STOP
☼ flashing green	●	●	-	-	No partner reachable, CPU in RUN
☼ flashing green	●	☼	-	-	No partner reachable, CPU in STOP

DIAG (red / green)	**NETWORK** (red / green)	**CONNECT** (green)	**SIGNAL QUALITY** (yellow / green)	**VPN** (green)	**Meaning**
flashing green	○	●	-	-	Telecontrol configuration exists, partner not reachable, CPU in RUN mode
flashing green	○	flashing green	-	-	Telecontrol configuration exists, partner not reachable, CPU in STOP mode
Quality of the mobile wireless connection					
-	-	-	●	-	Good network (-73 ... ≥ -51 dBm)
-	-	-	●	-	Medium strength network (-89 ... -74 dBm)
-	-	-	flashing yellow	-	Weak network (-109 ... -90 dBm)
-	-	-	○	-	No network (≤ -110 dBm)
flashing red	-	-	○	-	Missing external power supply
VPN/SINEMA Remote Connect connection					
-	●	-	-	●	VPN/SINEMA Remote Connect connection established
-	●	-	-	flashing green	Attempting to establish a configured VPN/SINEMA Remote Connect connection
-	-	-	-	○	VPN/SINEMA Remote Connect connection not configured or currently not established on the CP
Loading firmware					
flashing green / flashing red	flashing green	flashing green	flashing green	flashing green	Loading firmware. The "DIAG" LED flashes alternating red and green.
flashing green	flashing green	flashing green	flashing green	flashing green	Firmware was successfully loaded.
flashing red	flashing green	flashing green	flashing green	flashing green	• Error loading firmware or • Internal error of the CP; remedy: Power OFF → ON

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 144).

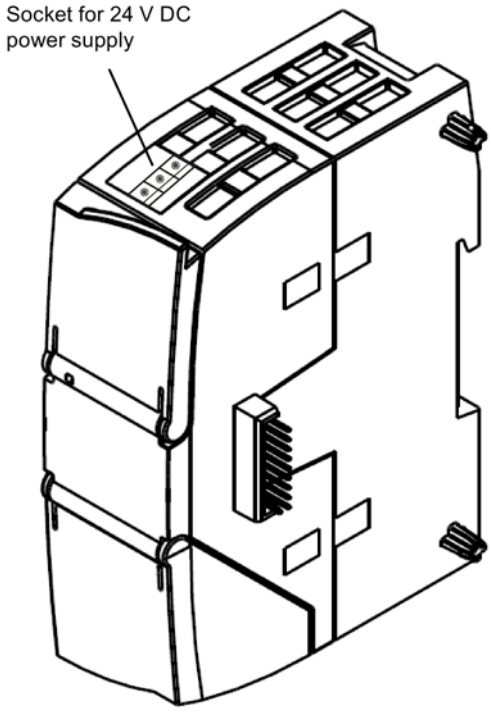


Figure 2-2 Socket for the 24 V DC power supply

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 the antenna permitted in the section Accessories (Page 155).

More detailed information on the electrical connections

For technical information on the electrical connections, refer to the section Technical specifications (Page 141).

Installation, connecting up, commissioning 3

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

NOTICE
Protection of the external power supply 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: DEHN+SOEHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt, Germany

3.1.1 Notices on use in hazardous areas

⚠ WARNING
EXPLOSION HAZARD DO NOT OPEN WHEN ENERGIZED.

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

WARNING

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.

WARNING

EXPLOSION HAZARD

DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.

WARNING

EXPLOSION HAZARD

SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.

WARNING

When used in hazardous environments corresponding to Class I, Division 2 or Class I, Zone 2, the device must be installed in a cabinet or a suitable enclosure.

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

WARNING

Requirements for the cabinet/enclosure

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

WARNING

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

WARNING

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

3.1.3 Notices regarding use in hazardous areas according to UL HazLoc

WARNING

EXPLOSION HAZARD

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, wiring and commissioning

Prior to installation and commissioning

WARNING

Read the system manual "S7-1200 Programmable Controller"

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 (Page 45)".

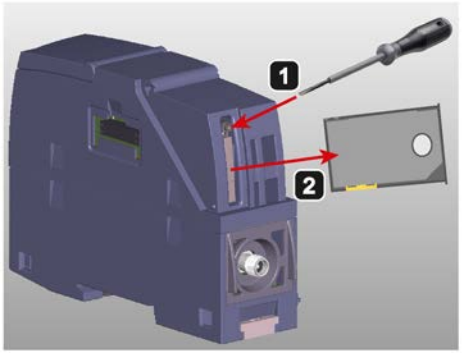
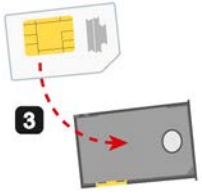
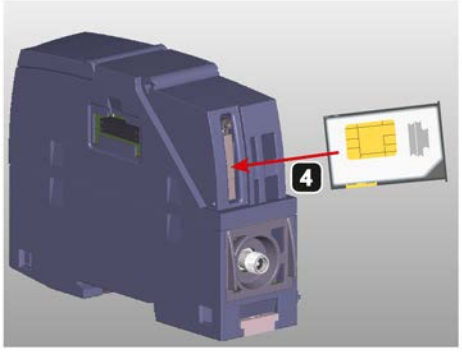
Inserting the SIM card

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

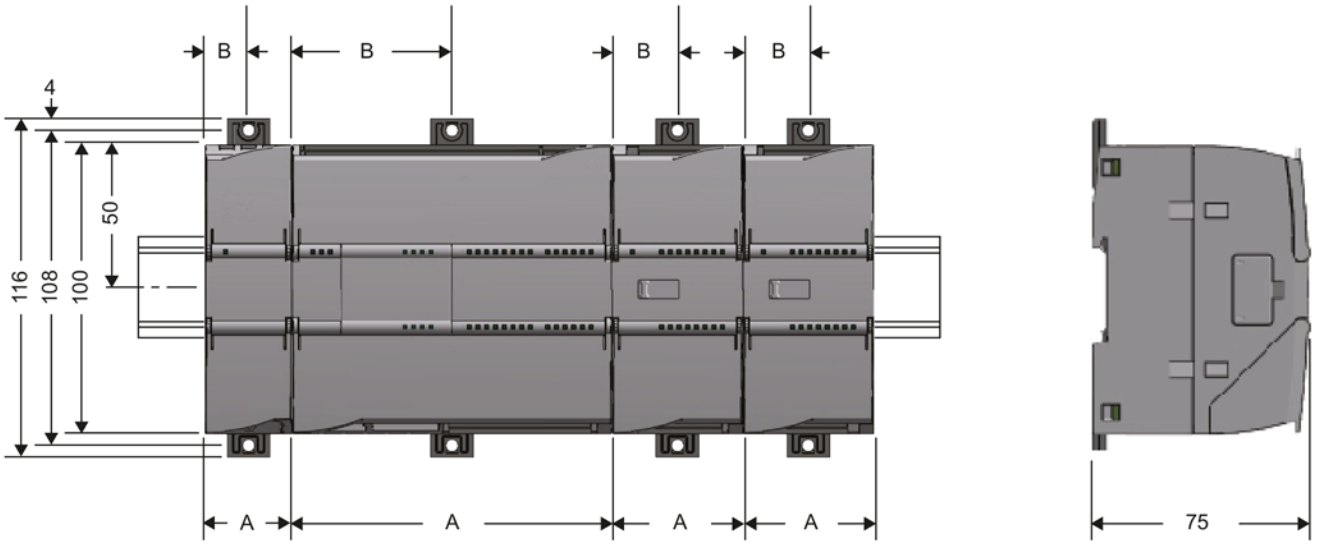


Figure 3-1 Dimensions for installation of the S7-1200

Table 3- 1 Dimensions for installation (mm)

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

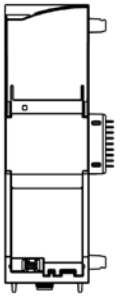
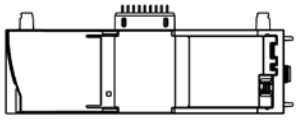
* Width B: The distance between the edge of the housing and the center of the hole in the DIN rail mounting clip

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

NOTICE
Installation location 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. 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 141).

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 141).

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. 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 144).
5	Connect the antenna to the SMA socket of the CP.	Lower surface of the CP
	Notice • Protect the antenna connector using suitable overvoltage protection equipment if the antenna cable is longer than 30 m. • Protect the antenna connector with suitable lightning protection if you install the antenna outdoors. • If you install several CPUs close to each other, keep to a minimum clearance of 50 cm between the antennas.	
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.	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. You will find more detailed information on loading in the following sections of the STEP 7 online help: • "Loading project data" • "Using online and diagnostics functions"

Note

Time synchronization for telecontrol via SINEMA RC

When using SINEMA Remote Connect for telecontrol communication, set the CPU time manually during commissioning; see note in section Telecontrol via SINEMA RC (Page 55).

3.3 Notes on operation

CAUTION

Minimum clearance to the device

The device may only be operated when the distance between the device (or antenna) and user is at least 20 cm.

NOTICE

Closing the front panels

To ensure interference-free operation, keep the front panels of the module closed during operation.

Configuration 4

4.1 Security recommendations

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

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
- Check regularly for new features on the Siemens Internet pages.
  - You can find information on Industrial Security here:
    Link: (http://www.siemens.com/industrialsecurity)
  - You can find information on security in industrial communication here:
    Link: (http://w3.siemens.com/mcms/industrial-communication/en/ie/industrial-ethernet-security/Seiten/industrial-security.aspx)
  - You can find a publication on the topic of network security (6ZB5530-1AP02-0BA5) here:
    Link:
    (http://w3app.siemens.com/mcms/infocenter/content/en/Pages/order_form.aspx?nodeKey=key_518693&infotype=brochures)
    Enter the following filter: 6ZB5530

Physical access

Restrict physical access to the device to qualified personnel.

APNs from mobile wireless providers.

If you configure an APN of the network provider for the mobile wireless CP, then - depending on the APN being used - it is possible that the CP can be reached publically on the Internet.

Remember this security risk when selecting the APN.

Security functions of the product

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

- Protection levels
  - Configure a protection level of the CPU.

    You will find information on this in the information system of STEP 7.
- Security function of the communication
  - Enable the Security functions of the CP.
  - Use the secure Open User Communication via the appropriate program blocks.
  - Disable access to the Web server of the CPU (CPU configuration) and on the CP.
- Protection of the passwords of program blocks

  Protect the passwords stored in data blocks for the program blocks from being viewed. The procedure is described in the STEP 7 information system.

  If you want to change parameters, for example a password, in a DB later, remember the following: The contents of a DB with know-how protection are no longer visible and can only be changed via the source or by direct assignment of parameters.
- Logging function

  Enable the function in the Security configuration and check the logged events regularly for unauthorized access.

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.

  See also the preceding section for information on this.
- Do not use one password for different users and systems.

Protocols

Secure and non-secure protocols

- Only activate protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.

  The NTP protocol provides a secure alternative with NTP (secure).

Table: Meaning of the column titles and entries

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

- **Protocol / function**

  Protocols that the device supports.

- **Port number (protocol)**

  Port number assigned to the protocol.

- **Default of the port**
  - Open

    The port is open at the start of the configuration.
  - Closed

    The port is closed at the start of the configuration.

- **Port status**
  - Open

    The port is always open and cannot be closed.
  - Open after configuration

    The port is open if it has been configured.
  - Open (login, when configured)

    As default the port is open. After configuring the port, the communications partner needs to log in.

- **Authentication**

  Specifies whether or not the protocol authenticates the communications partner during access.

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
S7 and online connections	102 (TCP)	Open when the function is enabled.	Open after configuration	No
Communication via SINEMA RC	8448 (TCP)	Closed	Open after configuration	Yes
HTTP	80 (TCP)	Closed	Open after configuration	Yes
HTTPS	443 (TCP)	Closed	Open after configuration	Yes

Ports of communications partners and routers

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

These can be:

- TeleControl Basic / 55097 (TCP) - can be set
- NTP / 123 (UDP)

- SMTP / 25 (TCP)
- DNS / 53 (UDP)
- SINEMA RC autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC

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 21).

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

  Call numbers of the nodes that can instigate connection establishment by the CP with an SMS message or call.
- 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 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 62).

- 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 Time-of-day synchronization

Synchronization method of the CP

Note

Time-of-day synchronization of the CP

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.

With security functions enabled, you need to enable time-of-day synchronization.

Note

Recommendation for setting the time

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

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

- **Time from partner**

  The CP adopts the time-of-day from the communications partner in the master station.

  Only when telecontrol communication is enabled.

- **NTP**

  The time of day is synchronized by an NTP server in the connected network.

  The method can also be used when the telecontrol communication is enabled.

  With CPs as of firmware version V3, the address of the NTP server can also be entered as a URL, e.g. <ntp.server.com>. For this a DNS server is required.

- **NTP (secure)**

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

  On the CP you specify the servers used.

  You configure NTP servers of the type NTP (secure) in the global security settings of STEP 7.

- **Time from the CPU**

  As of V4.2, the CPU synchronizes all CMs/CPs of the station with a synchronization cycle of 10 seconds.

  Parameters of the CPU:
  If for the CPU the option "CPU synchronizes the modules of the device" is enabled, all smart modules of the station (CPs with of firmware ≥ V2.1.77) are synchronized with the CPU time in a synchronization cycle of 10 seconds.

Parameter groups for time-of-day synchronization

You can configure time-of-day synchronization in the following parameter groups:

- **Ethernet interface**

  Here you create the configuration under the following conditions:

  – Telecontrol communication is disabled.

  – The security functions are disabled.

- **Security**

  Here you create the configuration under the following condition:

  – The security functions are enabled.

Dependence of the synchronization method on the use of the CP

Depending on the use of the telecontrol communication or the security functions, the following synchronization methods can be selected:

- **Telecontrol communication disabled, security disabled**
  – NTP
  – Time from the CPU
- **Telecontrol communication disabled, security enabled**
  – NTP
  – NTP (secure)
  – Time from the CPU
- **Telecontrol communication and security enabled**
  – Time from partner
  – NTP
  – NTP (secure)
  – Time from the CPU

Time-of-day synchronization with the S7-1200

When using an external time source, the S7-1200 station can obtain the current time of day both via the CPU as well as via a CP.

With the S7-1200 there is no forwarding of the time of day from the station to the subnet.

Note

Recommendation: Time-of-day synchronization only by 1 module

Only have the time of day of the station from an external time source synchronized by a single module so that a consistent time of day is maintained within the station.

When the CPU takes the time from the CP, disable time-of-day synchronization of the CPU.

Time-of-day synchronization of the CPU

The following synchronization methods are possible for the CPU:

- **NTP**

  Only this option can be configured actively for the CPU:

- **Time from CP**

  The CPU adopts the time of day from a CP of the station if time forwarding from the CP to the CPU is enabled (see below).

Forwarding the time from the CP to the CPU

Note

Forwarding the time to the CPU

Depending on the firmware version of the modules involved, the time-of-day of the CP is forwarded to the CPU in different ways:

- Optional forwarding of the CP time to the CPU using a PLC tag
- Obligatory forwarding of the CP time to the CPU via the backplane bus

The forwarding of the CP time to the CPU depends on the firmware version of the CP and the CPU. Note the following behaviour.

- **CP firmware ≤ V2.1.6x**

  With this firmware version the CP can make the time-of-day available to the CPU as an option via a PLC tag. When this PLC tag is read cyclically by the CPU, the CPU adopts the CP time.

  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. For TLC tags, see parameter group "Communication with the CPU" of the CP.

- **CP firmware ≥ V2.1.77 and CPU firmware ≥ V4.2**

  If both modules in the station have the named firmware versions, the time of day of the CP is automatically forwarded to the CPU.

  Since the CPU automatically adopts the CP time, you no longer require the forwarding option using the PLC tag.

  If for the CPU the option "CPU synchronizes the modules of the device" is enabled in "PROFINET interface > Time synchronization", all smart modules of the station are synchronized with the CPU time.

4.5 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.

  To use telecontrol communication, the you also need to enable the security functions.

  For telecontrol communication via SINEMA Remote Connect see the section Telecontrol via SINEMA RC (Page 55).

  To use TeleService via the mobile wireless network you need to enable this function.

- **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.

  To use TeleService via the mobile wireless network you need to enable this function.

- **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.

- **Enabling SMS**

  On the CP enable the receipt and sending of SMS meesages.

  The function can be enabled regardless of whether telecontrol communication is enabled.

Open User Commmunication 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.

4.6 Telecontrol via SINEMA RC

For information on possible applications of communication via SINEMA Remote Connect, see section Connection to SINEMA RC (Page 15).

Requirements

Configure the SINEMA Remote Connect - Server before configuring the CP (not in STEP 7). The CP and the communication partner of the CP must be configured in the SINEMA RC Server.

Supported telecontrol protocols

The following protocols support communication via SINEMA Remote Connect:

- TeleControl Basic
- DNP3
- IEC 60870-5-104

Configuration of the telecontrol communication via SINEMA Remote Connect

Follow the steps below when configuring the CP for use of telecontrol communication via SINEMA RC:

1. In the "Communication types" parameter group activate telecontrol communication and select the protocol.

   The option for communication via SINEMA RC is not yet visible.

2. Change to the "Security" parameter group and enable the security functions.

   (In the "Communication types" parameter group the SINEMA RC option appears disabled and grayed out)

3. Open the "Security > VPN" parameter group and enable VPN.
4. For the parameter "VPN connection type" select the option "Automatic OpenVPN configuration via SINEMA Remote Connect Server" if this is not preset.

   (In the "Communication types" parameter group the SINEMA RC option becomes usable.)

5. Change to the "Communication types" parameter group and enable the option "Telecontrol communication via SINEMA Remote Connect".
6. Create the remaining configuration of the SINEMA RC connection of the CP under "Security > VPN".

   For information on the configuration, see section SINEMA Remote Connect (Page 79).

Manual setting the time of day during commissioning

Note

Time synchronization for telecontrol via SINEMA RC

When using SINEMA Remote Connect for telecontrol communication, the communication module needs the current time for authentication on the SINEMA RC Server. The module receives the time from the CPU or from an NTP server before the connection is established for the first time.

Recommendation:

During commissioning, set the time of the CPU manually at least once using the STEP 7 online functions. This is necessary especially if you have configured the "Time from partner" option for the time synchronization. In this way, you ensure that the CPU has a valid time of day when the station starts up and that the CP can exchange the required certificates with the SINEMA RC Server.

4.7 Mobile wireless communications settings

"Mobile wireless settings"

In this parameter group you configure the following parameters:

- **CP phone number**

  Telephone number of the CP

- **Activate PIN**

  If your service provider requires a PIN, enable this option.

- **PIN**

  PIN of the SIM card

- **Enable data services**

  Activates the use of the data services in the mobile wireless network for the CP.

  Note
  Subsequent disabling

  If you have already used data services in operation and then disable them later, you need to reload the configuration data and change the CPU to STOP and then RUN.

- **GPRS (2G) / UMTS (3G) / LTE**

  Enable the mobile wireless service(s) you want to use. You can enable individual mobile wireless services or all of them.

- **SMSC**

  Phone number of the SMS center (Short Message Service Center)

  The box has the following options:

  – No number

    As default, the CP adopts the SMSC data of the service provider directly from the inserted SIM card. if you want to use the SMSC number of the SIM card, leave the box empty.

  – Configured number

    If you want to use a different SMSC, enter the phone number of this SMSC.

    Note the following:

    Note
    Permanent storage of the SMSC number

    If you configure an SMSC number, the CP no longer accesses the SMSC data of the SIM card. This is also the case if you delete the SMSC number from the configuration again.

    Recommendation:
    When you configure an SMSC number, first note down the SMSC number of your service provider located on the SIM card. If you want to use it again later, you can then use the SMSC of your provider again by configuring the SMSC number.

"APN settings"

In this parameter group, you configure the data of the access point. You require the APN to send e-mails.

Note the information on security in the section Requirements for operation (Page 21).

By entering your country in the "Country" box, you can select one of the preset APNs from the drop-down list.

Alternatively configure the APN manually.

The CP supports APNs with IPv4 address.

User names and passwords can contain up to 64 characters. You will find the characters permitted in the section Permitted characters in the configuration (Page 110).

"List of preferred networks"

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

"TeleService settings"

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

You will find an overview of configuration for TeleService and more information on this topic in the section TeleService (Page 135).

4.8 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 addresses

Enter you configure IP address of the CP and, if applicable, the network connection.

If you enable security functions, for example when using telecontrol communication, for reasons of consistency you need to network the CP. To do this create any Ethernet network.

- 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 receiving data via Open User Communication.

Time-of-day synchronization

For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 52).

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 62).

(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 TCP connection monitoring time, the CP sends a keepalive to the communications partner.

  Default setting: 180 s. Permitted range: 1...65535 s.

  – **The parameter below the Ethernet interface**

    The monitoring time is configured for the Ethernet interface globally for all TCP connections. The parameter is preset to 180 seconds as default.

  – **The parameter below "Partner stations"**

    The parameter "TCP connection monitoring time" occurs again with the individual partners in the parameter group "Connection to partner". This parameter applies only to the individual partner. The value of 180 seconds preset on the Ethernet interface is adopted for the individual partners.

    If for any reason you want to change the value of the TCP connection monitoring time for individual partners, you can adapt the value for every partner individually in "Partner stations". If. for example, you want to check the connection at shorter intervals, reduce the value. If disruptions or delays occur often when transferring in your mobile wireless network, it may be advisable to increase the value.

- **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.

  Default setting: 180 s. Permitted range: 1...65535 s.

  – **The parameter below the Ethernet interface**

    The monitoring time is configured for the Ethernet interface as a global setting for all TCP connections.

  – **The parameter below "Partner stations"**

    As with the TCP connection monitoring time, the value of "Partner stations" can be adapted for each partner individually.

Advanced options > Transmission settings

- **Connection establishment 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.

  Default setting: 10 s. Permitted range of values for the basic value: 10...300 s

  Example:
  A configured 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 monitoring time**

  Time for the arrival of the acknowledgment from the partner (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.

  Default setting: 60 s. Permitted range: 1...65535 s.

- **Watchdog monitoring time**

  With the watchdog cycle, the CP checks the connection to the telecontrol server. The watchdog cycle is the interval without data exchange between the CP and telecontrol server after which the CP sends a watchdog frame to the telecontrol server. The watchdog cycle is only configured with TCSB (parameter "Keepalive monitoring time"). The value configured in TCSB is transferred by the telecontrol server to the CP the first time the connection is established.

  Each time the CP transfers data to TCSB and receives the acknowledgment from the telecontrol server, the CP starts the watchdog cycle. When the watchdog cycle has expired the CP sends a watchdog frame to the telecontrol server.

  After sending a watchdog frame, the CP starts the watchdog monitoring time within which the CP expects a reply from the telecontrol server. If the CP does not receive a reply from the Telecontrol server within the monitoring time, it terminates and re-establishes the connection.

  Default setting: 30 s. Permitted range: 0...65535 s. If you enter 0 (zero), the function is disabled.

- **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.

  Default setting: 8 s. Permitted range: 0...65535 s. If you enter 0 (zero), the function is disabled.

4.8.1 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 CP, you have access to the Web server of the CPU.

From a PC you can access the Web server of the station via TCSB if the PC is connected to the telecontrol server via LAN.

For the requirements, refer to the manual /4/ (Page 160).

With slow transmission paths between telecontrol server and station, make sure that you set the update time of the Web browser suitably low.

4.9 Partner stations

The parameter group is only displayed when telecontrol communication is enabled.

4.9.1 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 or host name (FQDN) of the telecontrol server. This can, for example, also be the FQDN of a DynDNS service.

  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**

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

  Default setting: 180 s. Permitted range: 1...65535 s.

  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 58).

You will find information on the acknowledgment of messages in the section "Acknowledgment (Page 64)".

– **The parameter below the Ethernet interface**

  The monitoring time is configured for the Ethernet interface globally for all TCP connections. The parameter is preset to 180 seconds as default.

– **The parameter below "Partner stations"**

  The parameter "TCP connection monitoring time" occurs again with the individual partners in the parameter group "Connection to partner". This parameter applies only to the individual partner. The value of 180 seconds preset on the Ethernet interface is adopted for the individual partners.

  If for any reason you want to change the value of the TCP connection monitoring time for individual partners, you can adapt the value for every partner individually in "Partner stations". If. for example, you want to check the connection at shorter intervals, reduce the value. If disruptions or delays occur often when transferring in your mobile wireless network, it may be advisable to increase the value.

- **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.

  Default setting: 10 s. Permitted range: 1...65535 s.

  – **The parameter below the Ethernet interface**

    The monitoring time is configured for the Ethernet interface as a global setting for all TCP connections.

  – **The parameter below "Partner stations"**

    As with the TCP connection monitoring time, the value of "Partner stations" can be adapted for each partner individually.

- **Connection mode**

  In the "Permanent" connection mode, there is a permanent connection to the communications partner.

  The CP only supports this connection mode.

  For information on connection establishment, refer to the section "Connection establishment (Page 65)".

- **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.

4.9.2 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.

4.9.3 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 58).

  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.

4.9.4 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 106).

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

Activate the option for enabling inter-station communication.

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 send buffer is shared by all communications partners.

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

4.10 DNS configuration

Configuring DNS servers

Configure a DNS server that can be reached in the network if the module itself or a communications partner is to be reachable using a host name. The communications partners also include NTP servers configured via an FQDN.

Configuration options:

- No configuration of a DNS server

  If you do not specify an address, DNS server addresses are obtained automatically from the provider of the mobile wireless network (recommended procedure). The requirement is that the network provider operates a DNS server in the network.

- Configuration of a DNS server

  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.

The addresses of the DNS servers can be configured in the IPv4 or IPv6 format.

4.11 Communication with the CPU

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

Communication with the CPU

Using the first three parameters you specify settings for the cyclic access of the CP to the CPU. You will find information on the structure of the scan cycle in the section Read cycle (Page 93).

- **Cycle idle time**

  Waiting time between two scan cycles of the CPU memory area

- **Max. number of write jobs**

  Maximum number of write jobs to the CPU memory area within a CPU scan cycle

- **Max. number of read jobs**

  Maximum number of low-priority read jobs from the CPU memory area within a CPU scan cycle.

- **Frame memory size**

  Here, you set the size of the frame memory for events (send buffer).

  The size of the frame memory is divided equally among all communications partners. You will find the size of the frame memory in the section Configuration limits and performance data (Page 19).

  You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Process image, type of transmission, event classes (Page 95).

Watchdog bit

- **CP monitoring**

  Via the watchdog bit the CPU can be informed of the status of the telecontrol communication of the CP.

CP time

- **CP time to CPU**

  Using this function, the CP can synchronize the CPU clock.

  You will find details in the STEP 7 information system.

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:

  Note

  Fast setting of the diagnostics trigger variable

  Triggers must not be set faster than a minimum interval of 500 milliseconds.

- **Frame memory 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.

- **Frame memory size**

  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.

  Meaning of the values (decimal)

  – 0 = Booked out of the network
  – 1 = Wrong PIN
  – 2 = Wrong, defective SIM card or not plugged in.
  – 3 = Waiting for PIN / no PIN configured
  – 4 = Booked into the 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.

- **TeleService status**

  The PLC tag (BOOL) indicates whether a TeleService session is active.

  – 0 = No TeleService session active

  – 1 = TeleService session active

- **VPN status**

  The PLC tag (BOOL) indicates whether a VPN tunnel is established:

  – 0 = No VPN tunnel established

  – 1 = VPN tunnel established

- **Connection to SINEMA Remote Connect**

  The PLC tag (BOOL) indicates whether there is a connection to the SINEMA RC server:

  – 0 = No connection established

  – 1 = Connection established

4.12 Security

Note the range and application of the security functions of the CP, refer to the section Security functions (Page 17).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 70).

4.12.1 Security user

Creating a security user

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

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

1. Create a user with the associated parameters such as authentication mode, session duration, etc.
2. Assign this user the role "NET Standard" or "NET Administrator" in the area below "Assigned roles".

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

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

Parameter groups

If security functions are enabled, you will find the following parameter groups here:

- **CP identification**

  Here, you configure parameters for authenticating the CP with the telecontrol server.

  You will find details below.

- **Time-of-day synchronization**

  For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 52).

- **Authorized phone numbers**

  You will find details below.

- **E-mail configuration**

  You will find details below.

- **Certificate manager**

  You will find details below.

- **Firewall**

  You will find details below.

- **Log settings**

  Here you make the settings for logging events relevant for security.

  You will find details below.

- **VPN**

  Here you configure the VPN communication.

  You will find details below.

In the global security settings of STEP 7 among other things you will find the following parameter groups:

- **VPN groups**

  Here you configure the VPN groups.

- **User management**

  Here you configure the users, roles and rights of the security users.

  This is for example necessary for TeleService access, see section TeleService (Page 135).

4.12.2 CP identification

In the "CP identification" parameter group, you configure the following information for authenticating the CP with the telecontrol server:

- Project number

  The project number is the same for all telecontrol CPs in a STEP 7 project. TCSB evaluates project numbers from 1 ... 2000.

  If you change the project number, this parameter is changed for all CPs in the STEP 7 project.

- Station number

  For each S7-1200 station with a telecontrol CP, an individual station number is configured. TCSB evaluates station numbers from 1 ... 8000.

- Telecontrol password

  Password for the authentication of the CP on the telecontrol server

  8 ... 29 characters of the ASCII character set 0x20...0x7e

  The password can be the same for all CPs of the STEP 7 project. The same password is configured in TCSB for this station.

- Access ID

  The displayed Access ID is formed from the hexadecimal values of project number, station number and slot. The parameter of the type DWORD is allocated as follows:

  – Bits 0 - 7: Slot

  – Bits 8 to 20: Station number

  – Bits 21 to 31: Project number

See also

Permitted characters in the configuration (Page 110)

4.12.3 Firewall

4.12.3.1 Pre-check of messages by the MAC firewall.

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.

4.12.3.2 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.

4.12.3.3 Firewall settings for configured connection connections via a VPN tunnel

IP rules in advanced firewall mode

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

In advanced firewall mode ("Security > Firewall > IP rules") select the action "Allow*" for both communications directions of the VPN tunnel.

See section Settings for online security diagnostics and downloading to station with the firewall activated (Page 72) for information on this.

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

Setting the firewall for online functions

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

1. In the global security settings (see project tree), select the entry "Firewall > Services > Define services for IP rules".
2. Select the "ICMP" tab.
3. Insert a new entry of the type "Echo Reply" and another of the type "Echo Request".
4. Now select the CP in the S7 station.

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

4.12.4 Authorized phone numbers

SMS messages received only from subscribers with an authorized phone number

The CP only accepts an SMS if the sending communication partner is authorized based on its phone number. These phone numbers are configured for the CP in STEP 7 in the "Authorized phone numbers" list in the Security settings.

"Authorized phone numbers"

A phone number entered here gives the sender who transfers this phone number the right to trigger connection establishment by the CP.

- If only an asterisk (*) is entered in the list, the CP accepts SMS messages from all senders.
- An asterisk (*) after a phone number body authorizes connection establishment for all nodes connected to the body (extension numbers).

  Example: +49123456* authorizes +49123456101, +49123456102, +49123456207 etc.

If the "Authorized phone numbers" list is empty, the CP cannot be induced to a connection establishment by a mobile phone.

4.12.5 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 the message editor ("Messages" entry in STEP 7), you configure the individual e-mails, see section Messages (Page 107).

E-mail configuration

If you want to use the secure transfer of e-mails, the module must have the current date and the current time of day.

With the default setting of the SMTP port 25, the module 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 module 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 module 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.

Use the certificate by taking the following steps:

1. Save the certificate of your e-mail service provider in the file system of the engineering station.
2. Import the certificate into your STEP 7 project with "Global security settings > Certificate manager".
3. Use the imported certificate with every module that uses encrypted e-mails via the "Certificate manager" table in the local "Security“ parameter group.

For the procedure, refer to the section Certificate manager (Page 82).

See also

Permitted characters in the configuration (Page 110)

4.12.6 Log settings - Filtering of the system events

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

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

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

4.12.7 VPN

4.12.7.1 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 handled unrestricted through a physical network. This allows networks to be connected together via an intermediate network.

VPN tunnels ensure integrity and confidentiality during data transmission.

Properties

- VPN forms a logical network that is embedded in a physical network. VPN uses the usual addressing mechanisms of the physical network, however it transports only the frames of the VPN subscribers and therefore operates independent of the rest of the physical network.
- VPN allows communication of the subscribers in the VPN network with the physical network.
- VPN is based on tunnel technology and can be configured for individual subscribers.
- 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)
- Protection of computers and their communication within and automation network
- Secure remote access from a PC/PG to automation devices or networks protected by security modules via public networks.

4.12.7.2 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.

4.12.7.3 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 this user.
2. Enable the "Activate security features" option
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.

Select "Activate security features"

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.

4.12.7.4 Communications partners in a VPN group

Configuring communications partners

If a node is intended to communicate with several CPs via VPN connections, all communications partners must be assigned to the same VPN group.

The CP itself can only communicate with a single communications partner via VPN.

4.12.7.5 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.

4.12.7.6 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 parameter group "VPN“ in the local security settings.
4. For each VPN connection with the CP as a passive VPN subscriber, change the default setting "Initiator/Responder" to the setting "Responder".

4.12.7.7 SYSLOG

Use of SYSLOG only with 1 VPN connection

If you want to use SYSLOG with level 7 (debug) via Vpn connections, this is only possible with a single established VPN connection.

4.12.7.8 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect - Server

  Configure SINEMA RC - Server as necessary (not in STEP 7). The communication module and its communication partners must be configured in the SINEMA RC Server.

- Exporting the CA certificate (optional)

  If you want to use the server certificate as authentication method of the communication module during connection establishment, export the CA certificate from SINEMA RC - Server. Then import the CA certificate from SINEMA RC - Server to the engineering station.

  Alternatively, you can use the fingerprint of the server certificate as authentication method of the communication module.

Note

Recommended authentication method:

The recommended authentication method is the one using the CA certificate. The certificate is valid for 10 years.

The fingerprint, on the other hand, is derived from the server certificate. Its validity may be significantly shorter.

Configuration of SINEMA Remote Connect

Importing your own certificate

1. Navigate to the parameter group "Security > Certificate manager".
2. Open the certificate selection with a double-click on the first free table row of the local certificate manager.
3. Select the CA certificate of SINEMA RC - Server.

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

VPN > General

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

   If you select "Internet Key Exchange (IKE) ...", you can use communication via IPsec tunnels.

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- CA Certificate

  Under "CA certificate" select the CA certificate from SINEMA RC - Server that was previously imported and activated in the local certificate manager.

  The module generally checks the CA certificate of the server and its validity period. The two options cannot be changed.

- Fingerprint

  When you select this authentication method, you enter the fingerprint of the server certificate of SINEMA RC - Server.

Authentication

- Device ID

  Enter the device ID generated for the module in SINEMA RC.

- Device password

  Enter the device password of the module configured in SINEMA RC.

  Max. number of characters: 127

Optional settings

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

- **Update interval**

  With this parameter you set the interval at which the CP queries the configuration on the SINEMA RC Server.

  Note that with the setting 0 (zero) changes to the configuration of the SINEMA RC Server may result in the CP no longer being capable of establishing a connection to the SINEMA RC Server.

- **"Connection type"**

  The two options of the parameter have the following effect on the connection establishment:

  – Auto

    The module establishes a connection to the SINEMA RCServer. The OpenVPN connection is retained until the connection parameters are changed by the SINEMA Remote Connect Server. If the connection is interrupted, the CP automatically re-establishes the connection.

    If the connection parameters are changed by the SINEMA Remote Connect Server, the CP requests the new connection data after the update interval configured above has elapsed.

  – PLC trigger

    The option is intended for sporadic communication of the module via the SINEMA RC Server.

    You can use this option when you want to establish temporary connections between the module and a PC. The temporary connections are established via a PLC tag and can be used in servicing situations, for example.

- **PLC tag for connection establishment**

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

  When the PLC tag is reset to 0, the connection is terminated again.

4.12.8 Certificate manager

Assignment of certificates

If you use communication with authentication for the module, for example SSL/TLS for secure transfer of e-mails, certificates are required. You need to import certificates of non-Siemens communications partners into the STEP 7 project and download them to the module with the configuration data:

1. Import the certificates of the communications partners using the certificate manager in the global security settings.
2. Then assign the imported certificates to the module in the table below the local security settings of the module.

For a description of the procedure, refer to the section Handling certificates (Page 82).

You will find further information in the STEP 7 information system.

4.12.9 Handling certificates

Certificate for authentication

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

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

Note

No certificate with security functions disabled.

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

For the secure transfer of e-mails via SSL/TLS and SSL certificate is created for the CP. It is visible in STEP 7 in "Global security settings > Certificate manager > Device certificates". The table "Device certificates" shows the issuer, validity, use of a certificate (service/application) and the use of a key. You can call up further information about a certificate by selecting the certificate in the table and selecting the shortcut menu "Show". The table also shows all other certificates generated by STEP 7 and all imported certificates.

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

1. Importing third-party certificates from communications partners

   ⇒ Global security settings of the project (certificate manager)

2. Assigning certificates locally

   ⇒ Local security settings of the CP ("Certificate manager" table)

These two steps are described in the next two sections.

Importing third-party certificates from communications partners

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

1. Save the third-party certificate in the file system of the PC of the connected engineering station.
2. In the STEP 7 project open the global certificate manager:

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

Assigning certificates locally

To be able to use an imported certificate for the CP, you need to specify it in the "Security" parameter group of the CP. Follow the steps outlined below:

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

   The "Certificate manager" table of the Global security settings is displayed.
4. In the table. select the required third-party certificate and to adopt it click the green check mark below the table.

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

Only now will the third-party certificate be used for the CP.

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

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

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

1. In the STEP 7 project open the global certificate manager:

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

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

Certificate for logging server

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

Change certificate: Subject Alternative Name

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

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

4.13 Data point configuration

4.13.1 Data point configuration

Data point-related communication with the CPU

No program blocks need to be programmed for telecontrol modules with data point configuration to transfer user data between the station and communications partner.

The data areas in the memory of the CPU intended for communication with the communications partner are configured data point-related on the module. Each data point is linked to a PLC tag or the tag of a data block.

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

PLC tags or DBs must first be created on the CPU 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 the can be used for data point configuration in the section Configuration limits and performance data (Page 19).

The formats and S7 data types of the PLC tags that are compatible with the protocol-specific data point types of the module can be found in the section Datapoint types (Page 91).

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 module.

Data received from the communications partner is written by the module 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 data point and message editor. You can open both editors alternatively as follows:

- Selecting the communication module

  Shortcut menu "Open the data point and messages editor"

- Via the project navigation:

  Project > directory of the relevant station > Local modules > required communication module

  By double-clicking on the entry, the data point or message editor opens.

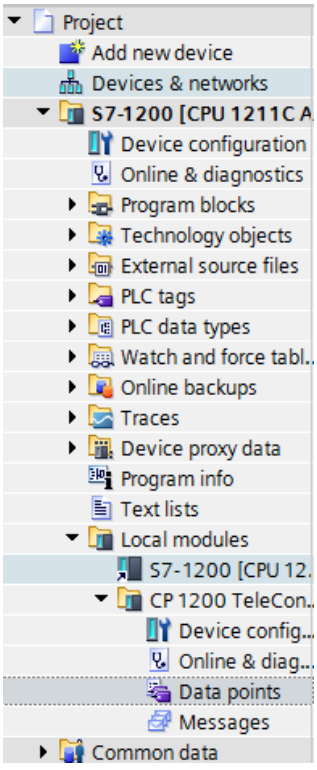


Figure 4-1 Configuring data points and messages

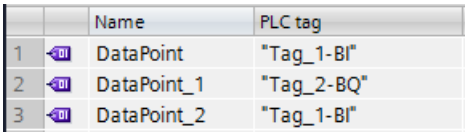
After opening the editor window using the two entries to the right above the table, you can switch over between the data point and message editor.

Figure 4-2 Switching over between the two editors

Creating obects

With the data point or message editor open, create a new object (data point / message) by double clicking "<Add object>" in the first table row with the grayed out entry.

A preset name is written in the cell. You can change the name to suit your purposes but it must be unique within the module.



		Name	PLC tag
1		DataPoint	"Tag_1-BI"
2		DataPoint_1	"Tag_2-BQ"
3		DataPoint_2	"Tag_1-BI"

Figure 4-3 Data point table

You configure the remaining properties of every object using the drop-down lists of the other table columns and using the parameter boxes shown at the bottom of the screen.

Assigning data points to their data source

After creating it, you assign a new data point to its data source. Depending on the data type of the data point a PLC tag can serve as the data source.

For the assignment you have the following options:

- Click on the table symbol  in the cell of the "PLC tag" column.

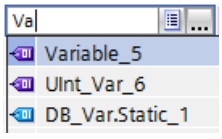
  All configured PLC tags and the tags of the created data blocks are displayed. Select the required data source with the mouse or keyboard.

- Click the symbol  .

  A selection list of the configured PLC Tags and the blocks is displayed. From the relevant table, select the required data source.

- In the name box of the PLC tag, enter part of the name of the required data source.

  All configured PLC tags and tags of the data blocks whose names contain the letters you have entered are displayed.

  Select the required data source.

Note

Assignment of parameter values to PLC tags

The mechanisms described here also apply when you need to assign the value of a parameter to a PLC tag. The input boxes fro the PLC tag (e.g.: PLC tag for partner status support the functions described here for selecting the PLC tag.

Arranging and copying objects

As with many other programs in the data point or message editor you can also arrange the columns, sort the table according to your requirements and copy and insert objects.

- Arrange columns

  If you click on a column header with the left mouse button pressed, you can move the column.

- Sorting objects

  If you click briefly with the left mouse button on a column header, you can sort the objects of the table in ascending or descending order according to the entries in this column. The sorting is indicated by an arrow in the column header.

  After sorting in descending order of a column the sorting can be turned off by clicking on the column header again.

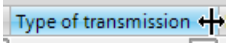
- Adapting the column width

  You can reach this function with the following actions:

  – Using the shortcut menu that opens when you click on a column header with the right mouse key.

    "Optimize width", "Optimize width of all columns"

  – If you move the cursor close to the limit of a column header, the following symbol appears:

    When it does, click immediately on the column header. The column width adapts itself to the broadest entry in this column.

- Showing / hiding columns

  You call this function using the shortcut menu that opens when you click on a column header with the right mouse key.

- Copying, pasting, cutting and deleting objects

  If you click in a parameter box of an object in the table with the right mouse key, you can use the functions named with the shortcut menu (copy, paste, cut, delete).

  You can paste cut or copied objects within the table or in the first free row below the table.

Exporting and importing data points

To simplify the engineering of larger plants, you can export the data points of a configured module and import them into other modules in the project. This is an advantage particularly in projects with many identical or similar stations or data point modules.

The export / import function is available when you select the module for example in the network or device view and select the relevant shortcut menu.

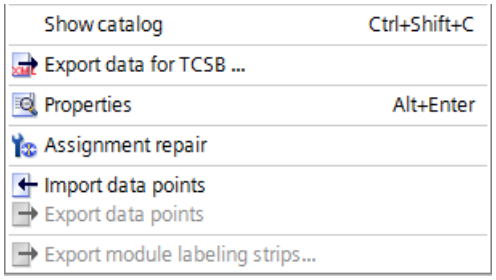


Figure 4-4 Shortcut menu of the module

When it is exported the data point information of a module is written to a CSV file.

Export

When you call the export function, the export dialog opens. Here, you select the module or modules of the project whose data point information needs to be exported. When necessary, you can export the data points of all modules of the project together.

In the export dialog, you can select the storage location in the file directory. When you export the data of a module you can also change the preset file name.

When you export from several modules, the files are formed with preset names made up of the station name and module name.

The file itself contains the following information in addition to the data point information:

- Module name
- Module type
- CPU name
- CPU type

Editing the export files

You can edit the data point information in an exported CSV file. This allows you to use this file as a configuration template for many other stations.

If you have a project with many stations of the same type, you can copy the CSV file with the data points of a fully configured module for other as yet unconfigured stations and adapt individual parameters to the particular station. This saves you having to configure the data points for every module in STEP 7. Instead, you simply import the copied and adapted CSV file to the other modules of the same type. When you import this file into another module, the changed parameter values of the CSV file are adopted in the data point configuration of this module.

The lines of the CSV file have the following content:

- Line 1: ,Name,Type,

  This line must not be changed.

- Line 2: PLC,<CPU name>, <CPU type>,

  Meaning: PLC (designation of the station class), CPU name, CPU type

  Only the elements <CPU name> and <CPU type> may be changed.

  The CPU type must correspond exactly to the name of the CPU in the catalog.

- Line 3: Module,<module name>,<module type>,

  Meaning: Module (Designation of the module class), module type, module name

  Only the elements <module name> and <module type> may be changed.

  Be careful when changing the module names if you want to import data points into several modules (see below).

  The module type must correspond exactly to the name of the module in the catalog.

- Line 4: Parameter names (English) of the data points

  This line must not be changed.

- Lines 5..n: Values of the parameters according to line 4 of the individual data points

  You can change the parameter values for the particular station.

Importing into a module

Before importing the data points make sure that the PLC tags required for the data points have been created.

Note that when you import a CSV file all the data points existing on the module will be deleted and replaced by the imported data points.

Select a module and select the import function from the shortcut menu of the module. The import dialog opens in which you select the required CSV file in the file directory.

If the information on the assignment of the individual data points to the relevant PLC tags matches the assignment in the original module, the data points will be assigned to the corresponding PLC tags.

When you import data points into a module, but some required PLC tags have not yet been created in the CPU, the corresponding data point information cannot be assigned. In this case, you can subsequently create missing PLC tags and them assign them the imported data point information. The "Assignment repair" function is available for this (see below).

If the names of the PLC tags in the module into which the import is made have different names than in the module that exported, the corresponding data points cannot be assigned to your PLC tags.

Importing into several modules

You can import the data points from several modules into the modules of a different project. To do this in the import dialog select all the required CSV files with the control key.

Before importing the data points, make sure that the respective stations have been created with CPUs of the same name, modules of the same name and PLC tags of the same name.

When you import the corresponding stations of the project are searched for based on the module names in the CSV files. If a target station does not exist in the project or the module has a different name, the import of the particular CSV file will be ignored.

Restrictions for the import of data points

In the following situations the import of data points will be aborted:

- An attribute required by the module is missing in the CSV file to be imported.

  Example: If a data point to be imported uses a time trigger, the import will be aborted if no time-of-day synchronization was configured for the module.

- The telecontrol protocol used by the module differs from that of the original module.

Only when importing into several modules:

- The import is aborted when a module or CPU name is different from the data in the CSV file.

Note:
Modules with the same telecontrol protocol are compatible with each other:

- TeleControl Basic

  All SIMATIC NET modules with the TeleControl Basic protocol:

  CP 1243-1, CP 1242-7 GPRS V2, CP 1243-7 LTE, CP 1542SP-1 IRC

- ST7

  CP 1243-8 IRC, CP 1542SP-1 IRC, ST7 TIM

- DNP3

  CP 1243-1, CP 1243-8 IRC, TIM modules capable of DNP3

- IEC

  CP 1243-1, CP 1243-8 IRC

Data points can be imported and exported between compatible modules.

Assignment repair

If you have named the PLC tags in a station into which you want to import differently from the station from which the CSV file was exported, the assignment between data point and PLC tag is lost when you import.

You then have the option to either rename the existing PLC tags appropriately or add missing PLC tags. You can then repair the assignment between unassigned data points and PLC tags. This function is available either via the shortcut menu of the module (see above) or with the following icon to the upper left in the data point editor: 

If a PLC tag with a matching name is found for a data point by the repair function, the assignment is restored. However the data type of the tag is not checked.

After the assignment repair make sure that you check whether the newly assigned PLC tags are correct.

4.13.2 Datapoint types

During the configuration of the user data to be transferred by the CP, each data point is assigned a 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).

As of the firmware version named in the preface along with STEP 7Basic V14, the CP supports the following data point types and data types.

The direction relates to the direction of transfer:

- "in": Monitoring direction:
- "out": Control direction

Data point types

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

Format (memory requirements)	Data point type	Direction	S7 data types	Address area
Bit	Digital input	in	Bool	I, Q, M, DB
	Digital output	in	Bool	Q, M, DB
Byte	Digital input	in	Byte, Char, USInt	I, Q, M, DB
	Digital output	out	Byte, Char, USInt	Q, M, DB
Integer with sign (16 bits)	Analog input	in	Int	I, Q, M, DB
	Analog output	out	Int	Q, M, DB
Counter (16 bits)	Counter input	in	Word, UInt	I, Q, M, DB
Integer with sign (32 bits)	Analog input	in	DInt	Q, M, DB
	Analog output	out	DInt	Q, M, DB
Counter (32 bits)	Counter input	in	UDInt, DWord	I, Q, M, DB
Floating-point number with sign (32 bits)	Analog input	in	Real	Q, M, DB
	Analog output	out	Real	Q, M, DB
Floating-point number with sign (64 bits)	Analog input	out	LReal	Q, M, DB
	Analog output	out	LReal	Q, M, DB
Block of data (1 .. 64 bytes)	Data	in / out	ARRAY [1)]	DB
	Data	in / out	ARRAY [1)]	DB

[1)] 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. The following S7 data types are compatible components of ARRAY:

- Byte, USInt (total of up to 64 per data block)
- Char (total of up to 64 per block of data) - CP as of firmware version 2.1.77
- Int, UInt, Word (total of up to 32 per data block)
- DInt, UDInt, DWord (total of up to 16 per data block)

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

Format of the time stamp

Time stamps are output by the OPC server applications in UTC format (48 bits) and contain milliseconds.

4.13.3 Status IDs of data points

Status IDs of data points

Along with the value of a data point, status identifiers of the data point are transferred in every frame. They can be evaluated by the communications partner.

The status bits are converted to the OPC quality code as follows by TCSB.

- Quality = BAD, if:

  NON_EXISTENT or OVER_RANGE = 1
- Quality = UNCERTAIN, if:

  RESTART or CARRY or SB = 1
- Quality = GOOD, if:

  Bits 1, 2, 3, 5 and 6 = 0

For the meaning of the status bits, see below. The entries in the table row "Meaning" relate to the entry in the table row "Bit status".

Table 4- 2 Bit assignment of status byte 0

Bit	7	6	5	4	3	2	1	0
Flag name	-	NON_ EXISTENT	SB	LOCAL_ FORCED	CARRY	OVER_ RANGE	RESTART	ONLINE
Meaning	-	Data point does not exist or S7 address unreachable	Substitute value	*(Bit is not set.)*	Counted value over-flow before reading the value	Limit value of the ana-log value prepro-cessing overshot / undershot	Value not updated after start	Value is valid, CPU in RUN
Bit status	*(always 0)*	1	1	*(irrelevant)*	1	1	1	1

Generation of events if a data point status changes

With data points that were configured as an event, the change to the status bit of the status identifiers described below also leads to an event being generated.

Example: If the value of the status "RESTART" of a data point configured as an event changes form 1 (value not yet updated) to 0 (value updated) when the station starts up, this causes an event to be generated.

4.13.4 Syntax of the data point names

Character set for data point names

When you create a data point, a preset name "DataPoint_n" is adopted. In the data point table and in the "General" tab of the data point you can change the name of the data point.

When assigning names only ASCII characters from the band 0x20 ... 0x7e (no. 32-126) may be used with the exceptions listed below.

Forbidden characters:

- . ' [ ] / \ |
  period, apostrophe, square brackets, slash, back slash, vertical line (pipe)

4.13.5 Read cycle

Priority of the data points

The cyclic reading of the values of input data points from their 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 "Read cycle" parameter. There you will find the two following options for input data points:

- Fast cycle
- Normal cycle

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.

4.13.6 Data point index

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 an input data point must be unique throughout all data point types (digital inputs, analog inputs etc.).

- Output

  The index of an output data point must be unique throughout all data point types (digital inputs, analog inputs etc.).

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 106).

4.13.7 Process image, type of transmission, event classes

Saving the data point values

The values of data points are stored in the image memory of the CP and transferred only when queried by the communications partner.

Events are also stored in the frame memory (send buffer) and can be transferred unsolicited.

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

- **Transfer after call: No event / static value**

  Static values are entered in the image memory (process image of the CP).

- **Triggered: event**

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

  The values of events are also entered in the send buffer of the CP.

  With DNP3, the value of the event is sent unsolicited to the communications partner if this function is enabled by the master.

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 butter can be found in the section Configuration limits and performance data (Page 19).

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 67).

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 data cannot be transferred for a longer period of time and the send buffer is threatening to overflow, the protocol-dependent response is as follows:

- Telecontrol Basic

  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 communication partner returns, the CP changes back to the send buffer mode as soon as the fill level of the send buffer has fallen below 50 %.

- DNP3 / IEC

  If the fill level of the send buffer reaches 100 %, no more values are saved until the fill level falls below 100 % again.

Types of transmission / event classes

The following types of transmission are possible:

- **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.

  After being called by the communications partner, the current value at the time is transferred.

- **Triggered (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 of the data point changes; see also the section Status IDs of data points (Page 92).

    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 the generation of an event.

  When data points are configured as an event via the "Type of transmission" parameter, the following event classes are available:

  – **Every value triggered**

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

  – **Current value triggered**

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

4.13.8 "Trigger“ tab

Trigger

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

Saving the value of a data point configured as an event

Saving the value of a data point configured as an event in the send buffer (frame memory) can be triggered by various trigger types:

- **Threshold value trigger**

  The value of the data point is saved 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 98).

- **Time trigger**

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

- **Event trigger (Trigger tag)**

  The value of the data point is saved 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 trigger tags in the bit memory area / DB:

  If the memory area of a trigger tag is in the bit memory or in a data block, the CP resets the trigger variable itself to 0 (zero) as soon as the value of the data point has been transferred. This can take up to 500 milliseconds.

Note

Fast setting of triggers

Triggers must not be set faster than a minimum interval of 500 milliseconds. This also applies to hardware triggers (input area).

Note

Hardware trigger

You need to reset hardware triggers via the user program.

Transferring the value of a data point configured as an event

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

- Spontaneous (unsolicited - direct transfer)

  The value is transferred immediately.

- Buffered transfer - Conditional spontaneous

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

  – The communications partner queries the station.

  – The value of another event with the transmission mode "Spontaneous" is transferred.

  – The fill level of the send buffer has reached 80 % of its maximum capacity.

4.13.9 Threshold value trigger

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 and before calculating the threshold value.

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

Note

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.

For the time sequence of the analog value preprocessing refer to the section Analog value preprocessing (Page 100).

Threshold value trigger

Function

If the process value deviates by the amount of the threshold value, the process value is saved.

Two methods are used to calculate the threshold value deviation:

- **Absolute method**

  With binary and counter values as well as with analog values with configured mean value generation, the absolute method is used to calculate the threshold value deviation.

- **Integrative method**

  With analog values without configured mean value generation, the integrating method is used to calculate the threshold value deviation.

  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 integrated deviation.

Absolute method

For each binary value a check is made to determine whether the current (possibly smoothed) value is outside the threshold value band. The current threshold value band results from the last saved value and the amount of the configured threshold value:

- Upper limit of the threshold value band: Last saved value + threshold value
- Lower limit of the threshold value band: Last saved value - threshold value

As soon as the process value reaches the upper or lower limit of the threshold value band, the value is saved. The newly saved value serves as the basis for calculating the new threshold value band.

Integrative method

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] (calculation cycle)	Process value stored in the send buffer	Current process value	Absolute deviation from the stored value	Integrated deviation
0	**20.0**	**20.0**	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	**20.5**	**20.5**	+0.5	**2.0**
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	**19.9**	**19.9**	-0.6	**-2.1**

With the changes in the process value shown in the example, the threshold value trigger configured with 2.0 fires twice:

- 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.

4.13.10 Analog value preprocessing

CPs with data point configuration support analog value preprocessing. For analog value data points, some or all of the functions described below can be configured.

Requirements and restrictions

You will find the requirements for the configuration of the preprocessing options and restrictions in the section relating to the particular function.

Note

Restrictions due to configured triggers

The analog value preprocessing options "Error suppression time", "Limit value calculation" and "Smoothing" are not performed if no threshold value trigger is configured for the relevant data point. In these cases, the read process value of the data point is entered in the image memory of the CP before the preprocessing cycle of the threshold value calculation (500 ms) elapses.

Sequence of the analog value preprocessing options

The values of analog inputs configured as an event are processed on the CPU according to the following scheme:

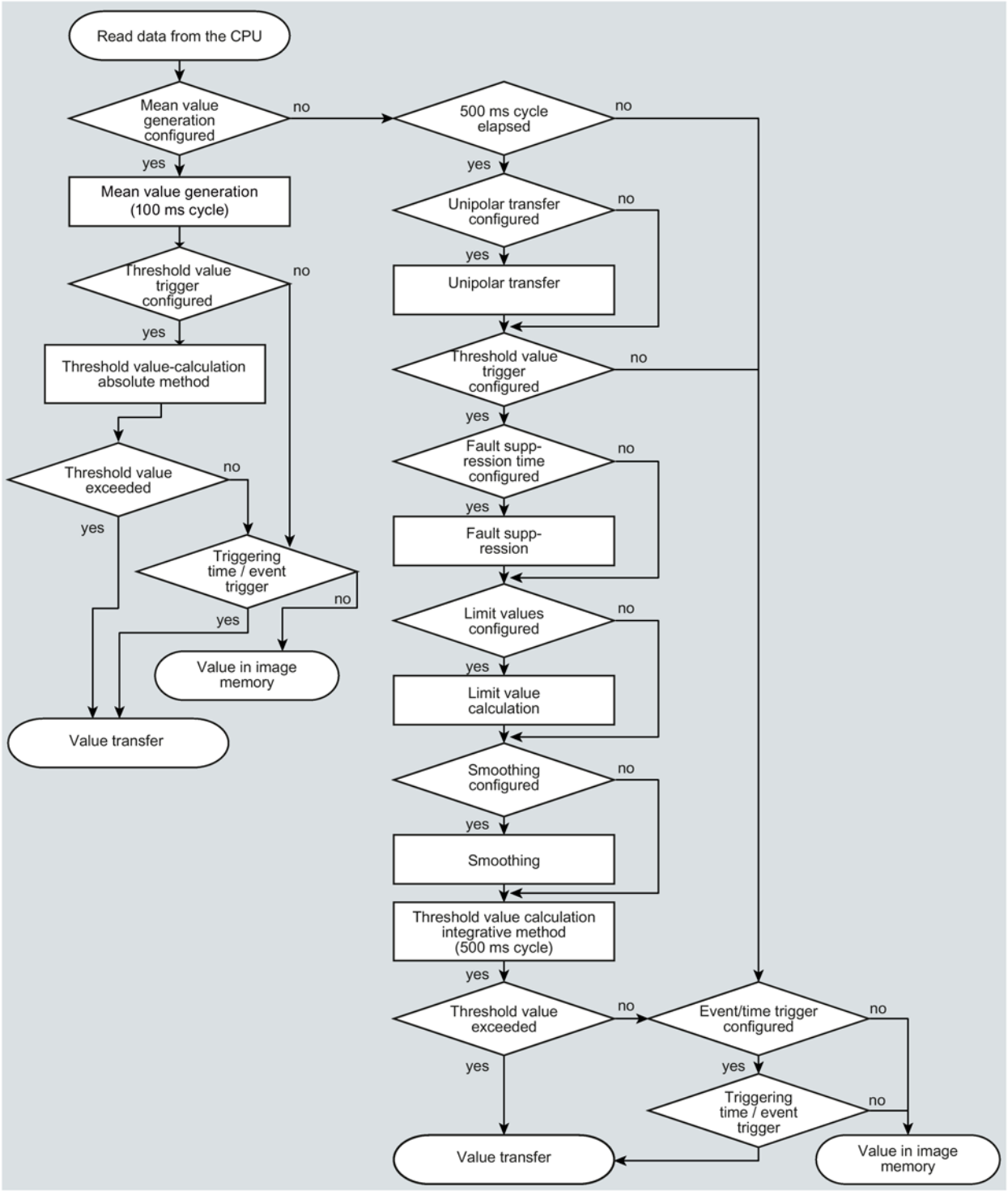


Figure 4-5 Sequence of the analog value preprocessing

The 500 millisecond cycle is started by the integrative threshold value calculation. In this cycle, the values are saved even when the following preprocessing options are enabled:

- Unipolar transfer
- Fault suppression time
- Limit value calculation
- Smoothing

Mean value generation

Note

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

Function

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

If mean value generation is active, it makes sense to configure a time trigger..

The current values of an analog data point are read in a 100 millisecond cycle and totaled. The number of read 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 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.

Input modules: Overflow range / underflow range

As soon as a value is acquired in the overflow or underflow range, mean value generation is stopped. The value 32767 / $7FFF_h$ or -32768 / 8000_h is saved as an invalid mean value for the current mean value calculation period and sent with the next message.

The calculation of a new mean value is then started. If the analog value remains in the overflow or underflow range, one of the two values named is again saved as an invalid mean value and sent when the next message 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.

Unipolar transfer

Restrictions

Unipolar transfer cannot be configured at the same time as mean value generation. Enabling unipolar transfer has no effect when mean value generation is activated.

Function

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: With process data from input modules, the value -32768 / 8000_h for wire break of a live zero input is transferred.

With a software input, on the other hand, all values lower than zero are corrected to zero.

Fault suppression time

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

The fault suppression time cannot be configured at the same time as mean value generation. A configured value has no effect when mean value generation is activated.

Function

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 transmission of an analog value in the overflow ($7FFF_h$) or underflow range (8000_h) is suppressed for the specified time. The value $7FFF_H$ or 8000_H 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.

Input modules

The suppression is adjusted to analog values that are acquired directly 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).

An analog value in the overflow range (32767 / $7FFF_h$) or underflow range (-32768 / 8000_h) 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.

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 / $7FFF_h$ or -32768 / 8000_h in the overflow or underflow range. If this is not the case, the parameter should not be configured for preprocessed values.

For finished values preprocess in the CPU, the limits for the overflow and underflow can be freely assigned.

Smoothing factor

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

The smoothing factor cannot be configured at the same time as mean value generation. A configured value has no effect when mean value generation is activated.

Function

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 n
y_{n-1} = smoothed value in the previous cycle n-1
x_n = acquired value 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

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

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 PLC tags of 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.

Function

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.

Status identifier "OVER_RANGE" / "overflow"

With protocols that support status identifiers, if the limit value is overshot or undershot, the status identifier of the data point is set for measured range violation known below as the identifier "OV". This status identifiers are described in the section Status IDs of data points (Page 92).

The "OV" 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: OV = 1
  - If the value then falls below the limit value: OV = 0
- Limit value 'low':
  - If the value falls below the limit value: OV = 1
  - If the value then exceeds the limit value: OV = 0

Configuration of the limit value

The limit value is configured as a whole decimal number. The range of values is based on the range of values of the raw value of analog input modules.

Entry as a decimal number according to the range of values of the assigned PLC tag from the bit memory or data area.

The entry of the value 0 (zero) is interpreted as a deactivated limit value.

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

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.

4.13.11 Partner stations: Configuring the inter-station communication

Telecontrol server enabled / Partners for inter-station communication

Here you specify who will be the communication partner of the data point.

If no CP was enabled as the partner for inter-station communication, the "Telecontrol server enabled" option is selected automatically. In this case, the telecontrol server is the 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 "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 (inter-station communication)

Specify the partner CP for inter-station communication for the selected data point by selecting the required partner from the drop-down list. The access ID of the relevant partner is shown in brackets.

The partners you specified in the "Partner stations" > "Partner for inter-station communication" can be selected.

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.

4.14 Messages

Configuration of the messages

If important events occur, the CP can send messages. The following are configurable:

- SMS

  The recipient can be a mobile phone or an S7-1200.

- E-mails

  The recipient can be a PC with an Internet connection or an S7-1200.

You configure the messages with the message editor of the CP. You can find this using the project tree:
directory of the station > Local modules > CP

For information on the network editor, refer to the section Data point configuration (Page 84).

You will find the characters permitted for message texts in the section Permitted characters in the configuration (Page 110).

Requirements and necessary information

To transfer messages, telecontrol communication (parameter group "Communication types") no longer needs to be enabled. With the CP you can send messages without using telecontrol communication.

You will find the general requirements for using mobile wireless services such as network, contract or IP address in the section Requirements for operation (Page 21).

You obtain the access data for the mobile wireless network and for an APN for transferring e-mails from your network provider. You configure this in the parameter group "Mobile wireless communication settings" see section Mobile wireless communications settings (Page 57).

You will find other required information for SMS messages and e-mails that you receive from your service provider in the following sections.

Configuring SMS messages

Additional required information:

- Number of the SMSC

You create the configuration in the following parameter groups.

- Enabling the SMS function

  "Communication types" > "Enable SMS"

- Configuration of the SMSC

  "Mobile wireless communication settings" see above.

- Configuring the SMS

  Message editor, see above.

Configuring e-mails

Additional required 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
- E-mail addresses of the recipients

You create the configuration in the following parameter groups.

- Enabling security functions

  To use e-mails you need to enable the security functions of the CP, parameter group "Security".

- Configuration of the service / protocol:

  "E-mail configuration", see section E-mail configuration (Page 73).

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

    "Global security settings"
  - Using the imported certificate for the CP:

    Parameter group "Security" > "Certificate manager"

"Message parameter"

Here you configure the phone number or the recipient, the subject (e-mail) and the text of the message.

"Trigger"

In the "Trigger" parameter group you configure triggering for sending the message and other parameters.

- **E-mail trigger / SMS trigger**

  Specifies the event for which the sending of the message is triggered.
  - **Use PLC tag**

    For the trigger signal to send the e-mail, the edge change (0 → 1) of the trigger bit "PLC tag for trigger" is evaluated that is set by the user program. When necessary, a separate trigger bit can be configured for each message. For information on the trigger bit, see below.

    Resetting the trigger bit:
    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.
    In all other cases, you need to reset the trigger bit with the user program.
  - **CPU changes to STOP**
  - **CPU changes to RUN**
  - **Connection to a partner interrupted**

    Triggers the sending of the message when the connection to a partner is interrupted.
  - **Connection to a partner established**

    Triggers the sending of the message when the connection returns.
  - **Connection establishment to partner failed**

    Triggers the sending of the message when the connection to a partner could not be established.
  - **Teleservice session started**
  - **Teleservice session ended**
  - **Weak mobile wireless network**

    Only for SMS

    If the mobile wireless connection for telecontrol communication is too weak, an SMS message is triggered and sent to the configured recipient.

- **PLC tag for trigger**

  PLC tag for the trigger "Use PLC tag"

  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.

- **Enable identifier for processing status**

  If the option is enabled, every attempt to send returns a status with information about the processing status of the sent message.

  The status is written to "PLC tag for processing status". If there are problems delivering messages, you can determine the status via the Web server of the CPU by displaying the value of the PLC tag there.

  For the significance of the status output in hexadecimal, refer to the section Processing status of messages (Page 130).

- **PLC tag for processing status**

  PLC tag of the type DWORD for the processing status

- **Include value**

  If you enable the option, the CP sends a value for the placeholder $$ from the memory area of the CPU in the message. To do this enter "$$" as a placeholder for the value to be sent in the message text.

  Select a PLC tag whose value will be integrated in the message. The value is entered in the message text instead of the placeholder $$.

  $$ can be a placeholder for data point types with a simple data type up to a size of 32 bits.

- **PLC tag for value**

  PLC tag in which the value to be sent is written.

4.15 Permitted characters in the configuration

Character set for APNs, e-mail servers, message texts and the Telecontrol password

The following permitted characters apply to:

- APN:

  User names and passwords

- SMTP server:

  User names and passwords

- Messages in the message editor:

  Message texts

- CP identification

  Telecontrol password

Entered as ASCII character sets (hexadecimal value and character name):

- 0x20

  Space

- 0x21 ... 0x5F

  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _

- 0x61 ... 0x7E

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

- 0x7C, 0x7E

  | ~

Program blocks

5

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 receive data via program blocks, the CP requires a fixed IP address 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 data

  – Connection establishment / termination and reception of data

Use as an alternative:

- **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

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

For changing configuration data of the CP during runtime:

- **T_CONFIG V1.0**

  Program controlled configuration of the CP

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

  Note

  No feedback from the CP

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

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

Connection descriptions in system data types (SDTs)

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

The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

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

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

Using the SDT

- **TCON_IP_V4**

  For transferring frames via TCP or UDP

- **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

  Programming recommendation:
  Set the parameter "WatchdogTime" from "MAIL_ADDR_PARAM" to a value higher than 3 minutes.

- **TMail_FQDN**

  For transferring e-mails addressing the e-mail server using its name (FQDN)

- **TMail_V4_SEC**

  For secure transfer of e-mails addressing the e-mail server using an IPv4 address

- **TMail_QDN_SEC**

  For secure transfer of e-mails addressing the e-mail server using the host name

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

You will find notes on programming SMS messages in the section Programming SMS messages via OUC (Page 116).

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 107). 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 (OUC).

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 DB.

Create a DB of the data type "Struct". Open the properties dialog of the DB (shortcut menu of the DB) and disable optimized block access in the "Attributes" parameter group.

In the structure of the DB, create the following data types for the SMS messages:

- 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 (+ 2 byte string header)

- String[160]

  String of 160 bytes for the message text (+ 2 byte string header)

  The SMS message text can contain max. 160 characters.

Per SMS message the structure requires memory space of 198 bytes.

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.

To store the received data from 10 SMS messages , you need to create an adequately large structure (2000 bytes) for the "DATA" parameter of the receiving block. As described above, the structure has the following organization:

- 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)

The received data of every SMS message gas the following structure:

- 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 (+ 2 byte string header)

- String[160]

  String of 160 bytes for the message text (+ 2 byte string header)

- Byte

  Status of the SMS message

  If more than one SMS message is received the status of every SMS is stored in this status byte:

  – 0 = Invalid

    1 = Unread

    2 = Read

When receiving multiple SMS messages, per SMS message the structure requires memory space of 200 bytes.

Length information at "LEN" and "DATA" for the blocks "TRCV" / "TRCV_C"

When receiving SMS messages via the blocks TRCV or "TRCV_C" if you enter length information in the "LEN" parameter, this can lead to incorrect information in the data storage of the received information.

Recommendation: Set LEN = 0 and enter the length information in the "DATA" parameter.

Character set for the SMS text

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

- 0x0A

  LF (line feed)

- 0x0D

  CR (carriage return)

- 0x20

  Space

- 0x21 ... 0x5A

  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- 0x61 ... 0x7A

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

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.

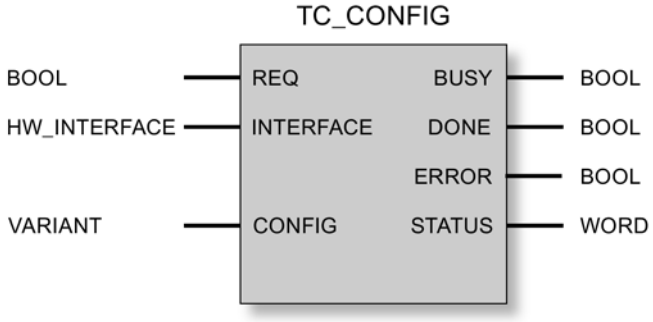
The configuration data to be modified on the CP is put together as necessary in blocks in IF_CONF "IF_CONF_..." for the individual parameters.

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 120).

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. 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 1: Error-free	Enable output 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 1: The instruction is executing	Condition code of the execution status of the block
DONE	OUTPUT	BOOL	0: - 1: The instruction executed successfully	This parameter indicates whether or not the job was completed without errors. For the meaning in conjunction with the parameters ERROR and STATUS, refer to Codes of the block.

Parameter	Declaration	Data type	Possible values	Description
ERROR	OUTPUT	BOOL	0: - 1: Error	Error code For the meaning in conjunction with the parameters DONE and STATUS, refer to Codes of the block.
STATUS	OUTPUT	WORD		Status code 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	0000_H	Job executed without errors
0	0	7000_H	No job processing active (first block call)
0	0	7001_H	Job processing started (first block call)
0	0	7002_H	Job processing already active (renewed block call when BUSY = 1)
0	1	$80E0_H$	Internal error
0	1	$80E6_H$	No query in progress (block call not started)
0	1	$80EB_H$	Query temporarily rejected (the CP is currently being configured by STEP 7)
0	1	$80F6_H$	Format error of a parameter in the called data block (wrong length, wrong format or invalid value) Check the "IF_CONF" SDT.
0	1	$80F7_H$	Wrong ID in the parameter fields of the configuration data: 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).

To be able to use the (SDT IF_CONF there must already be configured values present in the STEP 7 basic configuration of the CP.

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 Not relevant for the CP
2	Temporary validity of the configuration data, including deleting of existing permanent configuration data 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

"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] 1 = first telecontrol server, 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 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] of STRING [22]		Phone number subscriber authorized to wake up 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. Entry of the Public Land Mobile Network (PLMN) of the network provider consisting of Mobile Country Code (MCC) and Mobile Network Code (MNC). 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.

With IF_CONF_TS_Name only a TeleService server configured in STEP 7 can be changed but no new one created. If you attempt to create the configuration of a TeleService server with the block. the internal error 80E0 is output at TC_CONFIG.

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]: • 1 = server 1 • 2 = server 2 (not relevant)

Diagnostics and upkeep

6

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 32).

TeleService

From the engineering station you can connect to the remote station via mobile wireless using TeleService and view the diagnostics data of the CP. For information on establishing a TeleService connection, see below.

For the diagnostics contents see below ("Online > Online and diagnostics").

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

Here, you can obtain the following information about the online status of the selected module.

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

Using the online functions, you can read diagnostics information from the CP from an engineering station on which the project with the CP is stored.

If you want to operate online diagnostics with the station via the CP, you need to activate the online functions in the parameter group "Communication types".

"Diagnostics" group

Here, you can obtain the following 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 WAN 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 interface

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

  – Data point list

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

  – Protocol diagnostics

    With the function "Enable protocol trace" the frames received and sent by the module are copied for several seconds.

    With the function "Disable protocol trace", the logging is stopped and the data is written to a logging file.

    With the function "Save", you can save the log file on the engineering station and then analyze it.

  – Device-specific events

    Information on CP-internal events

- Time

  Information on the time on the device

"Functions" group

- Saving service data

  The function serves for logging of internal processes is situations in which you cannot eliminate unexpected or unwanted behavior of the module yourself.

  The log file is created with the "Save service data" button. The data is saved in a file with the format "*.dmp" that can be evaluated by the Siemens hotline.

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 159).

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

  Range of values and meaning:

  – 0 = Booked out of the network
  – 1 = Wrong PIN
  – 2 = Wrong SIM card
  – 3 = Waiting for PIN / no PIN configured
  – 4 = Booked into the network
- 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 default date of the CP (01.01.2000) is transferred as the trime.

  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 (≤ -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 Processing status of messages

Processing status

If the option "Enable identifier for processing status" is enabled in the message editor for a message, 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. Select this tag via the "PLC tag for processing status" box.

The meaning of the statuses is as follows:

Table 6- 1 SMS: Meaning of the status ID output in hexadecimal format

Status	Meaning
0000	Transfer completed free of errors
0001	Error in the transfer, possible causes: • SIM card invalid • No network • Wrong destination phone number (number not reachable)

Table 6- 2 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 Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.
8401	No channel available 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.

Status	Meaning
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 Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.
8500	Syntax error: Command unknown. 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. Try sending e-mails without authentication (no user name).
8501	Syntax error. Check the following configuration data: Message configuration > Message parameters: • Recipient address ("To" or "Cc").
8502	Syntax error. Check the following configuration data: Message configuration > Message parameters: • Email address (sender)
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: • CP configuration > E-mail configuration: – User name – Password – Email address (sender) • Message configuration > Message parameters: – Recipient address ("To" or "Cc").
8554	Transfer failed
85xx	Other error message from the e-mail server Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.

6.3 Loading firmware

Note
CPU STOP

Always set the CPU to STOP mode before you download a new firmware file to the CP:

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 address:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/dl)

Note that firmware versions as of V3 cannot be loaded on CPs with hardware product version 1.

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 32).

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 administration with the required rights.

   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 a user with the necessary rights.

   Use the user data configured in the user administration of the Web server of the CPU.

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.

6.4 Module replacement

Module replacement

⚠WARNING

Read the system manual "S7-1200 Programmable Controller"

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.

6.5 TeleService

6.5.1 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

TeleService server in "Mobile wireless communication 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

Users and roles in the global security settings

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.

"Authorized phone number" for TeleService in the global security settings

In some cases, it may be necessary to trigger connection establishment with an SMS message, see also the section Establishment of a TeleService connection (Page 137).

If you need to wake the CP to establish a TeleService connection with an SMS, the CP accepts an SMS only when the phone authorizes itself with its phone number. These phone numbers are configured for the CP in STEP 7 in the "Authorized phone numbers" list in the security settings.

- A phone number entered here gives the sender the right to trigger connection establishment.
- If only an asterisk (*) is entered in the list, the CP accepts SMS messages from all senders.
- An asterisk (*) after a phone number body authorizes connection establishment for all nodes connected to the body (extension numbers).

  Example: +49123456* authorizes +49123456101, +49123456102, +49123456207 etc.

Note

No wake-up without an authorized phone number

If the "Authorized phone numbers" list is empty, the CP cannot be woken up for connection establishment.

6.5.2 Establishment of 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 135).

Requirement for TeleService via a telecontrol connection: TeleService server

In TeleService via telecontrol, a TeleService server is required as the intermediary between S7 station and engineering station, see also the section Requirements for operation (Page 21).

- Telecontrol server

  If you use a telecontrol server, the intermediary can be the telecontrol server.

- TeleService gateway

  If there is no telecontrol server in your system, a TeleService gateway must exist as the intermediary.

For documentation of the two systems, refer to Documentation references (Page 159).

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.

Remember the following when establishing TeleService connections via mobile wireless.

Note

TeleService only by a TIA Portal instance

You can operate TeleService with a certain S7 station only from a single engineering station (TIA Portal instance / STEP 7 project). TeleService using several engineering stations at the same time with a station is not possible.

TeleService with several engineering stations with different S7 stations is possible if the suitable STEP 7 project exists on every engineering station.

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

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".

Mechanisms of connection establishment

The request for establishment of a TeleService connection is triggered by the engineering station. This request is sent via the intranet or Internet to the TeleService server (telecontrol server or TeleService gateway).

The TeleService server forwards to request to the CP in the S7 station. The TeleService server sends the request by e-mail to the SMS gateway which converts the e-mail and forwards it as an SMS to the CP in the S7 station via the mobile wireless network.

The TeleService connection is finally actively established by the CP.

Establishing a TeleService connection

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 menu "Online" > "Extended go online".

   The "Online access" dialog opens.
3. Choose the entry "TeleService via telecontrol" in the "Type of interface" drop-down list.
4. Choose the entry "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 via telecontrol" 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.

Information in the "Establish remote connection via telecontrol" dialog.

In this dialog, enter the data previously configured in STEP 7 under the following headings:

- **Telecontrol server / TeleService gateway...**

  Selection whether the TeleServiceTeleService 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

  – Own 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 135).

Ways to deal with connection establishment problems

If you have triggered the establishment of a TeleService connection with the engineering station and the connection is not established, among other things this may be because there is a connection disruption between the TeleService server and station or that the data of the SMS gateway configured on the TeleService server is incorrect.

In this case you can also use a wake-up SMS to make the station establish a TeleService connection. The phone number of the phone must be configured on the CP as "Authorized phone numbers".

Send an SMS to the phone number of the CP with the following text:

- Text for the wake-up SMS message for establishing a connection via the first configured TeleService server:

  ```
  TELESERVICE
  ```

  or

  ```
  TELESERVICE 1
  ```

- Text for the wake-up SMS message for establishing a connection via the second configured TeleService server:

  ```
  TELESERVICE 2
  ```

Sending the SMS does not replace the establishment of the TeleService connection on the engineering station.

Terminate TeleService connection

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

Technical specifications

7

7.1 General technical specifications

Table 7- 1 General technical specifications

Technical specifications		
Module name	**Article numbers**	
• CP 1243-7 LTE-EU	• 6GK7 243-7KX30-0XE0	
• CP 1243-7 LTE-US	• 6GK7 243-7SX30-0XE0	
Antenna connector		
Antenna connector	Quantity	1
	Design	SMA socket
	Nominal impedance	50 Ω
	Antenna cable, maximum permitted length	≤ 30 m
Electrical data		
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^2 (AWG 25)
	• Maximum	• 1.5 mm^2 (AWG 15)
	Max- tightening torque of the screw terminals	0.45 Nm (4 lb-in)
	Electrical isolation:	
	Power supply unit to internal circuit	710 VDC for 1 minute
Current consumption (typical)	From 24 VDC (external)	120 mA
	From the S7-1200 backplane bus	150 mA
Effective power loss (typical)	From 24 VDC (external)	1.8 W
	From the S7-1200 backplane bus	0.5 W
Permitted ambient conditions		
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

Technical specifications		
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Design, dimensions and weight		
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	• 35 mm DIN rail • Switch panel	

You will find additional functions and performance data in the section Application and functions (Page 11).

7.2 Technical specifications - wireless interface (CP 1243-7 LTE-EU)

Table 7- 2 Technical specifications of the wireless interface

Technical specifications - CP 1243-7 LTE-EU		
Article number	6GK7 243-7KX30-0XE0	
Frequency bands		
Supported frequency bands	LTE	B3 (1800 MHz) B7 (2600 MHz) B20 (800 MHz)
	UMTS / HSDPA+	B1 (2100 MHz) B5 (850 MHz) B8 (900 MHz)
	GSM	GSM (900/1800 MHz)
Wireless interface		
Maximum transmit power	LTE FDD (B3, B7, B20)	+23 dBm (Class 3)
	WCDMA FDD (B1, B5, B8)	+24 dBm (Class 3)
	EDGE 1800 MHz	+26 dBm (Class E2)
	EDGE 900 MHz	+27 dBm (Class E2)
	DCS 1800	+30 dBm (Class 1)
	GSM 900	+33 dBm (Class 4)
LTE	Transmission speed (maximum)	• Downlink: 100 Mbps • Uplink: 50 Mbps

Technical specifications - CP 1243-7 LTE-EU		
HSPA+	Transmission speed (maximum)	• Downlink (HSDPA): 42 Mbps • Uplink (HSUPA): 5.76 Mbps
EDGE	Properties	• Multislot class 10 end device class B coding scheme 1 to 9 (GMSK)
	Transmission speed	• Downlink: 236.8 kbps • Uplink: 236.8 kbps
GPRS	Properties	• Multislot class 10 device class B coding scheme 1 to 4 (GMSK)
	Transmission speed	• Downlink: 85.6 kbps • Uplink: 85.6 kbps
SMS	Mode outgoing	MO
	Service	Point-to-point

7.3 Technical specifications - wireless interface (CP 1243-7 LTE-US)

Table 7- 3 Technical specifications

Technical specifications - CP 1243-7 LTE-US		
Article number	6GK7 243-7SX30-0XE0	
Frequency bands		
Supported frequency bands	LTE	B2 (1900 MHz) B4 (1700 MHz) B5 (850 MHz) B17 (700 MHz)
	UMTS / HSDPA+	B2 (1900 MHz) B5 (850 MHz)
	GSM	GSM (850/1900 MHz)
Wireless interface		
Maximum transmit power	LTE FDD (B2, B4, B5, B17)	+23 dBm (Class 3)
	WCDMA FDD (B2, B5)	+24 dBm (Class 3)
	EDGE 1900 MHz	+26 dBm (Class E2)
	EDGE 850 MHz	+27 dBm (Class E2)
	PCS 1900	+30 dBm (Class 1)
	GSM 850	+33 dBm (Class 4)
LTE	Transmission speed (maximum)	• Downlink: 100 Mbps • Uplink: 50 Mbps

Technical specifications - CP 1243-7 LTE-US		
HSPA+	Transmission speed (maximum)	• Downlink (HSDPA): 21 Mbps • Uplink (HSUPA): 5.7 Mbps
EDGE	Properties	• Multislot class 10 end device class B coding scheme 1 to 9 (GMSK)
	Transmission speed	• Downlink: 236.8 kbps • Uplink: 236.8 kbps
GPRS	Properties	• Multislot class 10 end device class B coding scheme 1 to 4 (GMSK)
	Transmission speed	• Downlink: 85.6 kbps • Uplink: 85.6 kbps
SMS	Mode outgoing	MO
	Service	Point-to-point

7.4 Pin assignment of the socket for the external power supply

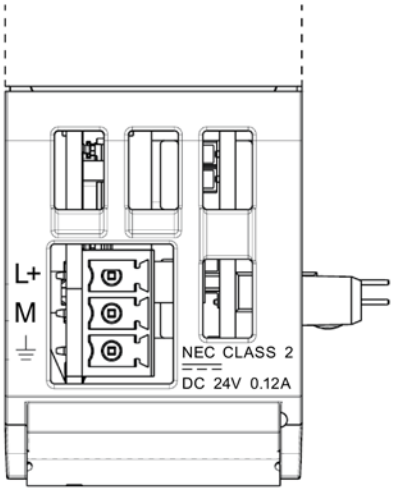


Figure 7-1 Socket for the external 24 VDC power supply (view from above)

Table 7- 4 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.

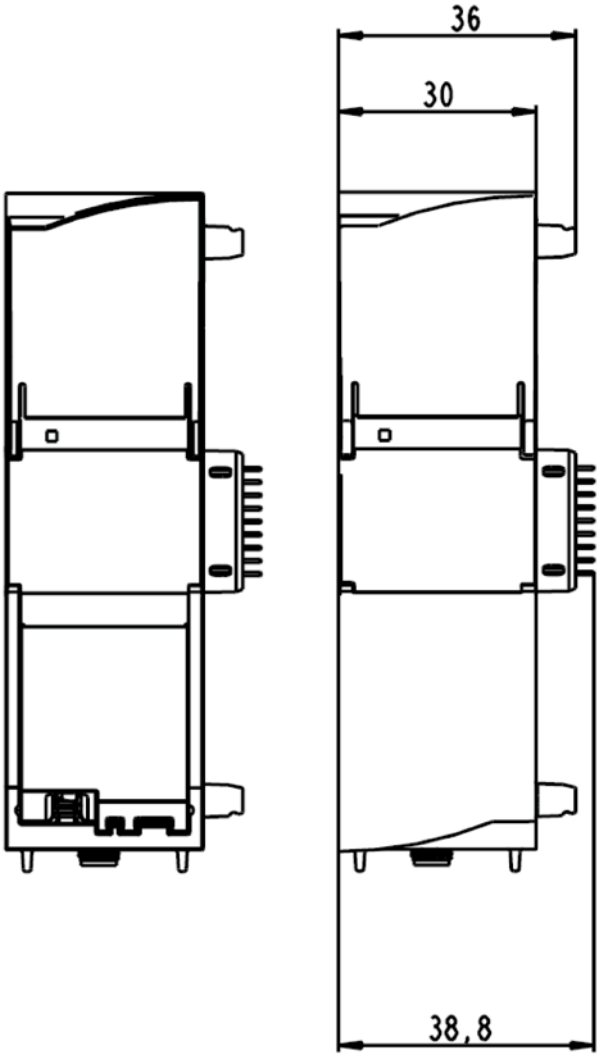


Figure A-1 Front view

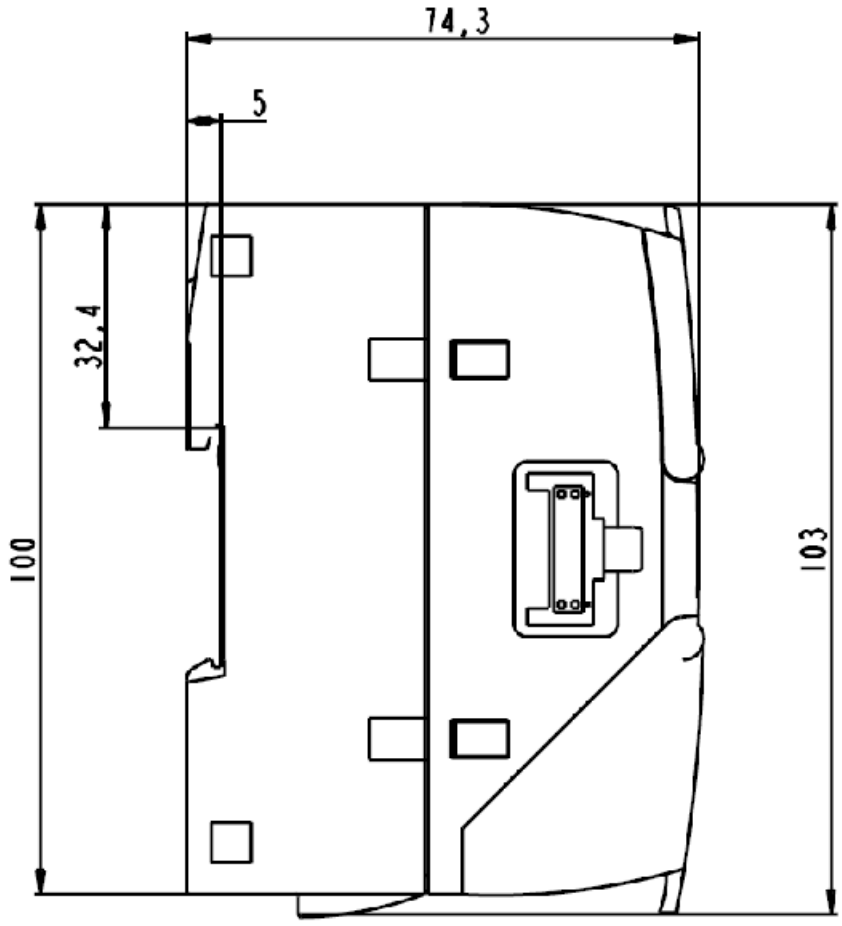


Figure A-2 Side view left

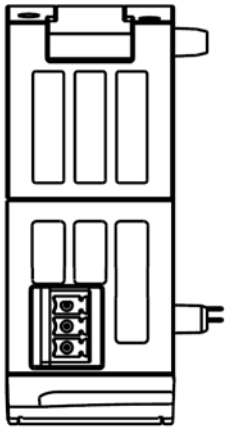


Figure A-3 From above

Approvals

B

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

CE

Valid only for the CP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

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

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

  Directive of the European Parliament and the Council of February 26 2014 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:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/cert)
Filter settings: Certificate type: "EC declaration of conformity"

IECEx

The CP meets the requirements of explosion protection according to IECEx.

IECEx classification: Ex nA IIC T4 Gc

IECEx certificate: IECEx DEK 14.0088X

The product meets the requirements of the following standards:

- EN 60079-0

  Hazardous areas - Part 0: Equipment - General requirements

- EN 60079-15

  Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

You can see the current versions of the standards in the IECEx certificate that you will find on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/cert)

Over and above this, the following conditions must be met for the safe deployment of the CP; see section Notes on use in hazardous areas according to ATEX / IECEx (Page 38).

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 and on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013)

ATEX

Valid only for theCP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

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

ATEX approval: II 3 G Ex nA II T4 Gc

Test number: KEMA 10 ATEX 0166X

Applied standards:

- EN 60079-0

  Hazardous areas - Part 0: Equipment - General requirements

- EN 60079-15

  Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

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

Over and above this, the following conditions must be met for the safe deployment of the CP; see section Notes on use in hazardous areas according to ATEX / IECEx (Page 38).

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 documentation and on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/cert)

R&TTE

Valid only for theCP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

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 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 V6.2.1

  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)

- ETSI EN 301 908-13 V6.2.1

  IMT cellular networks. Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive. Part 13: Evolved Universal Terrestrial Radio Access (E-UTRA) 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 Antennas (Page 155).

RoHS

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

Applied standard:

- EN 50581:2012

cULus

Underwriters Laboratories Inc. meets

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 61010-1-12 / CSA-IEC 61010-2-201

cULus HAZ.LOC.

HAZ. LOC.

Underwriters Laboratories Inc. meets

- ANSI ISA 12.12.01

  Nonincendive Electrical Equipment for Use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations
- CAN CSA C22.2 No. 213-M1987, 1st Ed. (R2013)
- Non-Incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4A; Ta = -20 °C...70 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...70 °C

FM

APPROVED

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 = 70 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 70 °C

National wireless approvals

To operate the CP in certain countries approvals for wireless operation must exist, the agreed marking must be present on the type plate and special instructions for the particular country must be adhered to. Some of the national approvals and instructions are shown below.

USA

Valid only for the CP 1243-7 LTE-US (6GK7 243-7SX30-0XE0)

- **FCC**

  7layers Report Reference: MDE_SIEM_1308_FCCb

  Test Specification:

  – PART 2 - GENERAL RULES AND REGULATIONS

  – PART 15 - RADIO FREQUENCY DEVICES

  FCC statement:
  "This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
  (1) This device may not cause harmful interference, and
  (2) this device must accept any interference received, including interference that may cause undesired operation.
  Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment."

  Additional statement for Digital Devices / Computer Peripheral Devices
  FCC §15.105 statement:
  "This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help."

- **Network Compatibility**

  AT&T approval

Canada

Valid only for the CP 1243-7 LTE-US (6GK7 243-7SX30-0XE0)

Approval IDs:

- ICTA: 5131-LE910NA
- FCC: RI7LE910NA

IC statement:

This device complies with part 15 of the FCC Rules and Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) this device must accept any interference received,
including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

South Africa

Valid only for theCP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

Approval Number TA-2015/1864

EAC (Eurasian Conformity)

Valid only for theCP 1243-7 LTE-EU (6GK7 243-7KX30-0XE0)

Customs union of Russia, Belarus and Kazakhstan

Declaration of the conformity according to the technical regulations of the customs union:

- TR CU
- RF Telecom

Mexico

Valid only for the CP 1243-7 LTE-US (6GK7 243-7SX30-0XE0)

La operación de este equipo está sujeta a las siguientes dos condiciones:

(1) es posible que este equipo o dispositivo no cause interferencia perjudicial y

(2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Country-specific mobile wireless approvals of SIMATIC NET devices

You will find an overview of the mobile wireless approvals of the SIMATIC NET devices for specific countries here:
Link: (www.siemens.com/mobilenetwork-approvals)

You can obtain further information on mobile wireless approvals of SIMATIC NET devices from Siemens Industry Online Support:
Link: (http://www.siemens.de/automation/support-request)

Current approvals

SIMATIC NET products are regularly submitted to the relevant authorities and approval centers for approvals relating to specific markets and applications.

If you require a list of the current approvals for individual devices, consult your Siemens contact or check the Internet pages of Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/cert)

Accessories

C

C.1 Antennas

The following antennas are available for use in mobile wireless networks and can be installed both indoors and outdoors. The antennas 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 Industrial Automation Customer Support under the following entry ID:

Link: (https://support.industry.siemens.com/cs/ww/en/view/23119005)

Flat antenna ANT794-3M

Figure C-2 Flat antenna ANT794-3M

Short name	Order no.	Explanation
ANT794-3M	6NH9 870-1AA00	Flat antenna for GSM networks (2G), for tri-band 900 / 1800 / 1900 MHz; weatherproof for indoor and outdoor areas; 1.2 m connecting cable connected permanently to the antenna; SMA connector, including adhesive mounting tape.

You will find detailed information in the documentation of the device. You will find this on the Internet on the pages of Siemens Industrial Automation Customer Support under the following entry ID:

Link: (https://support.industry.siemens.com/cs/ww/en/view/48729835)

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

For the TS gateway manual, see /2/ (Page 160).

Documentation references

D

Where to find Siemens documentation

- Article numbers

  You will find the article numbers for the Siemens products of relevance here in the following catalogs:

  – SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI

  – SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70

  You can request the catalogs and additional information from your Siemens representative. You will also find the product information in the Siemens Industry Mall at the following address:

  Link: (https://mall.industry.siemens.com)

- Manuals on the Internet

  You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

  Link: (https://support.industry.siemens.com/cs/ww/es/ps/15247/man)

  Go to the required product in the product tree and make the following settings:

  Entry type “Manuals”

- Manuals on the data medium

  You will find manuals of SIMATIC NET products on the data medium that ships with many of the SIMATIC NET products.

/1/

SIMATIC
S7-1200 Automation System
system manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/13683/man)

/2/

SIMATIC NET
CP 1243-7 LTE
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/man)

/3/

SIMATIC NET
TS Gateway (Version V3)
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/man)

/4/

SIMATIC NET
TeleControl Server Basic (Version V3)
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15918/man)

/5/

SIMATIC NET
Industrial Ethernet Security
Security basics and applications
Configuration manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15326/man)

Index

R

S

T

U

V

W