

SIMATIC NET

S7-1200 - TeleControl CP 1243-7 LTE

Operating Instructions

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

05/2021

C79000-G8976-C381-06

Preface

Application and functions

1

LEDs and connectors

2

Installation, connecting up, commissioning

3

Configuration

4

Program blocks

5

Diagnostics and upkeep

6

Technical specifications

7

Dimension drawings

A

Approvals

B

Accessories

C

Documentation references

D

Legal information

Warning notice system

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Preface

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 3
Firmware version V3.3
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 3
Firmware version V3.3
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.

Purpose of the manual

This manual describes the properties of this module and supports you when installing and commissioning the device. You will also find instructions for operation and information about the diagnostics options of the device.

Configuration is described depending on the use of the CP:

- **CP without telecontrol communication**

All relevant configuration steps for these applications are described in these operating instructions.

- **CP with telecontrol communication**

You will find the complete description of the configuration and diagnostics for these applications in the respective configuration manual; see below.

Refer to the information below in the section "Structure of the documentation".

New in this edition

- Hardware product version 3 with the following new functions, among others:
 - New mobile wireless interface
 - Support of IPv6

Note the following information on the antennas.

- Firmware version V3.3 with the following new functions, among others:
 - Support of the telecontrol protocol DNP3
 - Support of the telecontrol protocol IEC 60870-5

Note the structure of the documentation in this case.

Note

Allowed antennas depending on the hardware product version

The CP is approved with various antennas depending on the hardware product version.

Refer to the information in appendix Accessories (Page 113).

Replaced manual edition

Edition 12/2019

Structure of the documentation

The documentation of the CP consists of the following manuals and content:

- **Operating instructions**

- Application and functions
- Requirements (CPUs, configuration software, etc.)
- Hardware description
- Installation, wiring, commissioning, operation
- Configuration

This section of the operating instructions describes the configuration without use of the telecontrol functions.

If you use telecontrol functions, read the respective configuration manual; see below.

- Diagnostics, maintenance
- Technical specifications, approvals, accessories

- **Configuration Manual**

Configuration and diagnostics in STEP 7 Professional (TIA Portal)

The configuration manuals each describe the complete configuration of the CP with use of the telecontrol functions.

- **Configuration Manual TeleControl Basic**

Valid for all SIMATIC NET communication modules that support the TeleControl Basic protocol.

- **Configuration Manual DNP3**

Valid for all SIMATIC NET communications modules that support the DNP3 protocol.

- **Configuration Manual IEC 60870-5**

Valid for all SIMATIC NET communications modules that support the protocol IEC 60870-5-101/104.

You can find the Internet links for the manuals under /3/ (Page 116).

Current manual edition 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

Notes on this document

Terms

- **CP / module / device**

Simplified designation of the CP 1243-7 LTE-EU / CP 1243-7 LTE-US, valid for both CPs.

If a function is only relevant for one of the two CPs in the respective context, this is indicated by specifying the complete name.

- **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 99).

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>.

Search

To show all places where a term was found in a list, some PDF readers support the command <Ctrl>+<Shift>+<F>.

Sources of information and other documentation

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

License conditions

Note

Open source software

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

You will find the license conditions 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.

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>)

Security configuration

The latest safety standards are only supported with the current firmware version and with use of the latest configuration tool.

When the device is replaced with a newer one, the safety standards of the replaced device are supported, rather than the latest safety standards.

Firmware

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

Device defective

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

Decommissioning

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

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

You achieve this by resetting the CPU using the online functions of STEP 7.

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

	Preface	3
1	Application and functions	11
1.1	Connecting the S7-1200 to a mobile wireless network	11
1.2	Communications services.....	12
1.3	Communication via SINEMA RC	15
1.4	Other services and properties.....	16
1.5	Security functions	17
1.6	Configuration limits and performance data	19
1.7	Requirements for operation	21
1.8	Configuration examples	23
2	LEDs and connectors.....	27
2.1	Opening the housing	27
2.2	LEDs	28
2.3	Electrical connectors	31
2.3.1	Power supply	31
2.3.2	Wireless interface	32
3	Installation, connecting up, commissioning	33
3.1	Important notes on using the device	33
3.1.1	Notices on use in hazardous areas.....	33
3.1.2	Notes on use in hazardous areas according to ATEX / IECEx.....	34
3.1.3	Notices regarding use in hazardous areas according to UL HazLoc	35
3.2	Installing, wiring and commissioning	35
3.3	Notes on operation	40
4	Configuration.....	41
4.1	Security recommendations.....	41
4.2	Configuration in STEP 7.....	44
4.3	Communication types	46
4.4	Mobile wireless communications settings.....	47
4.5	Ethernet interface [X1]	49
4.5.1	Ethernet addresses	49
4.5.2	Advanced options	50
4.5.3	Access to the Web server.....	51
4.6	Time-of-day synchronization	51
4.7	DNS configuration	54
4.8	Communication with the CPU	55
4.9	Security	57
4.9.1	Security user.....	57
4.9.2	Firewall	58

4.9.2.1	Pre-check of messages by the MAC firewall.	58
4.9.2.2	Notation for the source IP address (advanced firewall mode)	58
4.9.2.3	Firewall settings for configured connection connections via a VPN tunnel.....	58
4.9.2.4	Settings for online security diagnostics and downloading to station with the firewall activated	58
4.9.3	Time-of-day synchronization	59
4.9.4	Authorized phone numbers	59
4.9.5	E-mail configuration	60
4.9.6	VPN	61
4.9.6.1	VPN (Virtual Private Network).....	61
4.9.6.2	Addressing the CP when using VPN	62
4.9.6.3	Creating a VPN tunnel for S7 communication between stations	62
4.9.6.4	Communications partners in a VPN group	64
4.9.6.5	CP as passive subscriber of VPN connections	64
4.9.6.6	SINEMA Remote Connect	65
4.9.7	Certificate manager	67
4.9.8	Handling certificates	68
4.10	Data points	70
4.11	Messages	70
4.12	Character set for passwords and messages.....	76
5	Program blocks	77
5.1	Program blocks for OUC	77
5.2	SMS messages via OUC	80
5.3	TC_CONFIG for changing configuration data of the CP.....	83
5.4	IF_CONF: SDT for the configuration data of the CP.....	85
6	Diagnostics and upkeep	91
6.1	Diagnostics options.....	91
6.2	Online security diagnostics via port 8448	94
6.3	Processing status of messages	94
6.4	Loading firmware	96
6.5	Module replacement.....	97
7	Technical specifications.....	99
7.1	General technical specifications	99
7.2	Technical specifications - wireless interface (CP 1243-7 LTE-EU)	100
7.3	Technical specifications - wireless interface (CP 1243-7 LTE-US)	101
7.4	Pin assignment of the socket for the external power supply.....	102
A	Dimension drawings.....	103
B	Approvals.....	105
C	Accessories	113
C.1	Antenna for CP as of hardware product version 3	113
C.2	Antenna for CP as of hardware product version 2	114
D	Documentation references	115
	Index	117

Application and functions

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 certified by AT&T supports the following mobile wireless standards:

- LTE
- UMTS

You will find the supported frequency bands in the section Technical specifications (Page 99).

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

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 105).

1.2 Communications services

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) / (Enhanced Data Rates for GSM Evolution)

Only CP 1243-7 LTE EU

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.

Communication types

The following communication types are possible:

- **Telecontrol communication with a control center**

The S7-1200 station with mobile wireless CP communicates with a master station via mobile wireless network and the Internet.

- **Event-controlled sending of messages (SMS / 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 the STEP 7 message editor. The use of program blocks is not necessary.

For information on the configuration, refer to sections E-mail configuration (Page 60) and Messages (Page 70).

- **Direct communication**

Direct communication between stations is possible in the following applications:

- Open User Communication via program blocks
- Sending of data to partner stations with telecontrol communication DNP3 / IEC with enabled "Master function" of the data points

Telecontrol

The CP supports the following types of WAN communication:

- **Telecontrol communication**

Connection of the S7-1200 to the following control center systems via mobile wireless and the Internet:

- Telecontrol server (TeleControl Basic / TCSB)
- DNP3 master
- IEC master

- **Inter-station communication**

Communication between stations via the master station (TeleControl Basic)

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.

E-mail

Independent of whether telecontrol communication is activated, the CP can send configured e-mails to PCs with Internet connection, triggered by events. The use of program blocks is not necessary for this. For information on configuration, see below.

Communication via SINEMA Remote Connect

Supported as of firmware version V3.1. Refer to section Communication via 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 77).

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

- S7 routing

As of CP firmware V2.1 with CPU $\geq$ V4.2

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 when the CP uses the telecontrol communication "TeleControl Basic" and when 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 can find more information in the configuration manual /3/ (Page 116).

1.3 Communication via SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

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

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

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

For the CP firmware version required for communication via SINEMA RC see section Communications services (Page 12).

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 configuration, refer to the telecontrol configuration manuals /3/ (Page 116).

Applications

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

Application example:

- (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

- **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 51).

- **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.

- **Diagnostics SMS message**

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

Further properties in telecontrol mode

- **Data point configuration**

Due to the data point configuration in STEP 7, you do not need to create program blocks to transfer the process data. The individual data points are processed one-to-one in the control system.

- **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

For example:

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

- **Analog value processing**

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

1.5 Security functions

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
- 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.

- **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

For information on configuring the security functions, refer to the section Security (Page 57).

You will find additional information on the functionality and configuration of the security functions in the STEP 7 information system.

Security functions of the telecontrol protocols

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
- **DNP3**
Secure Authentication

1.6 Configuration limits and performance data

Connection resources

- **Telecontrol connections**
 - DNP3 / IEC
The CP can establish connections to up to 4 communication partners.
A partner is a single or redundant master or a station (Direct communication).
 - TeleControl Basic
1 reserved connection for user data exchange with the telecontrol server
Additional Inter-station communication: The inter-station communication between the CPs of two stations takes place via the telecontrol server. It is configured in the "Partner stations" > "Partner for inter-station communication" parameter group.
Configuration limits for inter-station communication A total of max. 15, of which:
 - Send to partner: Max. 3 ("Send buffer" parameter enabled)
 - Receiving from partners: Max. 15 ("Send buffer" parameter disabled)
- **S7 connections and TCP / UDP / ISO-on-TCP connections**
Max. 14 connection resources, can be distributed as required for:
 - S7 connections (PUT/GET)
Including connections for S7 routing
 - Connections via program blocks (OUC) to S7 stations

- **PG/OP connections**
 - 1 connection resource for PG connections
 - 3 connection resources for OP connections
- **Online functions**
 - 1 connection resource is reserved for online functions.
- **TeleService connections**
 - Max. 1 TeleService connection
- **Connections to NTP servers**
 - Max. 1 connection to an NTP server

User data

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

User data per frame with the various connection types:

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

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

Number of data points for the data point configuration

The maximum number of configurable data points under the telecontrol protocols is:

- TeleControl Basic: 200
- DNP3: 500
- IEC: 500

Frame memory (send buffer)

The CP has a frame memory (send buffer) for the values of data points that are configured as event and are to be sent to the communication partners.

The send buffer has the following maximum size:

- TeleControl Basic: 64000 frames
- DNP3: 100000 events
- IEC: 100000 events

The send buffer is divided equally among all configured communications partners. The size of the frame memory can be set in STEP 7 ("Communication with the CPU" parameter group).

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

1.7 Requirements for operation

Hardware requirements

The following hardware is required in the S7-1200:

- CP
The requirement for the firmware version V3.3 is a CP with hardware product version 2 or 3.
- A CPU
The full functionality of the CP is only available with a CPU as of V4.4.
- An external antenna for the CP
Use only the antenna from the accessories program for the CP, refer to the appendix Accessories (Page 113).

Configuration software

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

STEP 7 Basic V17

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 12).

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), the mobile wireless network provider must assign a fixed IP address to the CP and forward the frames to the destination nodes.

You will find the applications that require a fixed IP address in the section Ethernet addresses (Page 49).

- 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 47).

Requirements for e-mail

Note the following requirements in the CP configuration for the transfer of e-mails:

- The security functions are enabled.
- The time of the CP is synchronized.

For the configuration, you require the data of the SMTP server and the user account:

- Server address, port number, user name, password, e-mail address of the sender (CP)
- With encrypted transfer: Server certificate

Software for telecontrol communication and TeleService

Requirement: Telecontrol communication is enabled.

- For the telecontrol communication

The telecontrol server requires the "TCSB" (TeleControl Server V3) software in the master station.

For the documentation of the application, see /4/ (Page 116).

- For TeleService

You can use the SINEMA Remote Connect application for TeleService.

You can find additional information in the configuration manuals TeleControl Basic, DNP3, IEC 60870-5, see /3/ (Page 116).

1.8 Configuration examples

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

You will find configuration examples for telecontrol applications in the configuration manuals /3/ (Page 116).

Sending SMS messages and e-mails

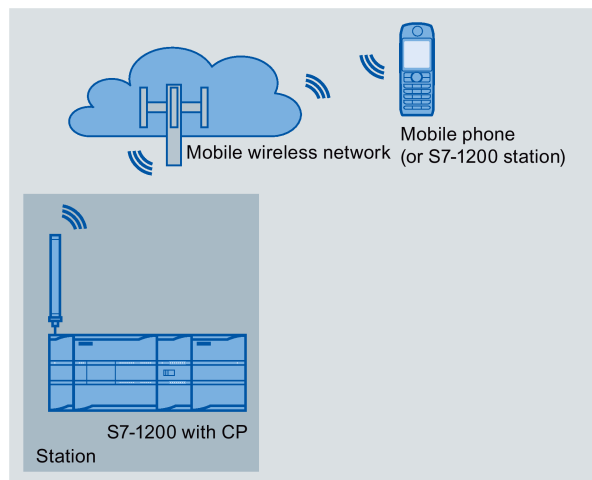


Figure 1-1 Sending messages by SMS from an S7-1200 station

SMS

A mobile wireless CP can send SMS messages to a mobile phone or a configured S7 station. The mechanisms for this are as follows:

- SMS messages generated and sent as the result of an event. They are configured in the messages editor.
- SMS messages that are sent or received by calling the corresponding program blocks of the Open User Communication.

See also the section "Direct communication between stations".

- Using a mobile phone, a diagnostics SMS can be requested, see section Diagnostics options (Page 91).

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. They are configured in the messages editor.
- E-mails sent as a result of calling the program block TMAIL_C.

For secure transmission of e-mails, the CP must have the current time.

Direct communication between stations

Direct communication between S7 stations is made possible by the program blocks of the Open User Communication (OUC).

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.

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

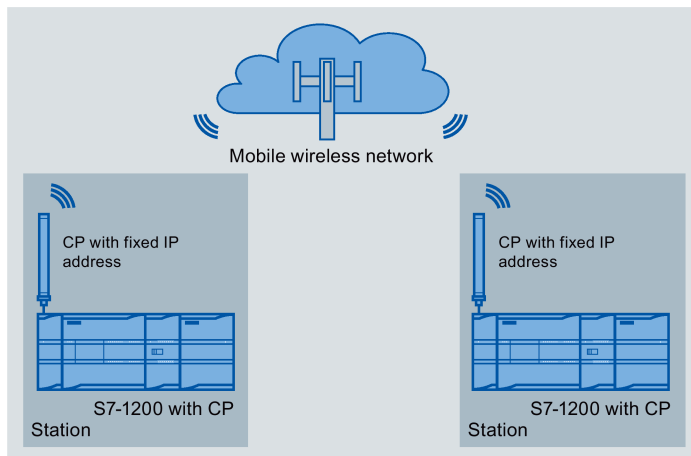


Figure 1-2 Direct communication between two S7-1200 stations

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.

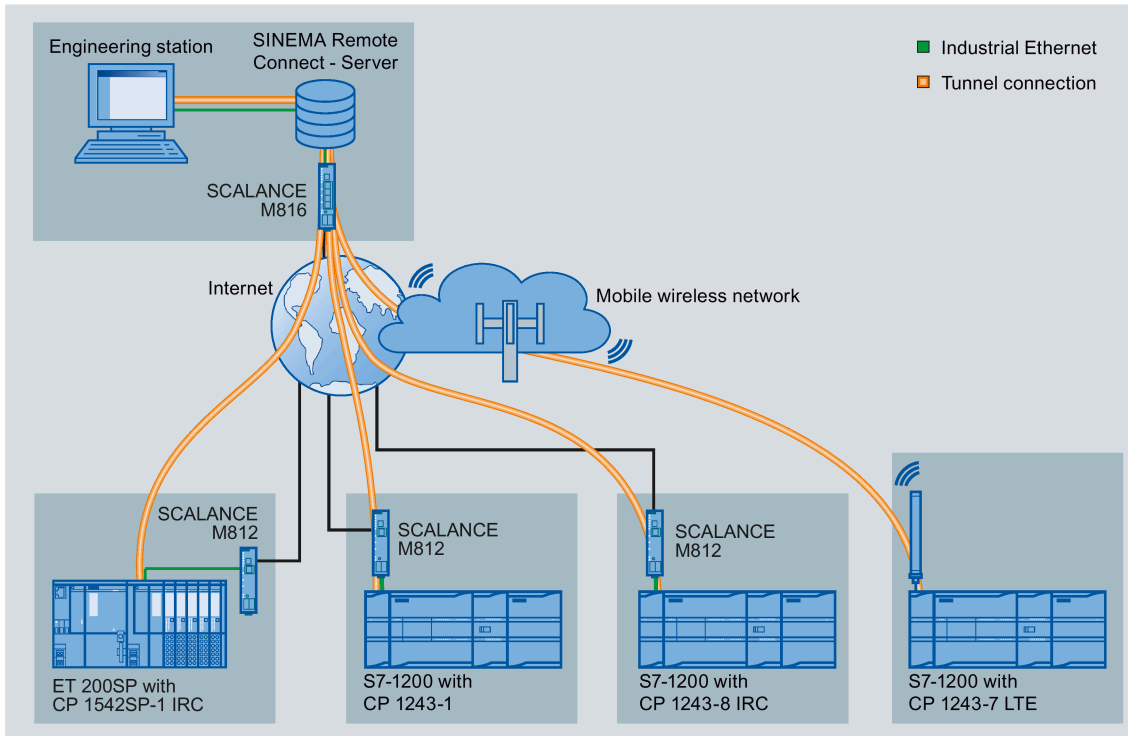


Figure 1-3 Connection of stations to engineering station via SINEMA RC

LEDs and connectors

2.1 Opening the housing

Location of the display elements and the electrical connectors

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

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

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

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

Opening the housing

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

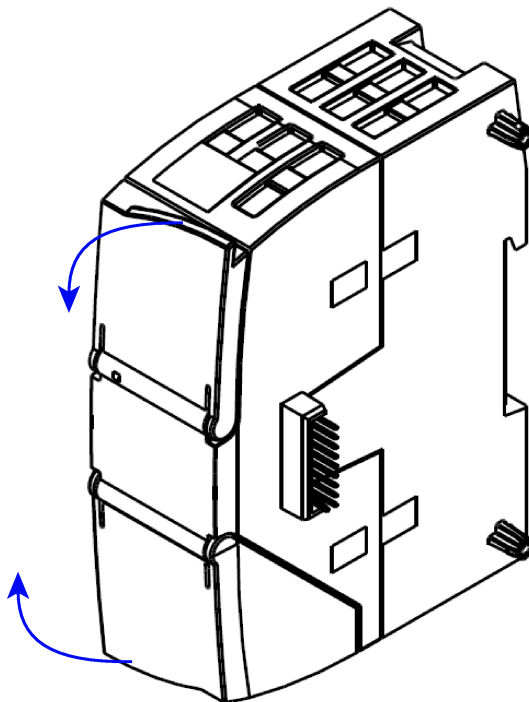


Figure 2-1 Opening the housing

2.2 LEDs

LEDs of the module

The CP has the following LEDs for displaying the status:

- "DIAG" LED on the front panel

The "DIAG" LED that is always visible shows the basic statuses of the module.

- LEDs below the upper cover of the housing

These LEDs provide further details on the module status.

Table 2- 1 LED on the front panel

LED / colors	Name	Meaning
 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
 flashing green			-	-	Telecontrol configuration exists, partner not reachable, CPU in RUN mode
 flashing green			-	-	Telecontrol configuration exists, partner not reachable, CPU in STOP mode

2.2 LEDs

DIAG (red / green)	NETWORK (red / green)	CONNECT (green)	SIGNAL QUALITY (yellow / green)	VPN (green)	Meaning
Quality of the mobile wireless connection					
-	-	-		-	Good network (-73 ... ≥ -51 dBm)
-	-	-		-	Medium strength network (-89 ... -74 dBm)
-	-	-		-	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
-		-	-		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					
 					Loading firmware. The "DIAG" LED flashes alternating red and green.
 flashing green					Firmware was successfully loaded.
 flashing red					- 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 102).

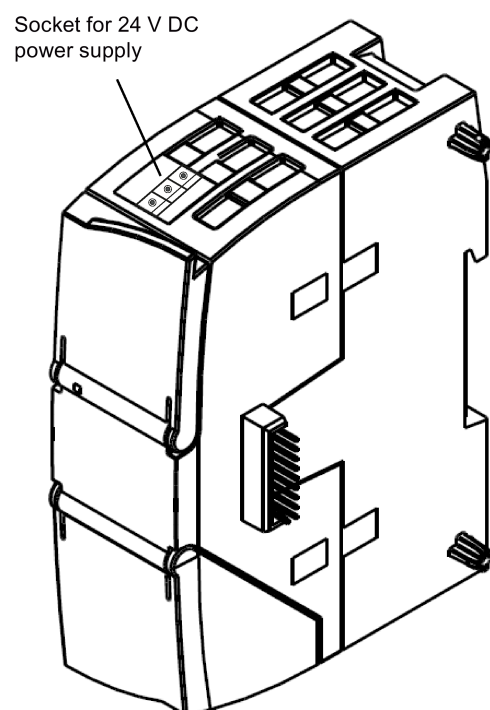


Figure 2-2 Socket for the 24 V DC power supply

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 113).

More detailed information on the electrical connections

For technical information on the electrical connections, refer to the section Technical specifications (Page 99).

Installation, connecting up, commissioning

3.1 Important notes on using the device

Safety notices on the use of the device

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

Overvoltage protection

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).

3.1 Important notes on using the device

 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 EC Directive 2014/34 EU (ATEX 114) or the conditions of IECEx, this enclosure or cabinet must meet the requirements of at least IP54 (in compliance with EN 60529) according to EN 60079-7.

! WARNING

Cable

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 41)".

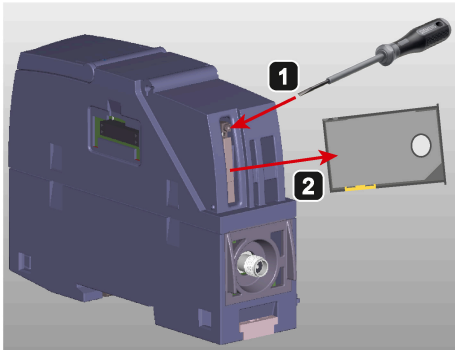
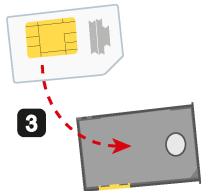
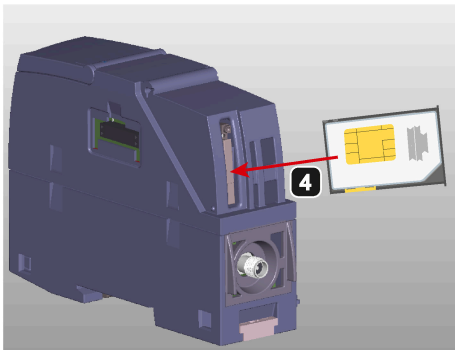
Inserting the SIM card

Note

Inserting and removing the SIM card

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

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

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

Dimensions for installation

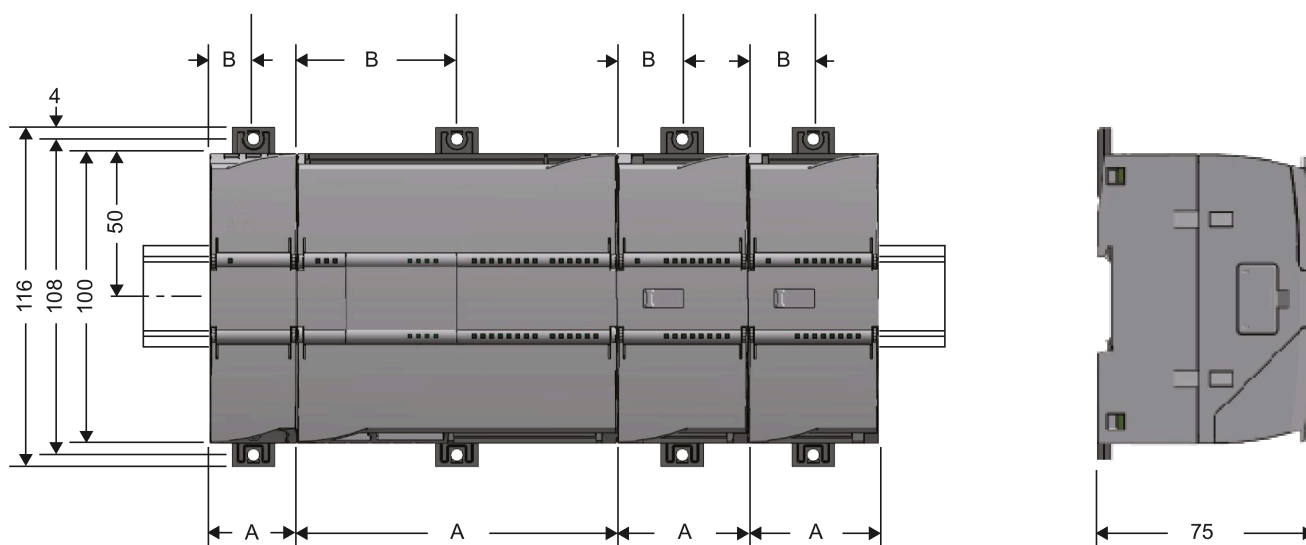


Figure 3-1 Dimensions for installation of the S7-1200

Table 3- 1 Dimensions for installation (mm)

S7-1200 devices		Width A	Width B *
CPU (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 inter- faces (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.

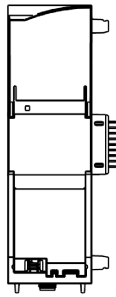
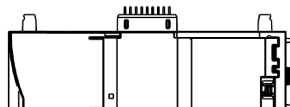
Procedure for installation and commissioning

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 99).

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 99).

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 102).
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"

Manual setting the time of day during commissioning

Note

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

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

The CP receives the time from 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 partner or the SINEMA RC Server.

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

4.1 Security recommendations

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

With enabled telecontrol communication, you should also refer to the information in the configuration manual.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Check regularly for new features on the Siemens Internet pages.
 - You can find information on Industrial Security here:
Link: (<http://www.siemens.com/industrialsecurity>)
 - You can find a selection of documentation on the topic of network security here:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/92651441>)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.

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

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

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 publicly 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
DNP3	20000 (TCP/UDP) Configurable	Closed	Open after configuration	Yes, when Secure Authentication is enabled.
IEC	2404 (TCP) Configurable	Closed	Open	No
S7 and online connections	102 (TCP)	Closed	Open after configuration *	No
Communication via SINEMA RC	443 (TCP)	Closed	Open after configuration	Yes
HTTP	80 (TCP)	Closed	Open after configuration	No
HTTPS	443 (TCP)	Closed	Open after configuration	Yes

* Some service providers consider the opening of port 102 a security vulnerability. To avoid opening port 102 during online diagnostics, see section Online security diagnostics via port 8448 (Page 94).

Ports of communication partners and routers

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

These can be:

- TeleControl Basic / 55097 (TCP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- SINEMA RC Autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)

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.

The following description applies to applications without telecontrol communication.

Configuration of the telecontrol communication

You will find the description on configuring the telecontrol communication in the configuration manual /3/ (Page 116).

Overview of the configuration steps in STEP 7

Notes:

- No Ethernet network needs to be created for the communication via the mobile wireless network.
- When enabling the security functions, you must create a network and at least network the interface so that the configuration data can be compiled.

Follow the steps below when configuring:

1. Create a STEP 7 project.
2. Create the necessary SIMATIC stations with the required modules and CPs.
3. Configure the CPs including the messages (e-mail / SMS).
4. If required, create the program blocks for S7 communication and Open User Communication and configure them as needed.
5. Save and compile the project.
6. 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.

Information required for the configuration

Information required for telecontrol communication

The information you need for this application is available in the configuration manual /3/ (Page 116).

Information required for mobile wireless communication

The following information is required for configuring a mobile wireless CP that uses e-mail and SMS messages but not telecontrol communication:

- Own phone number of the CP
- APN
Name of the access point (APN) from the mobile wireless network to the Internet (information from the mobile wireless network provider)
- APN user name
User name for the access point of the mobile wireless network provider
- APN password
Password for the access point of the mobile wireless network provider
- Node number of the SMS master station (SMSC) when using SMS
- PIN of the SIM card

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

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

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

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

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

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

4.3 Communication types

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

To minimize the risk of unauthorized access to the station via CP, you need to enable the communication 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 telecontrol communication on the CP.

Select the telecontrol protocol via the drop-down list "Protocol type".

- TeleControl Basic
- DNP3
- IEC 60870-5

Note that if you change the telecontrol protocol later, all protocol-specific data will be deleted. This includes the data point and partner information.

You can find additional information in the configuration manuals /3/ (Page 116).

- **Activate telecontrol communication via SINEMA Remote Connect**

Enables communication in the CP via SINEMA RS.

You can find the application cases of SINEMA Remote Connect and configuration notes on these applications in the section Communication via SINEMA RC (Page 15).

You can find additional information in the configuration manuals /3/ (Page 116).

For the SINEMA Remote Connect - Server manual, see /5/ (Page 116).

- **Enable 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 remains possible, however.

- **Enabling S7 communication to the CPU**

Enables the functions of S7 communication between the engineering station and the station CPU, as well as S7 routing.

If you configure S7 connections to the relevant station, and these run via the communication module, you need to enable this option for the communication module.

Please note:

Disabling this function means no security measure. To protect the station, use suitable security functions such as firewall, VPN or password protection of the CPU.

- **Enabling SMS**

Enables sending and receiving of SMS messages.

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

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

4.4 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.

"GPRS (2G)" is only supported by CP 1243-7 LTE EU.

- **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.

The CP supports APNs with IPv4 and IPv6 addresses.

Note the information on security in the section Security recommendations (Page 41).

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.

Note**Configuration of APN user name and password**

If your service provider requires an APN user name and a password, you can receive the information from them.

If your service provider does not require an APN user name or a password, it can be necessary to configure placeholders for the two parameters. This is the case, for example, when your provider uses the Provider Password Authentication Protocol (PAP) for authentication. In this case, ask your provider for the required details.

User names and passwords can contain up to 64 characters. You will find the characters permitted in the section Character set for passwords and messages (Page 76).

If your service provider does not require an APN user name or a password, it sometimes makes sense to configure placeholders for the two parameters.

"List of preferred networks"

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

"TeleService settings"

TeleService can only be used when telecontrol communication is enabled. For a description of the TeleService functions, refer to the configuration manual, see /3/ (Page 116).

4.5 Ethernet interface [X1]

4.5.1 Ethernet addresses

The Ethernet interface with mobile wireless CPs

Mobile wireless CPs do 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

Here you configure the IP address of the CP and 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.

IP protocol

- **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.

Please note:

A fixed IP address (IPv4/IPv6) is required for the following applications:

- When using S7 communication
- When receiving data via Open User Communication
- When using VPN
- When using SINEMA Remote Connect

- **Use IPv6 protocol**

In addition to IPv4, you can optionally enable IPv6 for the CP.

IPv6 is supported as of hardware product version 3 of the CP.

4.5.2 Advanced options

TCP connection monitoring

The settings made here apply globally to all configured TCP connections of the CP.

- **TCP connection monitoring time**

Function: If no data traffic takes place within the TCP connection monitoring time, the communication module sends a keepalive frame to the communication partner and expects an answer within the TCP keepalive monitoring time.

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

- **TCP keepalive timeout**

After sending a keepalive frame, the communication module expects a response from the communication partner within the keepalive monitoring time. If the module does not receive a response within the configured time, it closes the connection and tries to set it up again.

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

4.5.3 Access to the Web server

Access to the Web server of the CPU

The Web server is located in the CPU. Via the CP, you have access to the Web server of the CPU.

You can access the Web server of the station via Ethernet or the Internet.

Recommendation for slow transmission paths: Set a larger refresh cycle of the Web browser.

4.6 Time-of-day synchronization

Note

Time-of-day synchronization of the CP

With applications that require time-of-day synchronization, 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 an external clock at intervals of approximately 10 seconds is recommended. This achieves as small a deviation as possible between the internal time and the UTC time.

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.

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.

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

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 is where you configure when 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 CPU

- **Telecontrol communication disabled, security enabled**

- NTP
- NTP (secure)
- Time from CPU

- **Telecontrol communication and security enabled**

- Time from partner
- NTP
- NTP (secure)
- Time from CPU

Synchronization method of the CP

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

- **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 NTP (secure) method can be used when the security functions are enabled. It uses authentication with symmetrical keys. Various configurable hash algorithms are available for the integrity check.

In the global security settings, you can create and manage NTP servers of the type NTP (secure).

On the CP you specify the servers used.

- **Time from CPU**

As of V4.2, the CPU can synchronize all CMs/CPs of the station in a synchronization cycle of 10 seconds.

Parameters of the CPU:

If the option "CPU synchronizes the modules of the device" is enabled, you can initiate synchronization of all telecontrol CPs of the station with firmware $\geq$ V2.1.77 with the CPU time in a synchronization cycle of 10 seconds.

- **No time-of-day synchronization configured**

If no time synchronization is configured at the CP, the time of the CP can be synchronized under the following condition:

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

- **Time from partner**

With enabled telecontrol communication: The CP adopts the time-of-day from the communications partner.

You will find the description in the configuration manual /3/ (Page 116).

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:

- Forwarding of the CP time to the CPU using a PLC tag
 - 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 < V3**

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 ≥ V3.0 and CPU firmware ≥ V4.2**

If both modules in a station have one of the mentioned firmware versions, the time of the CP can be forwarded automatically to the CPU.

A condition for this is: The "CPU synchronizes the modules of the device" option is selected for the CPU under "PROFINET Interface > Time-of-day synchronization".

Then all intelligent modules of the station are synchronized with the CPU time.

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

4.7 DNS configuration

Configuring DNS servers

A DNS server may be required when the module itself, a communication partner, or an NTP or e-mail server, for example, should be reachable via the host name (FQDN).

When addressing a communication partner as FQDN, you need to configure a DNS server. The IP address (IPv4/IPv6) of the communication partner is determined via the configured DNS server. When using IPv6 addresses, make sure to configure the DNS servers accordingly.

When the CP uses mobile wireless service and the mobile wireless provider operates a DNS server in its network, the configuration has the following effects:

- No configuration of a DNS server

IP addresses are automatically obtained from the DNS server of the network operator (recommended procedure).

- Configuration of a DNS server

IP addresses are obtained from the configured DNS server. DNS servers of the network provider are not taken into account.

4.8 Communication with the CPU

Communication with the CPU

The first four parameters are only relevant for telecontrol communication.

Watchdog bit

- **CP monitoring**

The CP checks the connection with the CPU via the watchdog bit.

The CP transfers the bit to the CPU every 5 seconds and resets it in the next CPU sampling cycle. The bit is not transferred in the event of connection faults. This signals the connection fault to the CPU.

The PLC tag of the watchdog bit must be evaluated by the user program.

CP time

- **CP time to CPU**

The function allows the CPU to read the time of day of the CP. Using this approach, the CP can synchronize the CPU time.

Procedure:

- The CPU sets the input "Time trigger variable" (BOOL) to 1 with the user program.
- The CP then writes its time to the "CP time variable" (DTL) and resets the "Time trigger variable" value to 0.
- The user program reads the "CP time variable" to set the CPU time.

Recommendation:

Set the "Time trigger variable" no more frequently than once per second to avoid placing an unnecessary communication load on the backplane bus.

Note

Refer to the information in the section Time-of-day synchronization (Page 51).

CP diagnostics

In the parameter group "CP diagnostics", you have the option of providing the CPU with advanced diagnostics data of the CP using PLC tags.

You can display the states of the PLC tags via the Web server of the CPU.

- **Enable advanced CP diagnostics**

Enable the option to use advanced CP diagnostics.

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

The following PLC tags for the individual items of diagnostics data can be enabled selectively.

- **Diagnostics trigger tag**

If the PLC tag (BOOL) from the user program of the CPU is set to 1, the CP updates the values of the following PLC tags for the advanced diagnostics.

After writing the current values to the following PLC tags, the CP sets the "Diagnostics trigger tag" to 0, signaling to the CPU that the updated values can be read from the PLC tags.

Note

Fast setting of the diagnostics trigger tag

Trigger should not be set more often than once per second.

Depending on the CP type and the supported functions, PLC tags can be configured for the following diagnostics data:

- **Frame memory overflow warning**

- Only relevant for telecontrol communication -

- **Frame memory occupation**

- Only relevant for telecontrol communication -

- **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**
- Only relevant for telecontrol communication -
- **Date of last unsuccessful logon to TCSB**
- Only relevant for telecontrol communication -
- **TeleService status**
- Only relevant for telecontrol communication -
- **VPN IPsec status**
The PLC tag (BOOL) indicates whether a VPN IPsec tunnel is established:
 - 0 = No tunnel established
 - 1 = Tunnel established
- **Connection to SINEMA Remote Connect**
The PLC tag (BOOL) indicates whether an OpenVPN tunnel to SINEMA RC is established:
 - 0 = No tunnel established
 - 1 = Tunnel established

4.9 Security

For a description of the telecontrol-specific parameters, refer to the relevant configuration manual /3/ (Page 116).

4.9.1 Security user

Creating a security user

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

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

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

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

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

4.9.2 Firewall

4.9.2.1 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.

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

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

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

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

4.9.2.3 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 58) for information on this.

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

Setting the firewall for online functions

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

Global security functions:

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

Local security functions of the CP:

Now select the CP in the S7 station.

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

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

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

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

4.9.3 Time-of-day synchronization

You can find the description of the parameters in the section Time-of-day synchronization (Page 51).

4.9.4 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. You configure these phone numbers in the "Authorized phone numbers" list.

"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.

4.9.5 E-mail configuration

Configuring e-mails

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), you configure the individual e-mails, see section Messages (Page 70).

Requirements for e-mail

Note the following requirements in the CP configuration for the transfer of e-mails:

- The security functions are enabled.
- The time of the CP is synchronized.

For the configuration, you require the data of the SMTP server and the user account:

- Server address, port number, user name, password, e-mail address of the sender (CP)
- With encrypted transfer: Server certificate

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.

On configuration of the passwords, see Character set for passwords and messages (Page 76).

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 67).

4.9.6 VPN

4.9.6.1 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.

4.9.6.2 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.

4.9.6.3 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.

4.9.6.4 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.

4.9.6.5 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

4.9.6.6 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect Server

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

- Exporting the CA certificate (optional)

If you want to use the server certificate as authentication method of the communications module during connection establishment, export the CA certificate from SINEMA RC Server.

Then import the CA certificate from SINEMA RC Server to the engineering station.

Alternatively, you can use the fingerprint of the server certificate as authentication method of the communications module. The fingerprint's duration of validity may be shorter than that of the certificate.

Please note that you need to repeat the import of a certificate in the event of a module replacement.

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- CA Certificate

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

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

- Fingerprint

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

Authentication

- Device ID

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

- Device password

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

Max. number of characters: 127

Optional settings

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

- **Update interval**

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

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

- **"Connection type"**

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

- Auto

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

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

- PLC trigger

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

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

Note**Connection abort**

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

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

- **PLC tag for connection establishment**

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

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

4.9.7 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 by either:
 - Using the "Trusted certificates and root certification authorities" table in the global security settings
 - Using the "Certificates of the partner devices" table in the local certificate manager of the module (security)

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

For a description of the procedure, refer to the section Handling certificates (Page 68).

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

4.9.8 Handling certificates

Certificate for authentication

If you have configured secure communication with authentication for the communication module, own certificates and certificates of the communication partner are 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.

For the module to 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 module with third-party certificates, follow the steps below:

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

The steps are described in the following sections.

Importing third-party certificates from communications partners

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

1. Save the third-party certificate in the file system of the PC of the connected engineering station.
2. In the STEP 7 project open the global certificate manager:
Global security settings > Certificate manager
3. Open the "Trusted certificates and root certification authorities" tab.

4. Click in a row of the table can select the shortcut menu "Import".
5. In the dialog that opens, import the certificate from the file system of the engineering station into the STEP 7 project.

Assigning certificates in the global security settings

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

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

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

Assigning certificates locally

To be able to use an imported certificate for the module, the certificate needs to be displayed in the "Security" parameter group of the module. Follow the steps outlined below:

1. Select the module in the STEP 7 project.
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 module.

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

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

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 module.

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

4.10 Data points

For a description of the telecontrol-specific parameters, refer to the relevant configuration manual /3/ (Page 116).

4.11 Messages

Configuring messages

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

- E-mails

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

- SMS (only mobile wireless CPs)

The recipient can be a mobile phone or an S7 station.

You configure the messages with the message editor of the CP. Alternatively, you will find it:

- Via the shortcut menu of the CP
- Via the project navigation: Directory of the station > Local modules > CP

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 47).

You will find the characters permitted for message texts and additional parameters in the section Character set for passwords and messages (Page 76).

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

E-mails

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 perform 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 60).
- 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"

SMS

Required information:

- Number of the SMSC

You perform 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.

Configuration in the message editor

You configure the messages in STEP 7 in the data point and message editor. Alternatively, you can open the editor:

- By selecting the communications module
Shortcut menu "Open the data point and messages editor"
- Via the project navigation:
Project > directory of the relevant station > Local modules > required communications module

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

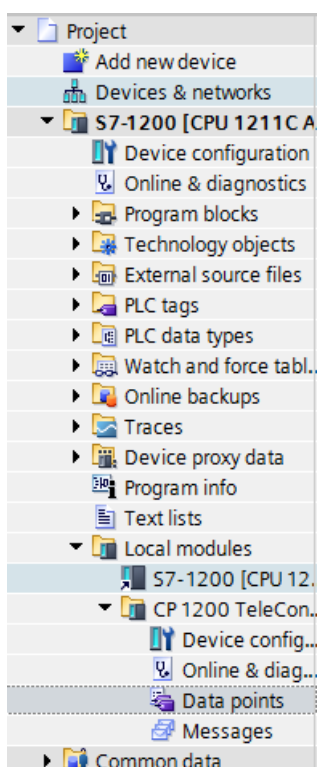


Figure 4-1 Opening the message editor via the project navigation

After opening the editor 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

The data point editor is only relevant for the telecontrol communication.

Creating objects

You create a new object (message) by double clicking "<Add object>" in the first table row with the grayed-out entry.

You can change the default name to suit your purposes, but it must be unique within the module.

Arranging columns and rows, showing/hiding columns

As with many other programs, you can arrange the columns and sort the table according to your needs:

- 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 right-click on a column header:
"Optimize width", "Optimize width of all columns"
- If you move the cursor close to the right limit of a column header, the following symbol appears:



When it does, double-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 right-click on a column header.

Copy messages

You can copy and paste messages. If you right-click in the row of an object in the table, you can access the functions listed below from the shortcut menu:

- Cut
- Copy
- Paste

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

You can also paste cut or copied objects into tables of other communications modules of the same type and with the same telecontrol protocol.

- Delete

If you hold down the <Ctrl> key, you can select several rows that are not contiguous.

If you hold down the <Shift> key, you can select the beginning and the end of a contiguous area.

Tab for configuring the messages

Select a message in the "Messages" table. You configure the parameters of this selected message in the tabs below the table.

"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.

Depending on the module used and the enabled services, you can select the following triggers:

- **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" that is set by the user program is evaluated. 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 memory area 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.

Note

Fast setting of the diagnostics trigger tag

Trigger should not be set more often than once per second.

- **CPU changes to STOP**

- **CPU changes to RUN**

- **Connection to a partner interrupted**

Triggers the sending of the message when the telecontrol connection to a partner is interrupted.

- **Connection to a partner established**

Triggers the sending of the message when the telecontrol connection returns.

- **Connection establishment to partner failed**

Triggers the sending of the message when the telecontrol connection to a partner could not be established.

- **TeleService session started**
Triggers the sending of the message when telecontrol communication is enabled and a TeleService connection is established.
- **TeleService session ended**
Triggers the sending of the message when telecontrol communication is enabled and a TeleService connection has been terminated.
- **Weak mobile wireless network**
(SMS only)
If the mobile wireless connection for telecontrol communication is too weak, an SMS message is triggered and sent to the configured recipient.
- **VPN connection established**
Triggers the sending of the message when the VPN connection is established or returns.
- **VPN connection terminated**
Triggers the sending of the message when the VPN connection is interrupted.
- **SINEMA RC connection established**
Triggers the sending of the message when the OpenVPN connection is established or returns.
- **SINEMA RC connection terminated**
Triggers the sending of the message when the OpenVPN connection is interrupted.
- **PLC tag for trigger**
PLC tag for the trigger "Use PLC tag"
- **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 the "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 94).
- **PLC tag for processing status**
PLC tag of the type DWORD for the processing status
- **Include value**
When the option is enabled, the CP sends a value from the memory area of the CPU for the placeholder \$\$ 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 \$\$.

\$\$ as placeholder for the values of data points supports the following data types:

- Bool, Byte, Char, Int, UInt, Word, DWord, UInt, DInt, Real, String,
- Arrays of the data types above

Note that the number of characters increases with the value. For the maximum number of characters, refer to the configuration limits.

- **PLC tag for value**

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

4.12 Character set for passwords and messages

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

The following permitted characters apply to:

- APN, e-mail server:
User names and passwords
- CP identification:
Telecontrol password
- Messages in the message editor:
Message texts

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

- 0x20
Space
- 0x21 ... 0x5F
!"#\$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN 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
| ~

In addition for message texts:

- Manual line break (↵)
In message texts, you can insert a line break using <Shift>+<Enter>.

Program blocks

5.1 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

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

In contrast to telecontrol communication, Open User Communication does not need to be enabled in the configuration because the 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**No different program block versions**

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

Requirements for Secure OUC

Requirements for the use of the secure transmission via Secure OUC:

- STEP 7: As of V16
- CPU firmware: As of V4.4
- CP firmware: As of V3.2

Supported program blocks for OUC

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

- **TSEND_C V3.0 / TRCV_C V3.0**

Compact blocks for:

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

As an alternative, use:

- **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 IP parameters

Refer to the information on T_CONFIG and on the SDTs "IF_CONF_..." in the section TC_CONFIG for changing configuration data of the CP (Page 83).

The address parameters can only be configured with temporary validity. 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 not created by selecting an entry from the "Data type" drop-down list in the declaration table of the block, but by entering the name manually in the "Data type" box, for example "TCON_IP_V4".

The corresponding SDT is then created with its parameters.

Usable SDTs

- **TCON_IP_V4**
For transferring frames via TCP or UDP
- **TCON_QDN**
For TCP or UDP communication via the fully qualified domain name (FQDN) (IPv4)
- **TCON_IP_RFC**
For transferring frames via ISO-on-TCP (direct communication between two S7 stations)
- **TADDR_Param**
For transferring frames via UDP
- **TMail_V4**
For transferring e-mails addressing the e-mail server using an IPv4 address

Recommendation for mobile wireless applications:

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)
- **TCON_IP_V4_SEC**
For the secure transfer of data via TCP
- **TCON_QDN_SEC**
For the secure transfer of data via the host name
- **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

Note on TMail_Vx_SEC / TMail_QDN_SEC:

With these SDTs, the mail server certificate is checked, but not the ID of the "TLSServerCertRef" (STEP 7 internal reference) certificate.

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 sending SMS messages in the section SMS messages via OUC (Page 80).

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 parameter assignment.

5.2 SMS messages via OUC

Sending e-mails / SMS messages via OUC

With mobile wireless CPs, you only require the program blocks and system data types (SDTs) described below to transfer SMS messages using Open User Communication (OUC).

In contrast, the event-driven sending of e-mails or SMS messages is independent of program blocks and is configured in STEP 7 in the message editor of the respective module.

SMS messages via program blocks

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 enter 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, parameterize the message text to be read out in the TRCV / TRCV_C blocks 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 has 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 mobile wireless 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.

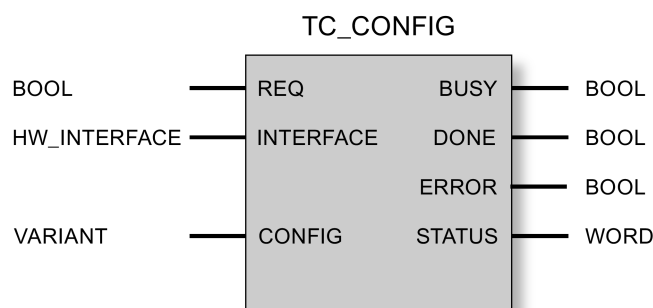
The configuration data to be modified on the CP is put together as necessary in blocks in IF_CONF "IF_CONF_..." for the individual parameters.

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 settings for IF_CONF, refer to the section IF_CONF: SDT for the configuration data of the CP (Page 85).

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	Range of 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.
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	0000H	Job executed without errors
0	0	7000H	No job processing active (first block call)
0	0	7001H	Job processing started (first block call)
0	0	7002H	Job processing already active (renewed block call when BUSY = 1)
0	1	80E0H	Internal error
0	1	80E6H	No query in progress (block call not started)
0	1	80EBH	Query temporarily rejected (the CP is currently being configured by STEP 7)
0	1	80F6H	Format error of a parameter in the called data block (wrong length, wrong format or invalid value) Check the "IF_CONF" SDT.
0	1	80F7H	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 mobile wireless 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.

5.4 IF_CONF: SDT for the configuration data of the CP

- 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.

- 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.
- Repeat the last step for all parameters you want to change on the CP using the TC_CONFIG instruction.
- 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)
SMSPProvider	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 as 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

6.1 Diagnostics options

The following diagnostics options are available:

LEDs of the module

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

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

Here, you can obtain the following information 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 in 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 115).

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 time.

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

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

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

Diagnostics options of the telecontrol server

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

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

- ConnectionState
- PLCCConnected
- 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.

TeleService

For a description of the TeleService functions, refer to the respective configuration manual, see /3/ (Page 116).

6.2 Online security diagnostics via port 8448

Security diagnostics via port 8448

Requirements:

- With an activated firewall, access must be enabled.

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

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

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

6.3 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 processing status is returned by the module itself or the servers of the service after transfer of a message to be sent.

E-mails sent via program blocks of Open User Communication return a different status via the block (see block help).

The returned statuses of the Messages configured in the message editor have the following meaning:

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.
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.

Status	Meaning
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.

6.4 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 the Siemens Industry Online Support.

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

Note

Effects on the retentive memory of the CPU

- If you use a SIMATIC memory card to install the firmware file, the retentive memory is retained.
- If you use the online functions to install the firmware file, retentive memory is lost.

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

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.

6.5 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. Exception: The data of the SINEMA RC configuration and the certificate of the SINEMA RC server are saved in the CP. They cannot be read from the CPU.

When the device is replaced with a newer one, the safety standards of the replaced device are supported, rather than the latest safety standards.

If you replace a module, remember to take the SIM card from the old module and insert it in the new CP.

Technical specifications

7.1 General technical specifications

Table 7- 1 General technical specifications

Technical specifications		
Module name		Article numbers
- CP 1243-7 LTE-EU - CP 1243-7 LTE-US		6GK7 243-7KX30-0XE0 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 - Maximum	0.14 mm² (AWG 25) 1.5 mm² (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
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation

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

Technical specifications	
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	
Wireless interface		
Supported frequency bands	Mobile wireless standard	Band no./Frequency
	LTE FDD	• 1 / 2100 MHz • 3 / 1800 MHz • 7 / 2600 MHz • 8 / 900 MHz • 20 / 800 MHz • 28A / 700 MHz
	HSDPA+	• 1 / 2100 MHz • 3 / 1800 MHz • 8 / 900 MHz
	GSM / GPRS / EDGE	3 / 1800 MHz 8 / 900 MHz
Maximum transmit power	4G / LTE FDD	+23 dBm (Class 3)
	3 G / WCDMA	+21 dBm (Class 3)
	EDGE LB	+27 dBm (Class E2)
	EDGE HB	+26 dBm (Class E2)
	GSM LB	+33 dBm (Class 4)
	GSM HB	+30 dBm (Class 4)
	TD-SCDMA	+21 dBm (Class 3)
LTE	Transmission speed (maximum)	• Downlink: 150 Mbps • Uplink: 50 Mbps

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

Technical specifications - CP 1243-7 LTE-EU		
HSPA+	Transmission speed (maximum)	- Downlink (HSDPA): 42 Mbps - Uplink (HSUPA): 42 Mbps
EDGE	Properties	- Multislot class 10 - end device class B - coding scheme 1 to 9 (GMSK)
	Transmission speed (maximum)	- Downlink: 236.8 kbps - Uplink: 236.8 kbps
GPRS	Properties	- Multislot class 10 - device class B - coding scheme 1 to 4 (GMSK)
	Transmission speed (maximum)	- 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 of the wireless interface

Technical specifications - CP 1243-7 LTE-US		
Article number	6GK7 243-7SX30-0XE0	
Supported frequency bands	Mobile wireless standard	Band no./Frequency
	LTE FDD	2 / 1900 MHz 4 / 1700 MHz 5 / 850 MHz 12 / 700 MHz 13 / 700 MHz 14 / 700 MHz 66 / 1700 MHz 71 / 617-698 MHz
	HSDPA+	2 / 1900 MHz 4 / 1700 MHz 5 / 850 MHz
Maximum transmit power	4G / LTE FDD	+23 dBm (Class 3)
	3 G / WCDMA	+21 dBm (Class 3)
	TD-SCDMA	+21 dBm (Class 3)
LTE	Transmission speed (maximum)	- Downlink: 100 Mbps - Uplink: 50 Mbps
HSPA+	Transmission speed (maximum)	- Downlink (HSDPA): 42 Mbps - Uplink (HSUPA): 42 Mbps
SMS	Mode outgoing	MO
	Service	Point-to-point

7.4 Pin assignment of the socket for the external power supply

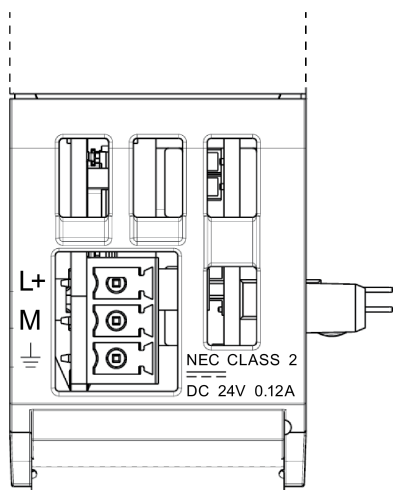


Figure 7-1 Socket for the external 24 VDC power supply (view from above)

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

Note

All dimensions in the drawings of the CP are in millimeters.

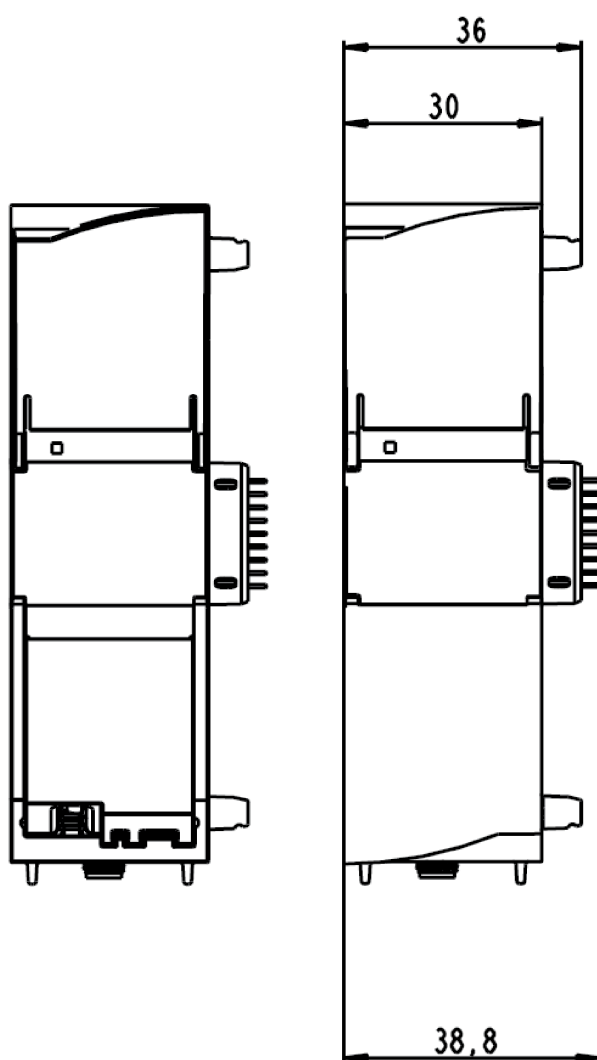


Figure A-1 Front view

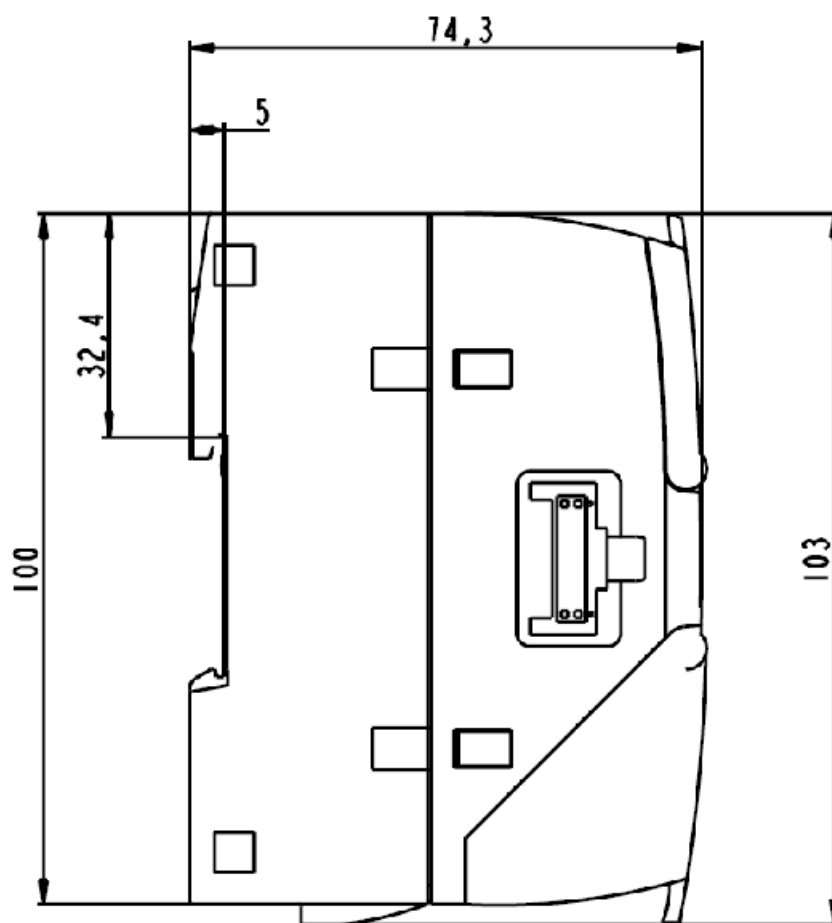


Figure A-2 Side view left

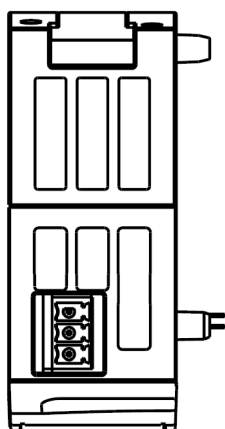


Figure A-3 From above

Approvals

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

EC declaration of conformity



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

- **2014/53/EU (Radio equipment / telecommunications directive)**

Directive of the European Parliament and of the Council of April 16, 2014 on the harmonization of the laws of the member states relating to placing radio equipment on the market and to cancel the directive 1999/5/EU

- **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
Digital Industries
P.O. Box 48 48
90026 Nuremberg
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 product meets the requirements of explosion protection according to IECEx.

IECEX classification:

- Ex ec IIC T4 Gc

Certificate: IECEx DEK 18.0018X

Applied standards:

- EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

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

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

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 34).

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

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

ATEX



The product meets the requirements of the EU directive 2014/34/EU "Equipment and protective systems intended for use in potentially explosive atmospheres".

ATEX approval:

- II 3 G Ex ec IIC T4 Gc

Type Examination Certificate: DEKRA 18 ATEX 0026X

Applied standards:

- EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

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

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 34).

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

- In the SIMATIC NET Manual Collection under "All documents" > "Use of subassemblies/modules in a Zone 2 Hazardous Area"
- On the Internet at the following address:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/78381013>)

R&TTE

The CP meets the requirements of the EC directive 1999/5/EC "Radio equipment and telecommunications terminal equipment" according to the requirements of article 3 (1) a, 3 (1) b and 3 (2).

Article 3 (1) a - Health and Safety

Harmonized standards:

- EN 60950-1+A11+A1+A12+A2
Information technology equipment - Safety - Part 1: General requirements
- EN 62311
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
Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments
- EN 61000-6-2+AC
Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN 61000-6-3+A1+AC
Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments

- EN 61000-6-4+A1

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

- EN 55022+AC Class A / B

Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement

- EN 55024

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 Accessories (Page 113).

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.



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



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

Antennas

The approved antennas for mobile wireless operation depend on the hardware product version of the CP. You will find the antenna permitted in the appendix Accessories (Page 113).

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

Approval Number TA-2015/1864

EAC (Eurasian Conformity)



Valid only for the CP 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

Depending on the hardware product version, the CP is permitted together with the following antennas for mobile wireless operation.

C.1 Antenna for CP as of hardware product version 3

The following antenna is available for use in mobile wireless networks and can be installed both indoors and outdoors. The antenna must be ordered separately.

Antenna ANT896-4ME



Figure C-1 Antenna ANT896-4ME

Short name	Order no.	Explanation
ANT896-4ME	6GK5896-4ME00-0AA0	Omnidirectional antenna for LTE networks (4G), GSM networks (2G) and UMTS networks (3G); weather-proof for indoor and outdoor areas, IP68, - 40 °.. + 70 °C, N-Connect female incl. toothed washer and nut.

The antenna must be ordered separately, see antenna accessories.

You will find detailed information in the documentation of the device. You will find this on the Internet on the pages of Siemens Industry Online Support at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/100699507>)

C.2 Antenna for CP as of hardware product version 2

Antenna ANT794-4MR

The quadband ANT794-4MR antenna is available for use in mobile wireless network networks. It can be installed both indoors and outdoors.

The antenna must be ordered separately.



Figure C-2 ANT794-4MR GSM/GPRS antenna

Short name	Order no.	Explanation
ANT794-4MR	6NH9 860-1AA00	Omnidirectional antenna for LTE networks (4G), GSM networks (2G) and UMTS networks (3G); weather-proof 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:

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

Documentation references

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/

/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 - TeleControl
Siemens AG
Configuration manuals of the protocols:
- TeleControl Basic
- SINAUT ST7
- DNP3
- IEC 60870-5
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21764/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
SINEMA Remote Connect - Server
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21816/man>)

Index

A

- Article number, 3
- AT&T, 11
- Authorized phone numbers, 59

C

- CDMA, 12
- Consistent data area, 20
- Cross-references (PDF), 6

D

- Data buffering, 20
- Direct communication, 13, 24
- Disposal, 8

E

- E-mail
 - Configuration, 71
 - Number of messages, 21
 - Program block (OUC), 77

F

- Firmware - version, 3
- Frame memory, 20

G

- Gateway (VPN), 64
- Glossary, 8

H

- Hardware product version, 3

I

- IMEI, 3
- Importing a certificate - e-mail, 60

- Inserting/removing a SIM card, 36
- Inter-station communication, 13
- IP address - fixed, 49
- IP configuration, 16
- IPv6, 49

L

- Logging server, 69

N

- NTP, 52
- NTP (secure), 53
- IPsec tunnel,

O

- Online diagnostics, 91
- Online functions, 47, 91
- OUC (Open User Communication), 77

P

- Passive VPN connection establishment, 64
- PIN
 - Configuration, 45
 - Incorrect entry, 45
- Port 8448, 94
- Program blocks, 14

R

- Recycling, 8
- Replacing a module, 97

S

- S7 connections
 - Enable, 46
- S7 routing, 14, 46
- Safety notices, 33
- Security, 17
- Security diagnostics, 94
- Send buffer, 20

Service & Support, 8
SIMATIC NET glossary, 8
SMS
 Configuration, 71
 Number of messages, 21
 Program block (OUC), 77
 Reception, 59
SMTPS, 60
SSL/TLS, 60
STARTTLS, 60
STEP 7 - version, 21

T

TCSB, 6
Telecontrol communication, 13
Time stamp, 20
Time-of-day synchronization, 16
Training, 8

U

User data, 20

V

VPN, 21, 61

W

Web server
 Access, 51
 Diagnostics data, 92
Wireless approvals, 110