SIEMENS

SIMATIC NET

S7-1200 - TeleControl
SIMATIC CP 1242-7 GPRS V2

Operating Instructions

Preface

Application and functions 1

LEDs and connectors 2

Installation, wiring, commissioning, removal 3

Configuration 4

Program blocks 5

Diagnostics and upkeep 6

Technical specifications 7

Dimension drawings A

Approvals B

Accessories C

References D

05/2024
C79000-G8976-C311-05

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 Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C311-05
Ⓟ 06/2024 Subject to change

Copyright © Siemens 2015 - 2024.
All rights reserved

Preface

Validity of this manual

This document contains information on the following product:

CP 1242-7 GPRS V2
Article number 6GK7 242-7KX31-0XE0
Hardware version 3
Firmware version V3.5

Communications processor for connection of the SIMATIC S7-1200 via GSM mobile wireless networks



Figure 1 CP 1242-7 GPRS V2

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.

Product names

- **CP / module / device**
  In this document, the term "CP" is also used instead of the full product name "CP 1242-7 GPRS V2".
- **TCSB**
  TeleControl Server Basic V3, OPC server for telecontrol communication

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

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

- **CP without telecontrol communication**
  The relevant configuration steps for these applications are described in this manual.
- **CP with telecontrol communication**
  You will find the complete description of the configuration and diagnostics for these applications in the Configuration Manual /3/ TeleControl configuration manuals (Page 112).

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

New in this edition

- New firmware version V3.5 with new functions:
  - Options for reconnecting to the mobile wireless network
  - Expansion of time synchronization functions
  - Improvements to telecontrol functions
    For a description, refer to the respective configuration manual; see "Structure of the documentation" below.
- Editorial revision

Replaced manual edition

Edition 12/2019

Current manual edition on the Internet

You will also find the current edition of this manual on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15921/man)

With the "E-mail on update" option, you an enable an automatic notification when new documents are published in SIOS for the selection you have made in the project tree.

Structure of the documentation

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

- **Operating instructions**
  - Application and functions (without telecontrol)
  - Requirements (CPUs, configuration software, etc.)
  - Hardware description
  - Installation, wiring, commissioning, operation
  - Configuration
    The section "Configuration" only describes the configuration of the telecontrol-independent functions.
    If you use telecontrol functions, read the respective configuration manual.
  - Diagnostics, maintenance
  - Technical specifications, approvals, accessories
- **Configuration manual TeleControl Basic**
  Valid for all SIMATIC NET communications modules that support the TeleControl Basic protocol.
  - Configuration and diagnostics in STEP 7 Professional (TIA Portal)

Required experience

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

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

Sources of information and other documentation

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

Cross-references

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

To return to the original page after jumping to a cross-reference, some PDF readers support the command <Alt>+<Left arrow>.

License conditions

Note

Open source software

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

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

- OSS_CP124x7_99.pdf

Firmware

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

Note on firmware/software support

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

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry.

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 customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

See also:
Security functions (Page 18)
Security recommendations (Page 41)

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 - 1 device with pictogram

Recycling and disposal



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

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

Keep to the local regulations.

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

SIMATIC NET glossary

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

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

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

Training, Service & Support

You will find information on Training, Service & 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 **13**

1.1 Connecting the S7-1200 to a GSM network 13

1.2 Communications services 14

1.3 PUT/GET: Restrictions in the CPU 15

1.4 Other services and properties 16

1.5 Security functions 18

1.6 Configuration examples - Intended operating environment 18

1.6.1 TeleControl 20

1.7 Configuration limits and performance data 21

1.8 Requirements for operation 22

2 LEDs and connectors **25**

2.1 Opening the housing 25

2.2 LEDs 26

2.3 Electrical connections 29

2.3.1 Wireless interface 29

3 Installation, wiring, commissioning, removal **31**

3.1 Important notes on using the device 31

3.1.1 Notices on use in hazardous areas 31

3.1.2 Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex 32

3.1.3 Notes on use in hazardous areas according to UL HazLoc and FM 32

3.2 Installation, removal and repairs in hazardous areas 33

3.3 Installing, connecting and commissioning 34

3.4 Notes on operation 40

3.5 Disassembly 40

4 Configuration **41**

4.1 Security recommendations 41

4.2 Configuration in STEP 7 44

4.3 Communication types 45

4.4 Mobile wireless communications settings 46

4.5 Ethernet interface [X1] 49

4.5.1 Ethernet addresses 49

4.5.2 Advanced options 50

4.5.3 MTU size 50

4.5.4 Access to the Web server ... 51
4.6 Time-of-day synchronization ... 51
4.7 Partner stations ... 55
4.8 DNS configuration ... 55
4.9 Communication with the CPU ... 56
4.10 Security ... 58
4.10.1 Security user ... 58
4.10.2 Time-of-day synchronization ... 58
4.10.3 Authorized phone numbers ... 59
4.10.4 E-mail configuration ... 59
4.10.5 Certificate manager ... 60
4.10.6 Handling certificates ... 61
4.11 Data points ... 64
4.12 Messages ... 64
4.13 Character set for passwords and messages ... 70
5 Program blocks ... 73
5.1 Program blocks for OUC ... 73
5.2 SMS messages via OUC ... 75
5.3 TC_CONFIG for changing configuration data of the CP ... 78
5.4 IF_CONF_*: SDTs for the configuration data of the CP ... 81
6 Diagnostics and upkeep ... 87
6.1 Diagnostics options ... 87
6.2 Processing status of messages ... 90
6.3 Firmware download ... 92
6.4 Module replacement ... 93
7 Technical specifications ... 95
7.1 Technical specifications of the CP ... 95
7.2 Pin assignment of the socket for the external power supply ... 97
A Dimension drawings ... 99
B Approvals ... 101
C Accessories ... 109
C.1 Antennas ... 109
D References ... 111
D.1 /1/ S7-1200 system manual ... 111
D.2 /2/ CP 1242-7 GPRS V2 ... 111
D.3 /3/ TeleControl configuration manuals ... 112
D.4 /4/ TeleControl Server Basic (version V3) ... 112

Index **113**

Application and functions

1

1.1 Connecting the S7-1200 to a GSM network

The CP is intended for use in industrial environments.

IP-based WAN communication via GSM

Using the CP, the S7-1200 SIMATIC controller can be connected to GSM networks. The CP allows the following types of WAN communication:

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

The CP supports the following services for communication via the GSM network and the Internet:

- GPRS (General Packet Radio Service)
  The packet-oriented service for data transmission "GPRS" is handled via the GSM network.
  Note: The CP is not suitable for GSM networks in which the code multiplex method "Code Division Multiple Access" (CDMA) is used.
- SMS (Short Message Service)
  The CP can send and receive SMS messages.
- E-mail
  The CP can send e-mails via the GSM network and the Internet.

The CP supports the following frequency bands:

- 850 MHz
- 900 MHz
- 1 800 MHz
- 1 900 MHz

You will find the countries in which the CP is approved on the Internet on the pages of Siemens Industry Online Support.

Link: (www.siemens.com/mobilenetwork-approvals)

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

1.2 Communications services

The CP 1242-7 GPRS V2 is intended for use in an industrial environment. The following applications are supported by the CP:

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.

Telecontrol communication

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

- Communication with a control center
  Remote S7-1200 stations communicate via the mobile wireless network and the Internet with a telecontrol server in the master station. The telecontrol server communicates with a higher-level control system using the integrated OPC server function.
- Event-driven sending of messages using SMS or e-mail
  Via the mobile wireless network, the CP sends SMS messages to mobile phones or e-mails to PCs with an Internet connection.
  Both types of messages are configured in telecontrol communication in STEP 7. The use of program blocks is not necessary.
  For information on the configuration, refer to sections E-mail configuration (Page 59) and Messages (Page 64).
- Inter-station communication between S7-1200 stations via the telecontrol server
  In this application, the CP establishes a connection to the telecontrol server via the mobile wireless network. The telecontrol server forwards the messages to the destination station.

For this communications service, the CP and TCSB use their own protocol on OSI layer 7 that among other things supports certain security functions, see section Security functions (Page 18).

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 telecontrol communication services (see above), OUC program blocks need to be used to transfer SMS/e-mails; see section Program blocks for OUC (Page 73).

You will find examples of applications in the section TeleControl (Page 20).

S7 communication

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

The following instructions are supported:

- PUT / GET
  You will find details on the program blocks in the information system of STEP 7
- S7 routing
  As of CP firmware V2.1 with CPU ≥ 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 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/ TeleControl configuration manuals (Page 112).

1.3 PUT/GET: Restrictions in the CPU

Communications services without connections

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

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

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

A prerequisite for enabling this option is enabling an access option in the "Access Control > Access level" parameter group. Set the option "Read access" or "Full access".
Note: This setting is connected with security restrictions.

When the "No access (complete protection)" option is enabled, PUT/GET communication cannot be enabled.

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

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

The activation of communication services described below applies to the use of the communications module together with a CPU V4.0 to V4.6.

- Option enabled
  Access to CPU data from the client side via the communications module using PUT/GET is possible.
- Option disabled
  Access to CPU data from the client side via the communications module using PUT/GET is not possible.

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

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

Configuring PUT/GET

You can find additional information on the following Siemens Industry Customer Support page in the documentation specified in the "Download" section:
Link: (https://support.industry.siemens.com/cs/ww/en/view/82212115)

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

Security functions of the CP

The CP supports the following security functions:

- **TeleControl Basic**
  - **Encrypted telecontrol communication**
    As an integrated (unconfigurable) security function, the TeleControl Basic protocol encrypts the data for transfer.
    You configure the interval of the key exchange between the CP and telecontrol server in STEP 7 in the parameter group "Ethernet interface (X1) > Advanced options > Transmission settings".
  - **Authorized phone numbers**
    To authorize nodes allowed to establish a connection to the CP (e.g. mobile phones), an authorized phone number is configured for each subscriber.
  - **Telecontrol password**
    To authenticate the CP with the telecontrol server
- **STARTTLS / SMTPS**
  For the secure transfer of e-mails
- **NTP (secure)**
  NTP with support of RFC5905 and RFC5906 with shared key for secure transfer during time-of-day synchronization
- **HTTPS**
  For secure access to the Web server of the CPU

Note

Plants with security requirements - recommendation

If you have systems with high security requirements, use the secure protocols NTP (secure) and HTTPS.

1.6 Configuration examples - Intended operating environment

You will find example system configurations as intended operating environment for use of the CP below.

For protection of the company and plant network, the following security components are recommended:

- External firewalls with Intrusion Detection System (IDS) protect the company network against external attacks.
- DMZ firewalls in the backbone level protect the plant network.
- Security modules protect each individual automation cell.

Note

Security information

To protect your system, refer to the information in the section Security recommendations (Page 41).

Sending SMS messages and e-mails

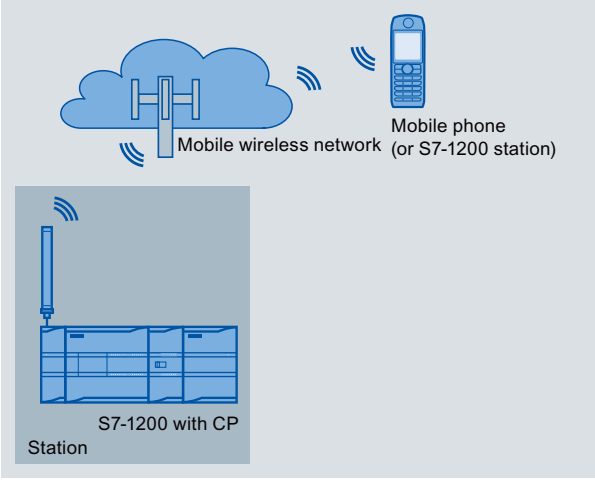


Figure 1-1 Sending messages by SMS from an S7-1200 station

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 that are sent or received due to calling the corresponding program blocks of 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 87).
  For all mobile phones that send SMS to the CP, the authorized 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 to the CP, the authorized phone number must be specified in the STEP 7 configuration of the CP (parameter group "Security > Authorized phone number").

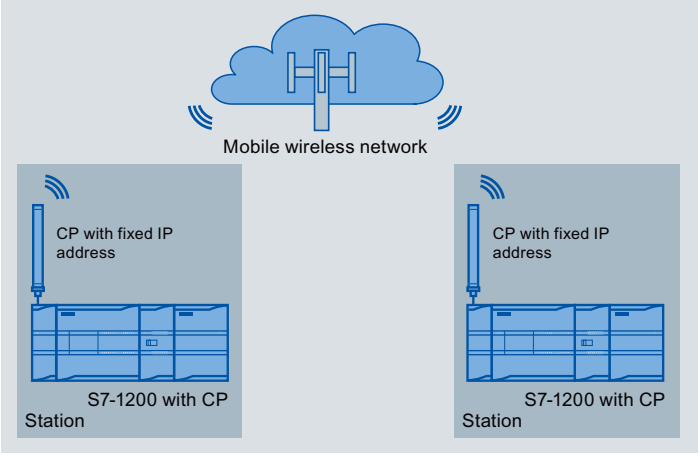


Figure 1-2 Direct communication between two S7-1200 stations

1.6.1 TeleControl

You can find configuration examples for applications with telecontrol communication in the configuration manual; see /3/ TeleControl configuration manuals (Page 112).

1.7 Configuration limits and performance data

Number of connections for the telecontrol communication

- 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:
  - Receive from partners: Max. 15
  - Send to partner: Max. 3 ("Send buffer" parameter enabled)

Number of simultaneous TeleService connections

- Max. 1 TeleService connection

Number of simultaneous connections for S7 communication and Open User Communication

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

The maximum number can be divided up as follows:

- S7 connections: Maximum 8
- OUC connections: Maximum 8
  - TCP connections
  - ISO-on-TCP connections
  - UDP connections
- Additional free resources for S7 or OUC connections: Maximum 6

Number of connections to NTP servers

- Max. 1 connection to an NTP server
- 4 servers configurable

User data

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

User data per frame with the various connection types:

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

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

Number of data points for the data point configuration

The maximum number of configurable data points is 200.

Frame memory (send buffer)

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

The send buffer has a maximum size of 64 000 event messages divided into equal parts for 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 to be sent as e-mails or SMS can be configured in STEP 7.

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

1.8 Requirements for operation

Hardware requirements

The following hardware is required in the S7-1200 to use the CP with the current firmware version:

- CPU
  - The full functionality of the CP with the current firmware version is available with a CPU as of V4.6.
  - The CP with firmware version V3.0 (hardware version 2) is compatible with a CPU as of V4.1.
  - The CP up to firmware version V2.1 (hardware version 1) is compatible with a CPU up to firmware version V3.0.
- An external antenna for the CP
  Use only the antenna from the accessories program for the CP, refer to the appendix Antennas (Page 109).

Configuration software

To configure the module's full scope of functions in the current firmware version, the following configuration tool is required:

- STEP 7 Basic / Professional V19 Update 1

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 14).

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 Other services and properties (Page 16).
- 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 Security recommendations (Page 41).

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/ TeleControl Server Basic (version V3) (Page 112).
- 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/ TeleControl configuration manuals (Page 112).

LEDs and connectors

2

2.1 Opening the housing

Location of the display elements and the electrical connectors

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

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

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

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.

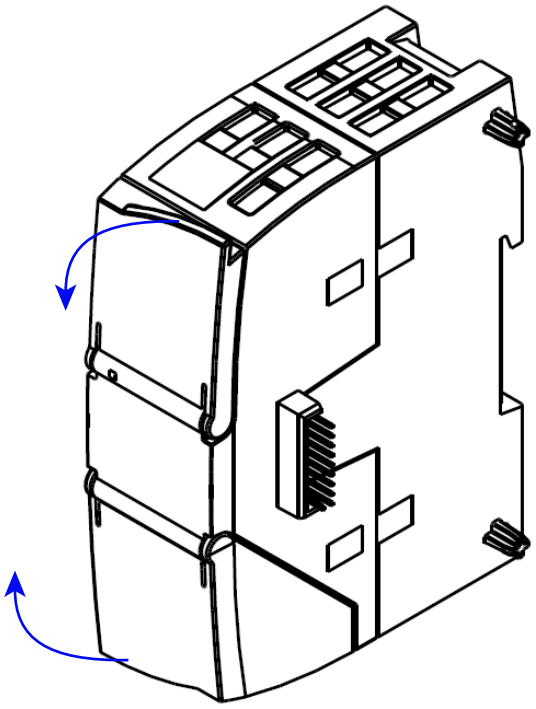


Figure 2-1 Opening the housing

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	TELESERVICE	Status of the TeleService connection

Note

LED colors when the module starts up

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

Display of the operating and communication status

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

Table 2-3 Meaning of the LED symbols

Symbol	○	● ● ●	☀ ☀ ☀	-
LED status	OFF	ON (steady light)	Flashing	Not relevant

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

DIAG (red / green)	**NETWORK (red / green)**	**CONNECT (green)**	**SIGNAL QUALITY (yellow / green)**	**TELESERVICE (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					
-	●	-	-	-	Connection exists to the GPRS service in the GSM network
-	○	-	-	-	No connection to the GPRS service in the GSM network
Connection to communications partners					
● green	●	●	-	-	Connection established to at least one partner, CPU in RUN

DIAG (red / green)	NETWORK (red / green)	CONNECT (green)	SIGNAL QUALITY (yellow / green)	TELESERVICE (green)	Meaning
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
TeleServiceconnection					
-		-	-		TeleService connection established
-	-	-	-		No TeleService connection established
Quality of the mobile wireless connection					
-	-	-		-	Good network (≥ -73 dBm)
-	-	-		-	Medium strength network (-89 ... -74 dBm)
-	-	-		-	Weak network (-109 ... -90 dBm)
-	-	-		-	No network (≤ -110 dBm)
flashing red	-	-		-	Missing external power supply
Loading firmware					
					Loading firmware. The "DIAG" LED flashes alternating red and green.

DIAG (red / green)	NETWORK (red / green)	CONNECT (green)	SIGNAL QUALITY (yellow / green)	TELESERVICE (green)	Meaning
flashing green					Firmware was successfully loaded.
flashing red					• Error loading firmware or • Internal error of the CP; remedy: Power OFF → ON

2.3 Electrical connections

2.3.1 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 Antennas (Page 109).

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 97).

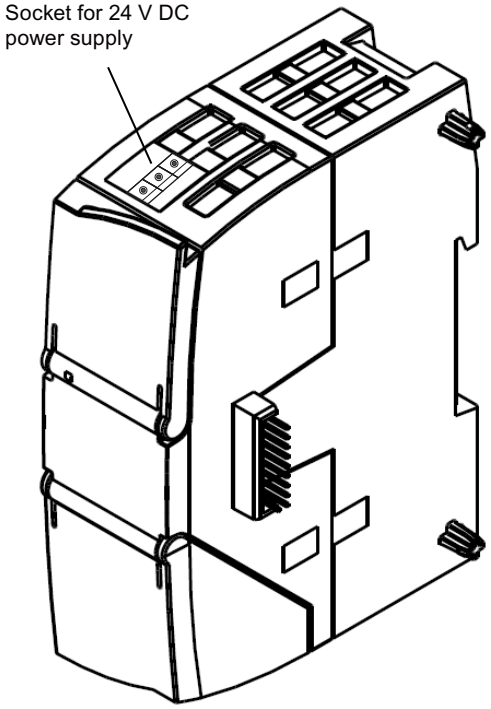


Figure 2-2 Socket for the 24 V DC power supply

More detailed information on the electrical connections

For technical information on the electrical connections, refer to the section Technical specifications (Page 95).

Installation, wiring, commissioning, removal 3

3.1 Important notes on using the device

Safety notices on the use of the device

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

Overvoltage protection

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

3.1.1 Notices on use in hazardous areas

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

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

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

WARNING

Requirements for the cabinet

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

WARNING

Suitable cables at high ambient temperatures in hazardous area

At an ambient temperature of ≥ 60 °C, use heat-resistant cables designed for an ambient temperature at least 20 °C higher. The cable entries used on the housing must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB/T 3836.1.

WARNING

If the cable or conduit entry point exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 60 °C, only use cables with admitted maximum operating temperature of at least 80 °C.

WARNING

Transient overvoltages

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

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

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

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

WARNING

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

WARNING

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

WARNING

EXPLOSION HAZARD

The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

3.2 Installation, removal and repairs in hazardous areas

WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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

WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

WARNING

Improper installation of shielded cables

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

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

⚠ WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

⚠ WARNING

Unprotected cable ends

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

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

⚠ WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

⚠ WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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

3.3 Installing, connecting and commissioning

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

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

⚠ WARNING

Open equipment

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

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

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)".

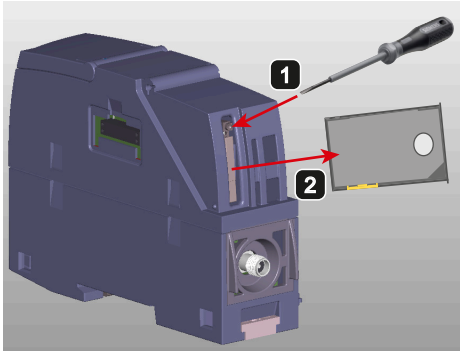
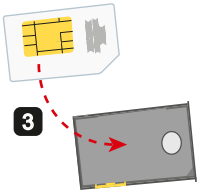
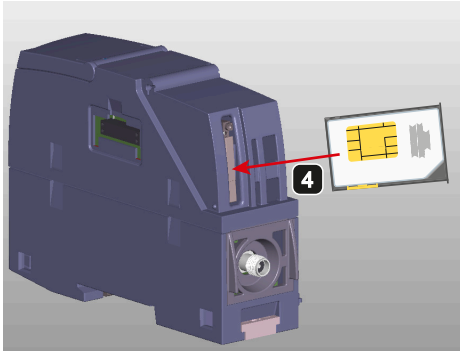
Inserting the SIM card

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

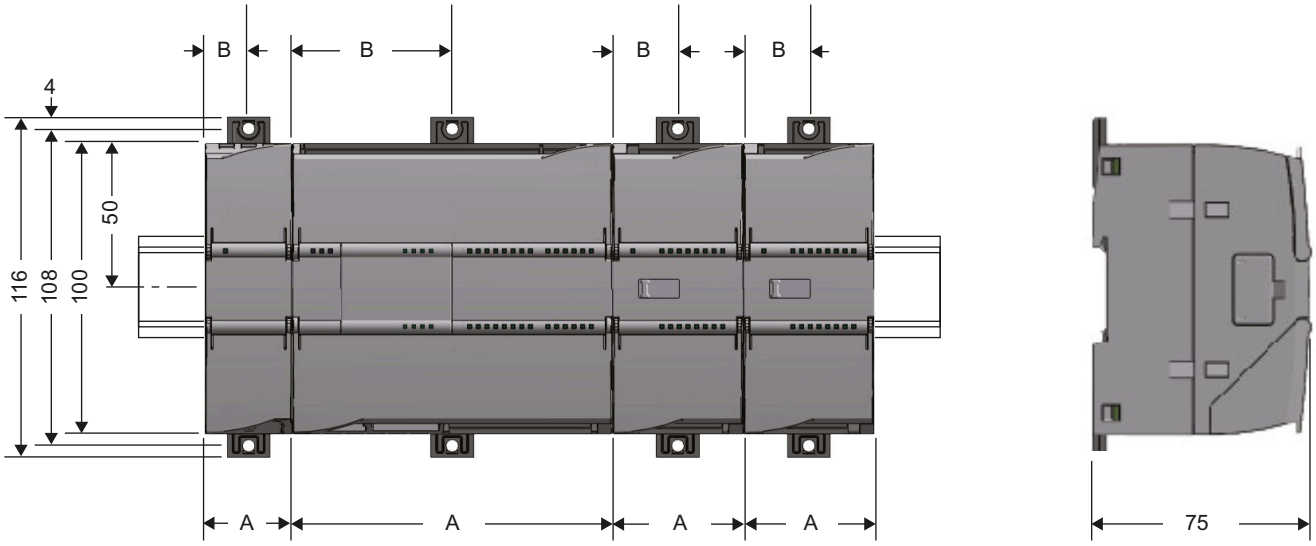


Figure 3-1 Dimensions for installation of the S7-1200

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 interfaces (Examples)	CM 1241 RS232 / CM 1241 RS485	30 mm	15 mm
	CM 1243-5 (PROFIBUS master) CM 1242-5 (PROFIBUS slave)	30 mm	15 mm
	CP 124x-7	30 mm	15 mm

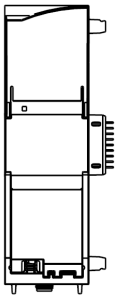
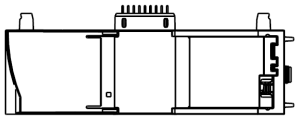
* Width B: The distance between the edge of the housing and the center of the hole in the DIN rail mounting clip

DIN rail mounting clips

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

Procedure for installation and commissioning

NOTICE
Installation location The module must be installed so that its upper and lower ventilation slits are not covered, allowing adequate ventilation. Above and below the device, there must be a clearance of 25 mm to allow air to circulate and prevent overheating. Remember that the permitted temperature ranges depend on the position of the installed device. You will find the permitted temperature ranges in the section Technical specifications of the CP (Page 95).

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 Technical specifications of the CP (Page 95).

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 97).
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"

⚠ WARNING

Power supply

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

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

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

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

3.4 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.

3.5 Disassembly

⚠ WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

Uninstalling

1. Remove the connectors of the data cables before you switch off the power supply and thus terminate the ground connection of the devices.
2. Switch off the power supply to the station.
3. Pull down the two lower DIN rail clamps on the rear of the devices into the extended position using a slotted screwdriver.
   This releases the locking mechanism.
4. Swing the devices out of the DIN rail profile to the front.

Configuration

4

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: (https://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 new firmware versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15921/dl)

Physical access

Restrict physical access to the device to qualified personnel.

APNs from mobile wireless providers

Note

Security risk: Publically accessible access points

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.

Check with your Internet service provider.

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.
  - 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.

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 this port is configured, the communications partner needs to log in.
- **Authentication**
  Specifies whether or not the protocol authenticates the communications partner during access.

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
S7 and online connections	102 (TCP)	Open	Open *	No
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 as a security vulnerability.

Ports of communication partners and routers

Make sure that you enable the required client ports in the corresponding firewall on the communication partners and in intermediary security modules.

These can be:

- TeleControl Basic / 55097 (TCP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP)
- SMTPS (STARTTLS) / 587 (TCP)
- SMTPS (SSL/TLS) / 465 (TCP)
- DNS / 53 (UDP)
- Broker port (can be set via configuration)
  - MQTT unsecured: 1883 (TCP)
  - MQTT via TLS: 8883 (TCP)

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 22).

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/ TeleControl configuration manuals (Page 112).

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/ TeleControl configuration manuals (Page 112).

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.
  For telecontrol communication, see the configuration manual /3/ TeleControl configuration manuals (Page 112).
- **Activate online functions**
  Enables access to the CPU for the online functions via the CP (diagnostics, loading project data etc.). If the function is enabled, the engineering station can access the CPU via the CP. If the option is disabled, you have no access to the CPU via the CP with the online functions. Online diagnostics of the CPU with a direct connection to the interface of the CPU however remains possible.
- **Enable 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 communications module, you need to enable this option for the communications module.
  Please note:
  Disabling this function means no security measure. To protect the station, use 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**
  Enables the use of the data service GPRS 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.

- **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 address.

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 70).

"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/ TeleControl configuration manuals (Page 112).

Reconnection settings

In this parameter group, you can define a trigger-controlled condition or a daily time at which the CP re-establishes the mobile wireless connection.

Mobile wireless connections can be terminated for a wide range of reasons. It may be intentional (through program blocks or maintenance times of the network provider) or be caused by faults or failed stations in the network.

You can plan the establishment of a mobile wireless connection exactly with the function of this parameter group.

During the connection establishment, all function requests to the CP are discarded until the CP has a new IP address.

Parameters

- Reconnection
  Enables scheduled reestablishment of a mobile wireless connection
- Reconnection type
  - Full restart including hardware
    Restart of communication functions of the CP, including restart of the mobile wireless engine
    This option can take several minutes.
  - Fast restart
    Restart of mobile wireless communication only. The mobile network engine is not restarted.
    This option shortens the duration of the restart somewhat.
- Cyclic restart
  Enables connection establishment at a fixed time.
  The cyclic restart is permanently enabled in the default setting.
  You can only disable the cyclic restart if you enable the "Restart trigger".
- Daily reconnection time
  You define the daily time for connection establishment here.
  To do this, click on the hours in the configuration field and enter them using the keyboard or the right arrow buttons. Then click on the minutes and set them.
- Restart trigger
  Enables connection establishment via a trigger set by the CPU, e.g. the occurrence of a specific event. Setting the trigger tag to 1 triggers connection establishment by the CP.
- Trigger tag
  Select a tag (Bool) which the CPU sets to 1 on the occurrence of the event.
  The trigger tag is automatically reset to 0 after the mobile wireless connection is established.

You can combine both options (cyclic and triggered) on the connection.

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.

When using security functions, you must network the interface.

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

4.5.2 Advanced options

TCP connection monitoring

The settings of the two parameters at the Ethernet interface apply to all TCP connections via this interface.

With mobile wireless CPs, the Ethernet interface is a placeholder for the mobile wireless interface.

- **TCP connection monitoring time**
  Function: If no data traffic takes place within the TCP connection monitoring time, the communications module sends a keepalive frame to the communications partner and expects an answer within the TCP keepalive timeout.
  Default setting: 180 s
  Monitoring is disabled with the setting zero (0).
  The permissible range depends on the module type.
- **TCP keepalive timeout**
  After sending a keepalive frame, the module expects a response from the communications partner within the keepalive timeout. If the module does not receive a response after three keepalive frames, it closes the connection.
  If disruptions or delays occur often when transferring in a mobile wireless network, it may be advisable to increase the value, for example, to 30 or 60 seconds.
  Default setting: 10 s
  The permissible range depends on the module type.

4.5.3 MTU size

MTU size

Option for interface-specific reduction of the maximum packet size on OSI Layer 3 (Maximum Transmission Unit - MTU)

If the frame size (e.g. segments) is limited in your plant, you can reduce the size of the packages sent by the communications module with this option.

Range of values: 1000 .. 1500 Byte

Default setting: 1500

4.5.4 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 with support of RFC5905
    NTP servers can be configured manually in the table.
  - NTP (secure)
    NTP with support of RFC5905 and RFC5906 with shared key
    NTP servers of the type NTP (secure) are configured in the global security settings and can be selected for the CP in the "Security > Time-of-day synchronization" parameter group.
  - Time from CPU
- **Telecontrol communication and security enabled**
  - Time from WAN
  - NTP / NTP (secure)
  - Time from CPU

Synchronization method of the CP

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

- **No time source**
  If no time synchronization is configured at the CP, the time of the CP can by 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.
- **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.
- **From local station**
  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 ≥ V2.1.77 with the CPU time in a synchronization cycle of 10 seconds.
- **Time from WAN**
  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/ TeleControl configuration manuals (Page 112).

CP-1200 time during startup

The CP has no valid time during startup.

For CPs with firmware version ≤ V2.0, the CP reads the CPU time once during startup, even if the option "No time source" is selected as time source. The subsequent time synchronization then depends on the configured synchronization method.

This option can only be used when telecontrol communication is enabled in the "From WAN" setting:

- Use PLC time before first synchronization by master
  You can find details on the function in the respective configuration manual.

"Time" parameter group: UTC and time zone settings

Validity:

The functions of this parameter group are valid for the CP as of firmware version V3.5.

Parameter:

- Take time zone values with daylight saving time from PLC
  When the option is enabled, the communications module takes the time zone from the CPU. When the option is disabled, the time zone of the communications module can be configured independent of the CPU.
- Time zone
  Here you set the UTC time zone that the communications module will use.
  If the "Take time zone values with daylight saving time from PLC" option is enabled, then this option is disabled and the module takes the values of the CPU.
- Use UTC
  Only valid for the CP with ST7 or IEC 60870-5 protocol; see configuration manual.

If the communications module does not take the time from the CPU, you can configure the changeover between daylight saving time and standard time:

- Activate daylight saving time
  Enables the time changeover (daylight saving/standard time)
  If the "Take time zone values with daylight saving time from PLC" option is enabled, then this option is disabled and the module takes the values of the CPU.
- Difference between standard and daylight saving time
  Time difference in minutes between standard and daylight-saving time
  Default setting: 60 minute time offset for daylight-saving time
- Beginning of daylight saving time / standard time
  Here you configure when each time changeover starts:
  - Week of the month
    Example:
    "First" means "First Sunday in March", if "Sunday" is configured as day of the week and "March" as month.
  - Day of the week
  - "in" = Month
  - "at" = time of changeover

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 Partner stations

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

4.8 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.

4.9 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. You can also use the value of diagnostic tags to send the states of the CP to communication partners via messages.

- **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.

The following 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 interface 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.
  - 0 = good network (≥ -73 dBm)
  - 1 = medium strength network (-89 ... -74 dBm)
  - 2 = weak network (-109 ... -90 dBm)
  - 3 = no network (≤ -110 dBm)
- **Mobile wireless signal quality (dBm)**
  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 = SIM card wrong, defective 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 -

4.10 Security

For a description of the telecontrol-specific parameters, refer to the relevant configuration manual /3/ TeleControl configuration manuals (Page 112).

4.10.1 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 Administrator" in the "Assigned roles" area below.

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.

4.10.2 Time-of-day synchronization

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

4.10.3 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.

Note:
SMS can sometimes be received with a delay of up to one minute.

"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.

4.10.4 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 64).

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 70).

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 60).

4.10.5 Certificate manager

Certificate manager of SIMATIC NET devices

SIMATIC NET communications modules generally use the global certificate manager. You can find this in the project navigation under "Security settings > Security features".

All certificates that are created and displayed by the configuration with the SIMATIC NET communications module can also be found in the global certificate manager.

Certificates for authentication

If you have configured secure communication with authentication for the communications 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.

Examples of services and functions that require certificates:

- Communication of the TIM 1531 IRC with the higher-level CPU
  The connection of the TIM to the CPU uses secure communication via TLS for all telecontrol protocols supported by the TIM.
  For communication via TLS, you need to use a newly created CPU certificate and specify it to the TIM in the "Subscriber numbers" parameter group.
  For information on the procedure, refer to the section Handling certificates (Page 61).
- Secure transfer of e-mails
  An SSL certificate is created for the module to transfer data via SSL/TLS. It is visible in STEP 7 in the local certificate manager and under "Global security settings > Certificate manager > Device certificates" with the "WebServer" service.

If a STEP 7 communications module is to communicate securely with non-Siemens partners, the relevant certificates of the communications partners must be exchanged. To do this, follow these steps:

1. Import the third-party certificates of the external communications partner
   Global security settings of the project > "Trusted certificates and root certification authorities"
2. Assigning a certificate to the communications module

Assigning certificates

If you create certificates for modules in STEP 7 retroactively or import third-party certificates into STEP 7, you need to assign them to the respective module, either via:

- Local certificate manager of the communications module > "Certificates of the partner devices"
- Global security settings of the project > "Trusted certificates and root certification authorities"

For information on the procedure, refer to the section Handling certificates (Page 61).

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

4.10.6 Handling certificates

Certificate for authentication

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

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

Note

No certificate with security functions disabled.

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

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

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

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

The steps are described in the following sections.

Importing third-party certificates from communications partners

Import the certificates of the communications partners of third-party vendors using the certificate manager in the global security settings. 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 CP, it needs to be displayed in the "Security" parameter group of the CP. Follow the steps outlined below:

1. In the STEP 7 project select the CP.
2. Navigate to the parameter group "Security > Certificate manager".
3. In the table, double-click on the cell with the entry "<Add new>".
   The "Certificate manager" table of the Global security settings is displayed.
4. In the table. select the required third-party certificate and to adopt it click the green check mark below the table.
   The selected certificate is displayed in the local table of the CP.

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

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

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

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

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

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

Change certificate: Subject Alternative Name

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

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

4.11 Data points

For a description of the telecontrol-specific parameters, refer to the relevant configuration manual /3/ TeleControl configuration manuals (Page 112).

4.12 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
  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 Character set for passwords and messages (Page 70).

You will find the characters permitted for message texts and additional parameters in the section E-mail configuration (Page 59).

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 Mobile wireless communications settings (Page 46).
- 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"
- Configuring the SMSC:
  "Mobile wireless communication settings"
- Configuring the SMS:
  Message editor

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.

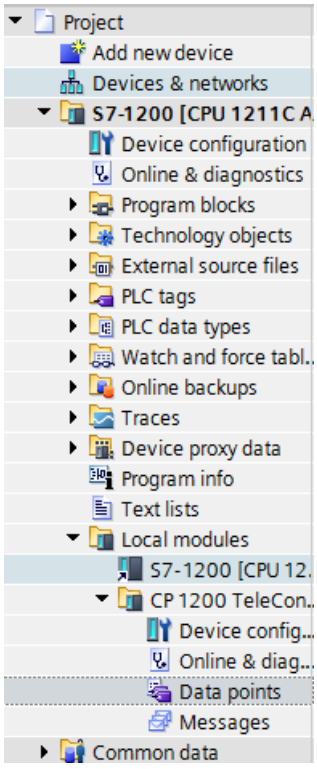


Figure 4-1 Opening the message editor via the project navigation

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 messages

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

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

Then select the "Message type" in the second column.

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.

Configuration of 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:
  - **Use PLC tag**
    For the trigger signal to send the message, 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.

    Frequent sending of SMS

    Depending on the system environment, sending an SMS can take up to 2 minutes. To guarantee secure transmission of SMS in mobile wireless modules, a minimum interval of 10 seconds is recommended for triggering SMS.
  - **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.
- **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 90).
- **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, UDInt, DInt, Real, String,
  - Arrays of the data types above
- **PLC tag for value**
  PLC tag in which the value to be sent is written.

4.13 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
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _
- 0x61 ... 0x7E
  a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
- 0x7C, 0x7E
  | ~

In addition for message texts:

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

Program blocks

5

5.1 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

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

In contrast to 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.

Supported program blocks for OUC

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

- **TSEND_C V3.0 / TRCV_C V3.0**
  Compact blocks for:
  - Connection establishment/termination and sending data
  - Connection establishment/termination and 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.

Note

Personal data unencrypted in TMAIL_C

Note that TMAIL_C uses personal data, such as user name and password, in its parameters. This data is stored unencrypted in a data block.

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 SMS messages via OUC (Page 75).
  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 via 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)

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 TC_CONFIG for changing configuration data of the CP (Page 78).

Connection establishment and termination

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

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

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

Note

Connection abort

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

5.2 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.

Note

Frequent sending of SMS

Depending on the system environment, sending an SMS can take up to 2 minutes.

To guarantee secure transmission of SMS, a minimum interval of 10 seconds is recommended for triggering SMS.

You can control this, for example, by setting the "REC" parameter in the TCON and TSEND_C blocks.

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 gas the following structure:

- DTL
  12 bytes for the time stamp of the received SMS message (time stamp from the network)
- String[22]
  String of 22 bytes for the phone number of the sender (+ 2 byte string header)
- String[160]
  String of 160 bytes for the message text (+ 2 byte string header)
- Byte
  Status of the SMS message
  If more than one SMS message is received the status of every SMS is stored in this status byte:
  - 0 = Invalid
    1 = Unread
    2 = Read

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

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

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

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

Character set for the SMS text

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

- 0x0A
  LF (line feed)
- 0x0D
  CR (carriage return)
- 0x20
  Space
- 0x21 ... 0x5A
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0x61 ... 0x7A
  a b c d e f g h i j k l m n o p q r s t u v w x y z

5.3 TC_CONFIG for changing configuration data of the CP

Meaning

With the program block TC_CONFIG, you can modify parameters of a 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_v4.

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

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

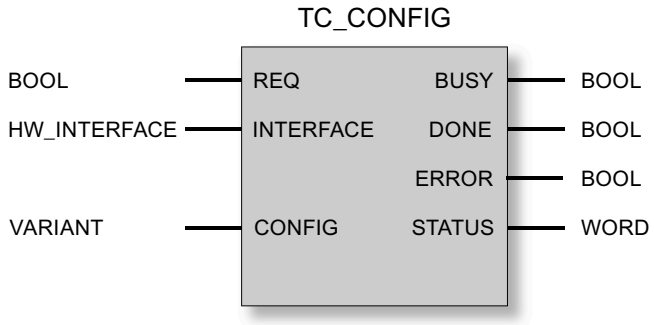
For detailed information on assigning the parameters of the SDT IF_CONF_v4, refer to the section IF_CONF_*: SDTs for the configuration data of the CP (Page 81).

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.

Requirements

- To be able to use the function, there must already be values present in the STEP 7 basic configuration of the CP.
- For using the "IF_CONF_PrefProvider" parameter field (preferred mobile wireless networks) of the SDT "IF_CONF_v4":
  The mobile wireless network to be used must be set as follows in the configuration of the CP:
  "Mobile wireless communication settings > List of preferred networks":
  "Preferred mobile wireless networks" = "Contract network and alternative networks"

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 tele-control 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 instruc-tion, 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

Parameter	Declaration	Data type	Range of values	Description
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	0000_H	Job executed without errors
0	0	7000_H	No job processing active (first block call)
0	0	7001_H	Job processing started (first block call)
0	0	7002_H	Job processing already active (renewed block call when BUSY = 1)
0	1	$80E0_H$	Internal error
0	1	$80E6_H$	No query in progress (block call not started)
0	1	$80EB_H$	Query temporarily rejected (the CP is currently being configured by STEP 7)
0	1	$80F6_H$	Format error of a parameter in the called data block (wrong length, wrong format or invalid value) Check the "IF_CONF" SDT.
0	1	$80F7_H$	Wrong ID in the parameter fields of the configuration data: Check the "IF_CONF" SDT.

5.4 IF_CONF_*: SDTs for the configuration data of the CP

Structure of the IF_CONF DB 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 function, there must already be values present in the STEP 7 basic configuration of the CP.

The IF_CONF DB is made up of a header followed by blocks that correspond to the parameters in the configuration of the CP.

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 the IF_CONF.DB:

1. Create a data block of the type "Global DB" with block access "Standard".
2. Create a structure (data type "Struct") in the table of the parameter configuration of the DB. You can specify any name.
3. Under this structure add a header by assigning the name of the header and typing it in in the cell of the data type "IF_CONF_Header".
   The header of the structure and its three parameters (see below) is created.
4. Create another structure for the first parameter to be changed by typing in the required data type (for example "IF_CONF_APN") in the cell of the data type.
5. Repeat the last step for all parameters you want to change in the CP using TC_CONFIG.
6. Finally, update the number of fields in the header in the "subfieldCnt" parameter.

Header of IF_CONF

Table 5-1 IF_CONF_Header

Byte	Parameter	Data type	Initial value	Description
0 ... 1	fieldType	UINT		Field type: Must always be 0.
2 ... 3	fieldId	UINT		Field ID: Must always be 0.
4 ... 5	subfieldCnt	UINT		Total number of blocks contained in the DB (structures) for the parameters to be changed

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 structures configured in the block.

"APN settings"

Corresponding parameter group in the configuration:
"Mobile wireless communication settings > APN settings"

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"

Corresponding parameter group in the configuration:
"Security > CP identification"

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

Parameter	Data type	Initial value	Description
Mode	UINT		Validity (1, 2) - see above (general parameters)
ModemName	STRING [22]		Access ID The value cannot be set.
ModemPassword	STRING [22]		Telecontrol password The password with the CP 1242-7 (6GK7 242-7KX30-0XE0) cannot be changed via the SDT.

"Telecontrol server" (DNS)

Corresponding parameter group in the configuration:
"Partner stations > Telecontrol server"

This field is only used when the telecontrol server is addressed with a name that can be resolved by DNS. If the telecontrol server is addressed with its IP address, the "IF_CONF_TCS_IP_V4" field is used.

If there is more than one telecontrol server, use the field once per server.

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"

Corresponding parameter group in the configuration:
"Mobile wireless communication settings > Mobile wireless settings"

Table 5-6 IF_CONF_SMS_Provider

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

"PIN"

Corresponding parameter group in the configuration:
"Mobile wireless communication settings > Mobile wireless 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 CP 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"

Corresponding parameter group in the configuration:
"Security > Authorized phone numbers"

Table 5-8 IF_CONF_WakeupList

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

"Preferred mobile wireless networks"

Corresponding parameter group in the configuration:
"Mobile wireless communication settings > List of preferred networks"

Requirement:
The mobile wireless network to be used must be set as follows in the configuration of the CP:

"Mobile wireless communication settings > List of preferred networks":
"Preferred mobile wireless networks" = "Contract network and alternative networks"

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

Parameter	Data type	Initial value	Description
Mode	UINT		Validity (1, 2) - see above (general parameters)
Provider [1...5]	ARRAY [1...5] of STRING [6]		Parameter "Contract network and preferred networks" 1st to 5th preferred mobile wireless network to which the CP dials in other than the contract network. 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)

Corresponding parameter group in the configuration:
"Mobile wireless communication settings > TeleService settings"

Access data of the TeleService server (switching station). If there is more than one TeleService server, use the field once per server.

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)

TeleService access (IP address of the server)

IP address of the TeleService server. No longer usable as of firmware version V2.1 of the CP.

If there is more than one TeleService server, use the field once per server.

Table 5-11 IF_CONF_TS_IF_V4

Parameter	Data type	Initial value	Description
Id	UINT	21	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 14
Mode	UINT		Validity (1: permanent, 2: temporary)
RemoteAddress	IP_V4		IP address of the TeleService server

Parameter	Data type	Initial value	Description
RemotePort	UINT		Port of the TeleService server
Rank	UINT		Priority of the server [1] or [2] 1 = server 1, 2 = server 2

Diagnostics and upkeep

6

⚠ WARNING

Cleaning the housing

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

Do not use any liquids or solvents.



⚠ CAUTION

Hot surfaces

Risk of burns during maintenance work on parts with a surface temperature above 70 °C (158 °F).

- Take appropriate protective measures, for example, wear protective gloves.
- Once maintenance work is complete, restore the touch protection measures.

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 26).

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

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

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

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

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

"Diagnostics" group

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

- General information on the module
  General information on the module
- Diagnostics status
  Information on the diagnostics status
- Ethernet port
  Address and statistical information
- Industrial Remote Communication
  Here, you obtain specific information on the WAN interface and other parameters of the CP.
  The entry job has the following subentries:
  - Partner
    Information about the address settings of the partner, connection statistics, configuration data of the partner and other diagnostics information.
  - Mobile wireless interface
    Diagnostics information on the network, statistical connection information, information on received/sent messages
  - Data point list
    Information on the data points such as configuration data, value, connection status etc.
  - Protocol diagnostics
    With the function "Enable protocol trace" the frames received and sent by the module are copied for several seconds.
    With the function "Disable protocol trace", the logging is stopped and the data is written to a logging file.
    With the function "Save", you can save the log file on the engineering station and then analyze it.
  - Device-specific events
    Information on CP-internal events
- Time
  Information on the time on the device

"Functions" group

- Saving service data
  The function serves for logging of internal processes is situations in which you cannot eliminate unexpected or unwanted behavior of the module yourself.
  The log file is created with the "Save service data" button. The data is saved in a file with the format "*.dmp" that can be evaluated by the Siemens hotline.

Diagnostics options via the Web server of the CPU

You will find details on the diagnostics options of the Web server in the S7-1200 system manual, see /1/ S7-1200 system manual (Page 111).

Diagnostics SMS message

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

```
CPDIAG
```

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

- Firmware version of the CP
- Mode of the CPU (RUN / STOP)
- Status of the mobile wireless network connection
  Range of values and meaning:
  - 0 = Booked out of the network
  - 1 = Wrong PIN
  - 2 = Wrong SIM card
  - 3 = Waiting for PIN / no PIN configured
  - 4 = Booked into the network
- Date and time of the last dial-in to the mobile wireless network
  The data is specified in the ISO 8601 format ("Attach: YYYY-MM-DD hh:mm:ss").
  If the time-of-day of the CP has not been synchronized at the time of the dial-in, the default date of the CP (01.01.2000) is transferred as the trime.
  If the last attempted dial-in to the mobile wireless network was not successful, "Attach: -" is sent.
- Name of the current mobile wireless network
- IP address of the CP
- Signal strength of the mobile wireless network
  - good: Good signal quality (-73 ... -51 dBm)
  - medium: Medium signal quality (-89 ... -74 dBm)
  - weak: Bad signal quality (-109 ... -90 dBm)
  - no signal: Signal too weak to be received (≤ -110 dBm)
- Received Signal Strength Indication (RSSI)- Received field strength at the station [0 ... 31]
- Status of the connection to the telecontrol server

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

Diagnostics options of the telecontrol server

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

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

- ConnectionState
- PLCConnected
- PLCCpuState

Failed mobile wireless transmission

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

TeleService

For a description of the TeleService functions, refer to the respective configuration manual, see /3/ TeleControl configuration manuals (Page 112).

6.2 Processing status of messages

Processing status

If the option "Enable identifier for processing status" is enabled in the message editor for a message, a status is output on the CP that provides information about the processing status of the sent message. The status is written to a PLC tag of the type DWORD. Select this tag via the "PLC tag for processing status" box.

The 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)

Status	Meaning
8535	SMTP authentication incomplete. Check the "User name" and "Password" parameters in the CP configuration.
8550	SMTP server cannot be reached. You have no access rights. Check the following configuration data: • CP configuration > E-mail configuration: – User name – Password – Email address (sender) • Message configuration > Message parameters: – Recipient address ("To" or "Cc").
8554	Transfer failed
85xx	Other error message from the e-mail server Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.

6.3 Firmware download

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/15921/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 26).

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.

6.4 Module replacement

Module replacement

⚠ WARNING

Read the system manual "S7-1200 Programmable Controller"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller" (refer to the documentation in the Appendix).

When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".

Make sure that the power supply is turned off when installing/uninstalling the devices.

The STEP 7 project data of the CP is stored on the local CPU. If there is a fault on the device, this allows simple replacement of this communications module without needing to load the project data to the station again.

When the station starts up again, the new CP reads the project data from the CPU.

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

7.1 Technical specifications of the CP

Table 7-1 Technical specifications

Technical specifications		
Product type designation	CP 1242-7 GPRS V2	
Article number	6GK7 242-7KX31-0XE0	
Frequency bands		
GPRS	GSM (850/900 MHz) DCS (1800 MHz) PCS (1900 MHz)	
Wireless interface		
Antenna connector	Quantity	1
	Design	SMA socket
	Nominal impedance	50 Ω
	Antenna cable, maximum permitted length	≤ 30 m
Maximum transmit power	DCS 1800, PCS 1900	+30 dBm (Class 1)
	GSM 850/950	+33 dBm (Class 4)
GPRS	Properties	• Multislot class 10 device class B coding scheme 1 to 4 (GMSK)
	Transmission speed	• Downlink: 80 kbps • Uplink: 40 kbps
SMS	Mode outgoing	MO
	Service	point-to-point
Electrical data		
External power supply	Power supply	24 VDC
	Permitted range	19.2 ... 28.8 V
	Design	Terminal block with plug, 3 terminals
	Cable cross-section	
	• Minimum	• 0.14 mm^2 (AWG 25)
	• Maximum	• 1.5 mm^2 (AWG 15)
	Max- tightening torque of the screw terminals	0.45 Nm (4 lb-in)
	Electrical isolation:	
	Power supply unit to internal circuit	710 VDC for 1 minute

Technical specifications		
Current consumption (typical)	From 24 VDC (external)	75 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, without condensation
Design, dimensions and weight		
Module format	Compact module 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 13).

7.2 Pin assignment of the socket for the external power supply

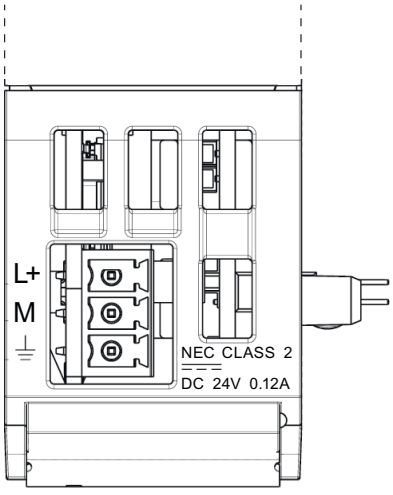


Figure 7-1 Socket for the external 24 VDC power supply (view from above)

Table 7-2 Pin assignment of the socket for the external power supply

Pin	Labeling	Function
1	L+	+ 24 VDC
2	M	Ground reference for + 24 VDC
3	⏚	Ground connector

Dimension drawings

A

Note

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

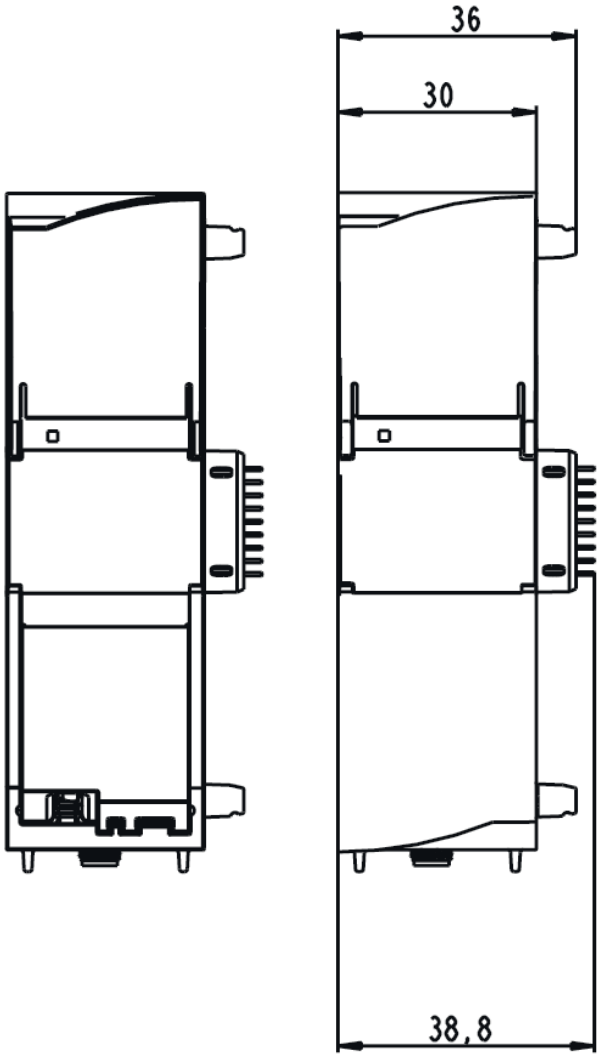


Figure A-1 Front view

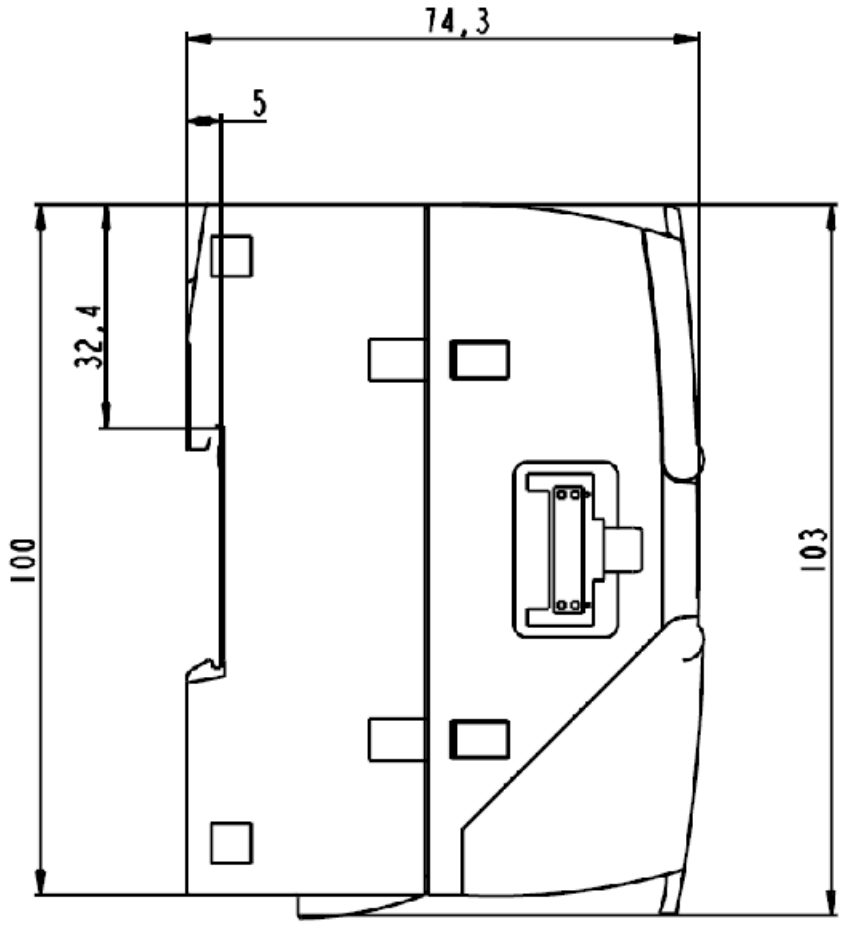


Figure A-2 Side view left

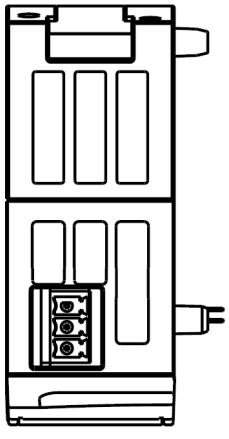


Figure A-3 From above

Approvals

B

Approvals issued

Note

Issued approvals on the type plate of the device

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

Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15921/cert)

You can view the considered standards in the respective certificate which is available on the Internet at the address listed above.

Address for declarations of conformity

The EU and the UK declarations of conformity are available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
P.O. Box 48 48
90026 Nuremberg
Germany

EC declaration of conformity

CE

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

- **2014/34/EU (ATEX explosion protection directive)**
  Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356
- **2014/53/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

- **2014/30/EU (EMC)**
  EMC directive of the European Parliament and of the Council of 26 February 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, p. 79-106
- **2011/65/EU (RoHS)**
  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

UK Declaration of Conformity

Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

The product meets the requirements of the following directives:

- UKEX Regulations
  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.
- EMC Regulations
  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.
- RoHS Regulations
  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX / IECEx / UKEX / CCC-Ex

Observe the information in the "Use of subassemblies/modules in a Zone 2 Hazardous Area" document, which you will find here:

- On the documentation DVD supplied with the product, under:
  "All documents" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- On the Internet at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013)

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 32).

The product meets the explosion protection requirements outlined below.

IECEx

Classification: Ex ec IIC T4 Gc, Certificate no.: IECEx DEK 18.0018X

The product meets the requirements of the standards:

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

ATEX

Classification: II 3 G Ex ec IIC T4 Gc, Certificate no.: DEKRA 18ATEX0026 X

The product meets the requirements of the standards:

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

UKEX

Classification: II 3 G Ex ec IIC T4 Gc, Certificate no.: DEKRA 21UKEX0003 X

The product meets the requirements of the standards:

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

Importer UK: Siemens plc (see above)

CCC-Ex

Classification:Ex na IIC T4 Gc, Certificate no.: 2020322310002998

The product meets the requirements of the following standards:

- GB 3836.1
  Hazardous areas - Part 0: Equipment - General requirements
- GB 3836.8
  Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

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).

Art. 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 Antennas (Page 109).

EMC

The CP meets the requirements of the EU Directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive).

Applied standards:

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

RoHS

The 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 IEC 63000

cULus



Underwriters Laboratories Inc. complied with

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

cULus HAZ.LOC.



Underwriters Laboratories Inc. complied with

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4A; Ta = -20 °C...60 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...60 °C

Ta: Refer to the temperature class on the type plate of the CP

Observe the conditions for safe usage of the CP according to the section Notes on use in hazardous areas according to UL HazLoc and FM (Page 32).

FM



Factory Mutual Research (FM)
Approval Standard Class number 3600 and 3611
Approved for use in:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

Observe the conditions for safe usage of the CP according to the section Notes on use in hazardous areas according to UL HazLoc and FM (Page 32).

Australia - RCM



The CP meets the requirements of the AS/NZS 2064 standards (Class A).

EAC (Eurasian Conformity)



Customs union of Russia, Belarus and Kazakhstan

Declaration of conformity according to the technical regulations of the customs union (TR CU)

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)



이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Note that in terms of the emission of interference, this device corresponds to limit class A. This device can be used in all areas except for residential environments.

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. Information on some of the national approvals is shown below.

Brazil



Instituto Brasileiro de certificação, Número do Certificado: 00091266

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Mexico

Instituto Federal De Telecommunicaciones, Número de certificado: RTISICP15-1010

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.

Taiwan

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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.

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/15921/cert)

Accessories

C

C.1 Antennas

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

Antenna ANT794-4MR



Figure C-1 Antenna ANT794-4MR

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

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

Flat antenna ANT794-3M

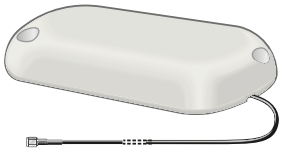


Figure C-2 Flat antenna ANT794-3M

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

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

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

References

D

Where to find Siemens documentation

- Article numbers
  You will find the article numbers for the Siemens products of relevance here in the following catalogs:
  - SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI
  - SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70

  You can request the catalogs and additional information from your Siemens representative. You will also find the product information in the Siemens Industry Mall at the following address:
  Link: (https://mall.industry.siemens.com)
- Manuals on the Internet
  You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:
  Link: (https://support.industry.siemens.com/cs/ww/en/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.

D.1 /1/ S7-1200 system manual

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

D.2 /2/ CP 1242-7 GPRS V2

SIMATIC NET
CP 1242-7 GPRS V2
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15921/man)

D.3 /3/ TeleControl configuration manuals

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)

D.4 /4/ TeleControl Server Basic (version V3)

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

Index

A

Authorized phone numbers, 59

C

CDMA, 13
Consistent data area, 21
Cross-references (PDF), 5

D

Data buffering, 22
Direct communication, 14, 20
Disposal, 7

E

E-mail
  Configuration, 65
  Number of messages, 22
  Programming (OUC), 73

F

Firmware version, 3
Frame memory, 22

G

Glossary, 7

H

Hardware version, 3

I

IMEI, 3
Importing a certificate - e-mail, 60
Inserting/removing a SIM card, 35
Instructions (OUC), 73
Inter-station communication, 14
IP configuration, 16

N

NTP, 53
NTP (secure), 53

O

Online diagnostics, 87
Online functions, 46, 87
OUC (Open User Communication), 73

P

PIN
  Configuration, 44
  Incorrect entry, 44
Program blocks, 14
PUT/GET, 21
  Enable in CPU, 16

R

Recycling, 7
Replacing a module, 93

S

S7 connections, 21
  Enable, 46
S7 routing, 15, 46
Safety notices, 31
Security, 18
Send buffer, 22
Service & Support, 7
SIMATIC NET glossary, 7
SMS
  Configuration, 65
  Number of messages, 22
  Programming (OUC), 73
  Reception, 59
SMTPS, 59
SSL/TLS, 59
STARTTLS, 59
STEP 7 - version, 23

T

TCSB, 4
Time stamp, 21
Time-of-day synchronization, 16
Training, 7

U

Uninstalling, 40
User data, 21

W

Web server
    Access, 51
    Diagnostics data, 88
Wireless approvals, 107