

SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-1

Operating Instructions




Preface

Application and functions	1
LEDs and connectors	2
Installation, connecting up, commissioning	3
Configuration	4
Program blocks (OUC)	5
Diagnostics and upkeep	6
Technical data	7
Approvals	A
Dimension drawings	B
Documentation references	C

Legal information

Warning notice system

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

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


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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Preface

Validity of this manual

This document contains information on the following telecontrol product:

- **CP 1243-1**
Article number 6GK7 243-1BX30-0XE0
Hardware product version 2
Firmware version V3.2

The CP 1243-1 is the communications processor for connecting the SIMATIC S7-1200 to control center systems via the public infrastructure (e.g. DSL). For the supported telecontrol protocols, see section Properties of the CP (Page 13).

With the help of VPN technology and the firewall, the CP allows protected access to the S7-1200.

The CP can also be used as an additional Ethernet interface of the CPU for S7 communication.



Figure 1 CP 1243-1

Behind the top hinged cover of the module housing, you will see the hardware product version to the right of the article number printed as a placeholder "X". If the printed text is, for example, "X 2 3 4", "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 MAC address under the lower hinged cover of the housing.

Product names and abbreviations

- **CP / submodule / module**

These abbreviations are used below instead of the full product name CP 1243-1:

- **TCSB**

This abbreviation will be used below for the "TeleControl Server Basic", version V3.

- **STEP 7**

This short form will be used below for the STEP 7 Basic / Professional configuration tool.

- **ES**

PC with the STEP 7 project

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 respective configuration manual /4/ (Page 106).

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

New in this edition

- New firmware version V3.2 with the following functional improvements, among others:
 - Increased number of data points
 - Extended telecontrol functions, see data point configuration
 - Support of additional OUC blocks
- New ATEX/IECEX approval
- New structure of the documentation

Replaced manual edition

Edition 02/2018

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**

Configuration and diagnostics in STEP 7 Professional (TIA Portal)

Valid for all SIMATIC NET communications modules that support the TeleControl Basic protocol.
- **Configuration manual DNP3**

Configuration and diagnostics in STEP 7 Professional (TIA Portal)

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

- **Configuration manual IEC 60870-5**

Configuration and diagnostics in STEP 7 Professional (TIA Portal)

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

You can find the Internet links for the manuals in the appendix Documentation references (Page 105).

Current manual edition on the Internet

You will find the current version of this manual on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15922/man>)

Required experience

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

- Automation engineering
- Setting up the SIMATIC S7-1200 system
- SIMATIC STEP 7 Basic / Professional

Cross references

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

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

License conditions

Note

Open source software

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

You will find the license conditions on the supplied data medium:

- OSS_CP1243x_99.pdf

Firmware

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

Security information

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

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

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

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

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

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

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

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary on the Internet at the following address:

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

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>)

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	Properties of the CP.....	13
1.2	Communications services	13
1.3	Communication via SINEMA RC	15
1.4	Other services and properties.....	16
1.5	Security functions.....	18
1.6	Configuration limits and performance data	20
1.7	Configuration examples	22
1.8	Requirements for use.....	25
1.8.1	Hardware requirements	25
1.8.2	Software requirements.....	25
2	LEDs and connectors.....	27
2.1	Opening the covers of the housing	27
2.2	LEDs	28
2.3	Electrical connectors.....	32
2.3.1	Power supply	32
2.3.2	Ethernet interface X1P1.....	32
3	Installation, connecting up, commissioning.....	33
3.1	Important notes on using the device.....	33
3.1.1	Notices on use in hazardous areas	34
3.1.2	Notes on use in hazardous areas according to ATEX / IECEx	35
3.1.3	Notices regarding use in hazardous areas according to UL HazLoc	35
3.1.4	Notices on use in hazardous areas according to FM	36
3.2	Installing, connecting up and commissioning	36
3.3	Note on operation	40
4	Configuration	41
4.1	Security recommendations	41
4.2	Configuration in STEP 7	45
4.3	Communication types	46
4.4	Time-of-day synchronization.....	47
4.5	Ethernet interface.....	50
4.5.1	Ethernet addresses.....	50
4.5.2	IPv6	51
4.5.3	CP identification	51

4.5.4	Time-of-day synchronization	51
4.5.5	Advanced options	52
4.5.6	Access to the Web server	52
4.6	Partner stations	52
4.7	DNS configuration	53
4.8	Communication with the CPU	53
4.8.1	Communication with the CPU	53
4.8.2	CP diagnostics	54
4.9	SNMP	56
4.10	Security	57
4.10.1	Security user	57
4.10.2	Parameter overview	57
4.10.3	Firewall	58
4.10.3.1	Pre-check of messages by the MAC firewall.	58
4.10.3.2	Notation for the source IP address (advanced firewall mode)	58
4.10.3.3	Firewall settings for configured connection connections via a VPN tunnel	59
4.10.3.4	Settings for online security diagnostics and downloading to station with the firewall activated	59
4.10.4	E-mail configuration	60
4.10.5	Log settings - Filtering of the system events	61
4.10.6	SNMP	61
4.10.7	VPN	63
4.10.7.1	VPN (Virtual Private Network).....	63
4.10.7.2	Creating a VPN tunnel for S7 communication between stations	64
4.10.7.3	VPN communication with SOFTNET Security Client (engineering station).....	66
4.10.7.4	Establishment of VPN tunnel communication between the CP and SCALANCE M	67
4.10.7.5	CP as passive subscriber of VPN connections.....	67
4.10.7.6	SYSLOG	67
4.10.7.7	SINEMA Remote Connect	68
4.10.8	Certificate manager.....	71
4.10.9	Handling certificates.....	71
4.11	Data points	74
4.12	Messages.....	74
4.13	Character set for messages.....	79
5	Program blocks (OUC).....	81
5.1	Program blocks for OUC	81
5.2	Changing the IP address during runtime	84
6	Diagnostics and upkeep.....	87
6.1	Diagnostics options	87
6.2	Web server S7-1200: Connection establishment	90
6.3	Online security diagnostics via port 8448	91
6.4	SNMP	92
6.5	Processing status of e-mails	93

6.6	Downloading firmware	95
6.7	Module replacement	96
7	Technical data	97
7.1	Technical specifications of the CP 1243-1.....	97
7.2	Pinout of the Ethernet interface	98
A	Approvals.....	99
B	Dimension drawings.....	103
C	Documentation references	105
	Index.....	107

Application and functions

1.1 Properties of the CP

Application

The CP is intended for operation in an S7-1200 automation system.

The CP allows connection of the S7-1200 to Industrial Ethernet or via the Internet to the following control center systems:

- Telecontrol server (OPC server application TCSB V3)
- DNP3 master station
- IEC master station

The CP can also be used as an interface extension of the CPU. In this role, it serves the purpose of network separation.

With a combination of different security functions such as firewall and protocols for data encryption, the CP protects the station or even entire automation cells from unauthorized access. It protects the communication between the station and communications partners from espionage and manipulation.

1.2 Communications services

Telecontrol communication

The following applications are supported:

- **Communication with a control center**

The CP is a communications processor of the SIMATIC S7-1200 for system attachment to the control center systems named above. The CP can communicate with redundant control centers.

For each control center system the relevant telecontrol protocol is activated on the CP ("Type of communication"). The protocols allow IP-based data transmission for telecontrol applications.

You will find the usable security functions in the section Security functions (Page 18).

- **Inter-station communication / Direct communication between stations**

Using the three telecontrol protocols, the CP enables communication with other S7 stations.

Messages / e-mail

With special events, the CP can send messages as e-mails.

The function is configured in telecontrol communication in STEP 7. The use of program blocks is not necessary.

You will find the requirements and functions in the section E-mail configuration (Page 60).

Communication via SINEMA Remote Connect

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

S7 communication and PG/OP communication

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

The CP supports the following functions:

- **PUT/GET**

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

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

- **PG functions**
- **Operator control and monitoring functions (HMI)**
- **S7 routing**

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

For S7 communication, the CP requires a fixed IP address.

Communication via Open User Communication (OUC)

Via the Ethernet interface of the CP and the program blocks of the Open User Communication on the CPU the CP has the following communication options:

- Communication with SIMATIC stations
- Sending e-mails

In contrast to the corresponding service of telecontrol communication (see above), to transfer e-mails via OUC, the TMAIL_C program block needs to be used, see section Program blocks for OUC (Page 81).

1.3 Communication via SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

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

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

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

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

Parameter groups

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

- Communication via SINEMA RC:
 - > "Security > VPN"
- Telecontrol communication via SINEMA RC:
 - > "Communication types"

For information on the configuration, refer to the telecontrol configuration manuals /4/ (Page 106).

Applications

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

Application example:

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

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

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

Table 1- 1 Use cases and parameters to be activated

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

* Explanation of the parameter abbreviations:

SRC - Security > VPN (activated) > "VPN connection type":

"Automatic OpenVPN configuration via SINEMA Remote Connect Server"

TC - Communication types > Telecontrol communication enabled

TC-SRC - Communication types >

"Activate telecontrol communication via SINEMA Remote Connect"

1.4 Other services and properties

Other services and properties

- **IP configuration - IPv4 and IPv6**

- IPv4 / IPv6

The CP supports IP addresses according to IPv4 and IPv6.

In IPv6 networks, an IPv6 address can be used in addition to an IPv4 address.

- Address assignment

The IP address, the subnet mask and the address of a gateway can be set manually in the configuration.

As an alternative, the IP address can be obtained from a DHCP server or by other means outside the configuration.

- **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 47).

- **Online functions**

From the engineering station you can access the station via the CP with the online functions of STEP 7.

The following online functions are available:

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

For information on the online functions, refer to the section Diagnostics options (Page 87).

- **SNMP**

As an SNMP agent, the CP supports data queries using SNMP (Simple Network Management Protocol).

For more detailed information, refer to section SNMP (Page 92).

Further properties in telecontrol mode

- **Data point configuration**

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

- **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 the event of a power failure.

- **Event-driven transfer of process data**

The CP transmits the data from the send buffer individually (spontaneously) or bundled to the communications partner. The transfer can be triggered by various triggers.

- **Analog value processing**

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

1.5 Security functions

Industrial Ethernet Security

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

- Data espionage
- Data manipulation
- Unauthorized access

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

The security functions can be used independently of telecontrol communication.

Security functions of the telecontrol protocols

- **TeleControl Basic**

- **Encrypted telecontrol communication**

As an integrated (unconfigurable) security function, the 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".

- **Telecontrol password**

To authenticate the CP with the telecontrol server

- **DNP3**

The security functions specific to DNP3 can be used.

- **IEC 60870-5**

For the IEC protocol there are no protocol-specific security functions available.

Further configurable security functions of the CP

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

- **Firewall**

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

- **VPN**

The following alternatives can be used:

- Secured communication via IPsec tunnels

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

- Remote maintenance via SINEMA Remote Connect

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

- **Logging**

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

- **STARTTLS / SMTPS**

For the secure transfer of e-mails

- **NTP (secure)**

For secure transfer during time-of-day synchronization

- **SNMPv3**

For secure transmission of network analysis information safe from eavesdropping

- **Protection for devices and network segments**

The protection provided by the firewall can cover individual devices, several devices or even entire network segments.

Note**Plants with security requirements - recommendation**

Use the following options:

- If you have systems with high security requirements, use the secure protocols NTP (secure), HTTPS and SNMPv3.
- If you connect to public networks, you should use the firewall. Think about the services you want to allow access to the station via public networks. By using the "bandwidth limitation" of the firewall, you can restrict the possibility of flooding and DoS attacks.

See also section Security recommendations (Page 41).

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

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

1.6 Configuration limits and performance data

Number of CMs/CPs per station

In each S7-1200 station, up to three CMs/CPs can be plugged in and configured; this allows three CP 1243-1 modules.

Connection resources

- **S7 connections and TCP / UDP / ISO-on-TCP connections**

Total number of connections on Industrial Ethernet: Maximum 14
of which:

- S7: Max. 14 (including connections for S7 routing)
- TCP/IP: Max. 14
- ISO-on-TCP: Max. 14
- UDP: Max. 14

Also:

- **Telecontrol connections**

With the various telecontrol protocols the CP can establish connections to the following partners:

TeleControl Basic

- To non-redundant or redundant telecontrol servers (TCSB).
- Additional Inter-station communication

The inter-station communication between the CPs of two stations takes place via the telecontrol server. It is configured in the "Partner stations" > "Partner for inter-station communication" parameter group.

Configuration limits for inter-station communication A total of max. 15, of which:

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

DNP3 / IEC 60870-5

- Communication with up to 4 partners

A partner is a single or redundant master or a station (Direct communication).

Direct communication between stations is made possible by the telecontrol connections.

- **Online connections**

Two resources for one online connection to an engineering station (STEP 7)

- **Programming device and HMI connections (OP)**

In total maximum of 4, of which:

- Resources for programming device connections: Max. 1
- Resources for HMI connections: Max. 3

Number of data points for the data point configuration

Maximum number of configurable data points

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

User data

The data to be transferred by the CP is assigned to various data points in the STEP 7 configuration.

The size of the user data per data point depends on the data type of the relevant data point (see Data point types).

Frame memory (send buffer)

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

The send buffer has a maximum size of 64000 events 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).

With the TeleControl Basic protocol the send buffer can also be used for up to three partners for inter-station communication. You create the configuration in the "Partner" parameter group.

Messages (e-mail)

- Sending of up to 10 messages (e-mails) can be configured with the message editor.
- Sending e-mails via the TMAIL_C program block

IPsec tunnel (VPN)

Up to 8 IPsec terminals can be established for secure communication with other security modules.

Firewall rules

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

The firewall rules are divided up as follows:

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

1.7 Configuration examples

You will find configuration examples for telecontrol applications in the configuration manuals /4/ (Page 106).

Configuration with CP for secure network separation

The following example shows a configuration with CP 1243-1 that protects the station and the lower-level automation cell.

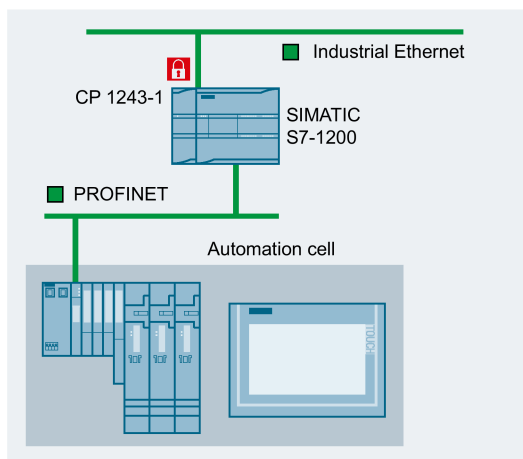


Figure 1-1 Secure communication with CP 1243-1

Configuration with sending of e-mails:

The following example shows a configuration with sending of e-mails. The telecontrol communication of the CP is disabled.

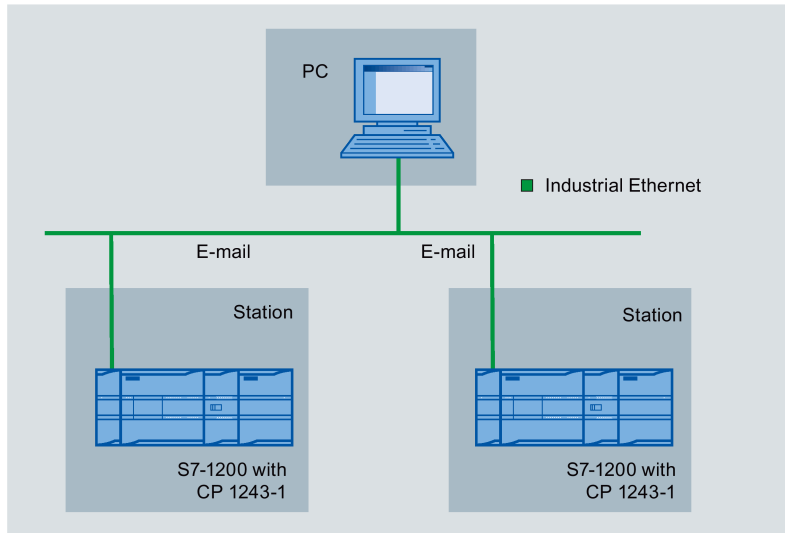


Figure 1-2 Sending e-mails

Remote maintenance with SINEMA RC

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

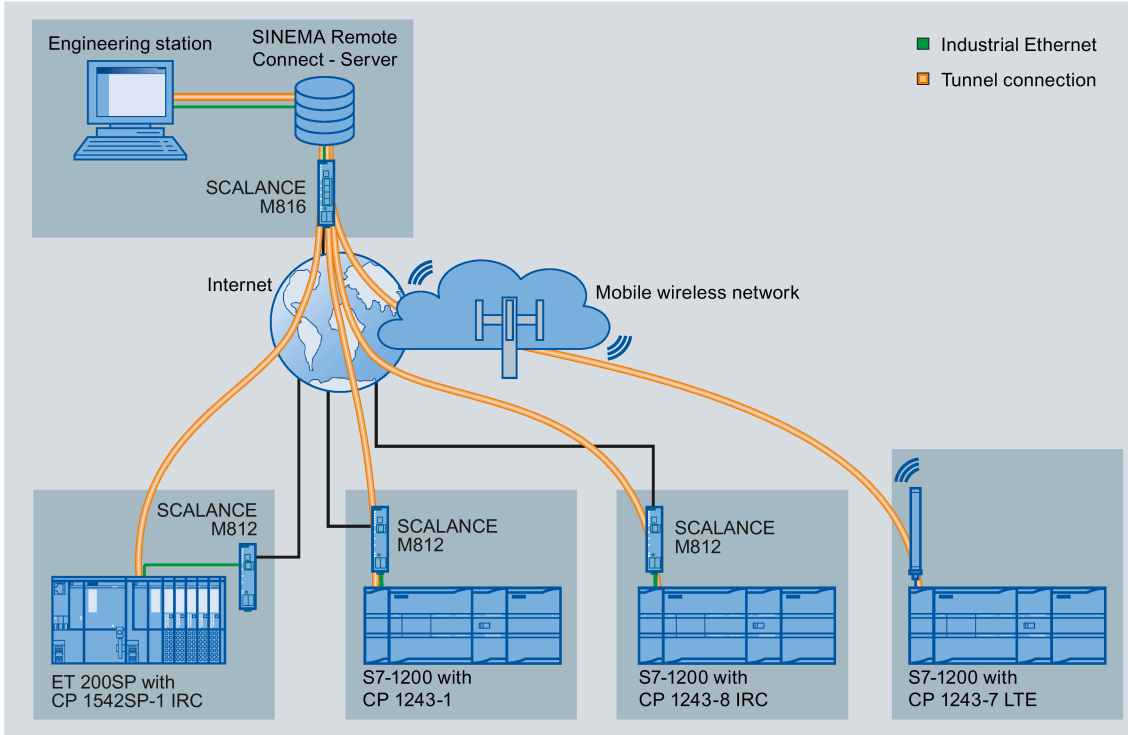


Figure 1-3 Connection of stations to engineering station via SINEMA RC

1.8 Requirements for use

1.8.1 Hardware requirements

CPU 1200

The CP can be used with:

- CPU with firmware version as of V3
- The full functionality of the CP is only available with a CPU as of V4.4.

1.8.2 Software requirements

Software for configuration and online functions

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

- STEP 7 Basic V16

LEDs and connectors

2.1 Opening the covers of 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 Ethernet connector is located behind the lower hinged cover of the module.

Opening the covers of the housing

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

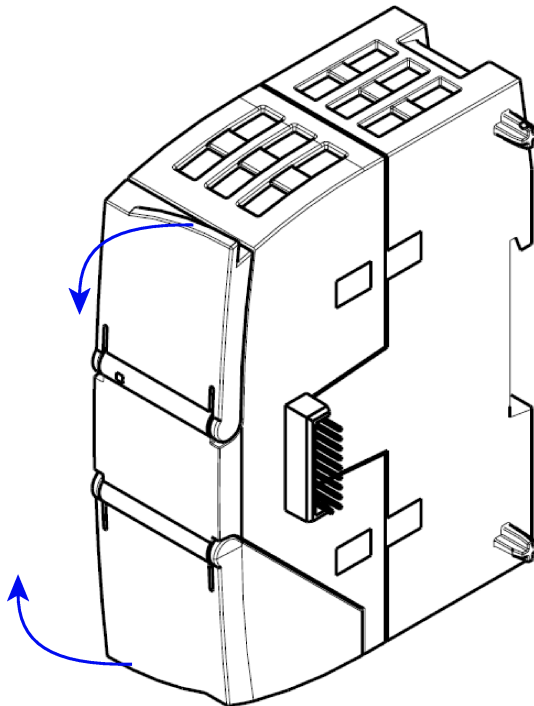


Figure 2-1 Opening the covers of the housing

2.2 LEDs

LEDs of the module

The module has various LEDs for displaying the status:

- **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**

The LEDs below the upper cover provide more detailed information 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 (color)	Name	Meaning
 (green)	LINK	Status of the connection to Industrial Ethernet
 (green)	CONNECT	Status of the connections to the communications partner
 (green)	VPN	Status of the VPN or SINEMA Remote Connect configuration
 (green)	SERVICE	Status of a connection for online functions

LED colors and illustration of the LED statuses

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






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 basic statuses of the CP ("DIAG" LED)

Table 2- 4 Display of the basic statuses of the CP

DIAG (red / green)	Meaning (if more than one point listed: alternative meaning)
Basic statuses of the CP	
 ○	<ul style="list-style-type: none"> • Power OFF • Incorrect startup
 green	Running (RUN) without serious error
 flashing green	<ul style="list-style-type: none"> • Partner not connected • Firmware loaded successfully
 flashing red	<ul style="list-style-type: none"> • Starting up • Module fault • Invalid STEP 7 project data
 flashing red-green	Error loading firmware































2.2 LEDs

Display of the operating and communications statuses

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

Table 2- 5 Display of the operating and communications statuses

DIAG (red / green)	-	LINK (green)	CONNECT (green)	VPN (green)	SERVICE (green)	Meaning (if more than one point listed: alternative meaning)
Module startup (STOP → RUN) or error statuses						
						Power OFF
 red						Startup - phase 1
 flashing red		-				Startup - phase 2
 green		-	-	-	-	Running (RUN) without serious error
						Incorrect startup
 red		-		-	-	Invalid STEP 7 project data
 flashing red		-		-	-	Missing STEP 7 project data
 flashing red				-	-	Backplane bus error
Connection to Industrial Ethernet						
-			-	-	-	Connection to Industrial Ethernet exists
 green			-	-	-	<ul style="list-style-type: none"> • Connection to Industrial Ethernet being established. • IP address being obtained.
-			-	-	-	No connection to Industrial Ethernet
Connection to communications partners						
 green				-	-	Connection established to at least one partner
 green				-	-	Partner reachable, CPU in STOP mode
 flashing green				-	-	Partner not reachable

DIAG (red / green)	-	LINK (green)	CONNECT (green)	VPN (green)	SERVICE (green)	Meaning (if more than one point listed: alternative meaning)
Connection for online functions						
 green			-	-		Connection for online functions established
 green			-	-		Attempt to establish connection for online functions
 green		-	-	-		No connection to engineering station
VPN/SINEMA Remote Connect connection						
 green			-		-	VPN/SINEMA Remote Connect connection established
 flashing green			-	 flashing green	-	Attempting to establish a configured VPN/SINEMA Remote Connect connection
-		-	-		-	VPN/SINEMA Remote Connect connection not configured or currently not established on the CP
Loading firmware						
						Loading firmware. The DIAG LED flashes alternating red and green.
 flashing green						Firmware was successfully loaded.
 flashing red						Error loading firmware

2.3 Electrical connectors

2.3.1 Power supply

Power supply

The CM is supplied with power from the backplane bus. It does not require a separate power supply.

2.3.2 Ethernet interface X1P1

Ethernet interface

The Ethernet connector is located behind the lower hinged cover of the module. The interface is an RJ-45 jack according to IEEE 802.3.

The pin assignment and other data relating to the Ethernet interface can be found in the section Technical data (Page 97).

Installation, connecting up, commissioning

3.1 Important notes on using the device

Safety notices on the use of the device


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


Overvoltage protection


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


3.1 Important notes on using the device


3.1.1 Notices on use in hazardous areas


 WARNING
EXPLOSION HAZARD
DO NOT OPEN WHEN ENERGIZED.

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


 WARNING
The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS). This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the equipment power supply must comply with NEC Class 2, as described by the National Electrical Code (r) (ANSI / NFPA 70). If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.


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


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

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


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

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

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

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


3.1.3 Notices regarding use in hazardous areas according to UL HazLoc

 WARNING
EXPLOSION HAZARD DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

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


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

3.1.4 Notices on use in hazardous areas according to FM

 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.


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
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 Installing, connecting up and commissioning

Prior to installation and commissioning

 CAUTION
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".

Pulling/plugging the module

NOTICE
Turning off the station when plugging/pulling the module
Before pulling or plugging the module, always turn off the power supply to the station.

Dimensions for installation

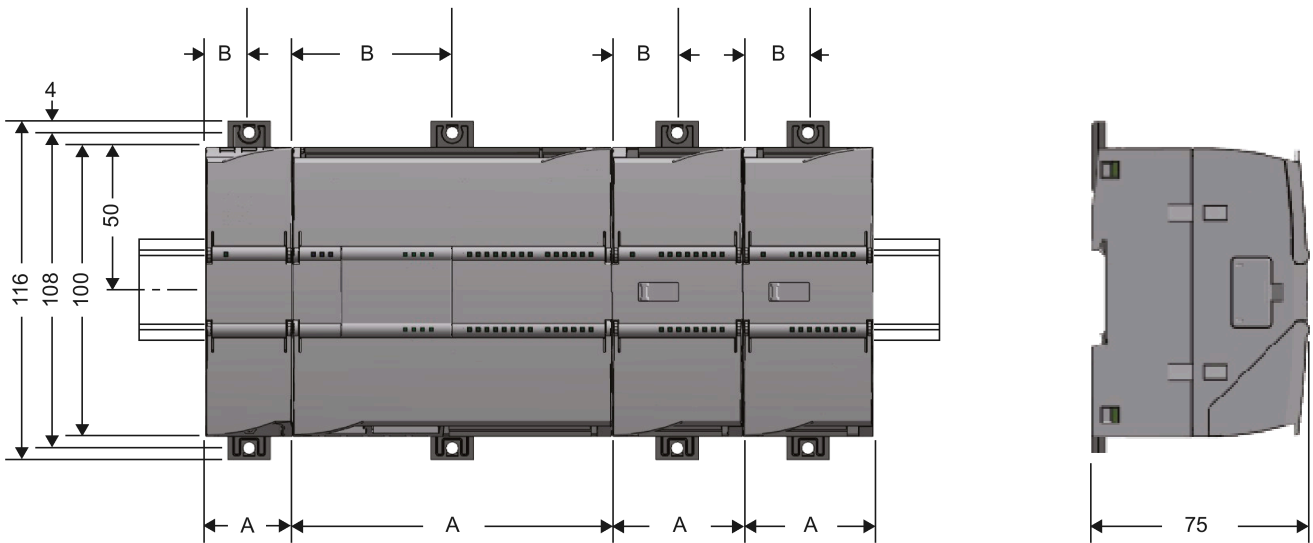


Figure 3-1 Dimensions for installation of the S7-1200

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
Communications inter- faces (examples)	CM 1241, CM 1243-5, CM 1242-5	30 mm	15 mm
	CP 1242-7, CP 1243-1, CP 1243-7, CP 1243-8 IRC	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

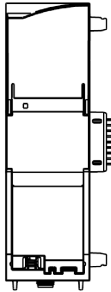
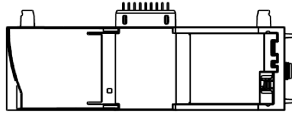
You will find detailed dimensions of the module in the section Dimension drawings (Page 103).

DIN rail clamps, control panel installation

All CPUs, SMs, CMs and CPs can be installed on the 35 mm 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.

Installation location

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 1243-1 (Page 97).

Device position / permitted temperature range	Installation location
Horizontal installation of the rack	
Vertical installation of the rack:	

Requirement: Configuration prior to commissioning

One requirement for the commissioning of the module is the completeness of the STEP 7 project data (see below, step 5).

Installing, connecting up and commissioning the module

Note

Connection with power off

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

Table 3- 2 Procedure for installation and connecting up

Step	What to do	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	Connect the Ethernet cable to the CP.	You will find the pinout of the interface in the section Technical data (Page 97).
4	Turn on the power supply.	
5	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 information system: <ul style="list-style-type: none"> • "Loading project data" • "Using online and diagnostics functions"
6	Close the front covers of the module and keep them closed during operation.	

Manual setting the time of day during commissioning

Note

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

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

The CP receives the time from the CPU or from an NTP server before the connection is established for the first time.

Recommendation:

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

3.3 Note on operation

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

Configuration

4.1 Security recommendations

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

With enabled telecontrol communication, you should also refer to the information in the relevant 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.
 - Here you can find information on Industrial Security:
Link: (<http://www.siemens.com/industrialsecurity>)
 - You can find a selection of documentation on the topic of network security here:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/92651441>)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.

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

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21764/dl>)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the PC directly to the Internet. If a connection from the CP to the Internet is required, arrange for suitable protection before the CP, for example a SCALANCE S with firewall, or use the CP.

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 and set up the firewall.
If you connect to public networks, you should use the firewall. Think about the services you want to allow access to the station via public networks. By limiting the "transmission speed" via IP packet filter rules in the firewall, you make use of the possibility of restricting flooding and DoS attacks.
 - Use the secure protocol variants NTP (secure) and SNMPv3.
 - Using the security functions of the telecontrol protocols.
 - Leave access to the Web server of the CPU deactivated.
- Protection of the passwords for access to program blocks
Protect the passwords stored in data blocks for the program blocks from being viewed. You will find information on the procedure in the STEP 7 information system under the keyword "Know-how protection".
- Logging function
Enable the function in the security configuration and check the logged events regularly for unauthorized access.

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
See also the preceding section for information on this.
- Do not use one password for different users and systems.

Protocols

Secure and non-secure protocols

- Only activate protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.
 - The NTP protocol provides a secure alternative with NTP (secure) if you do not use telecontrol communication.
 - The HTTP protocol provides a secure alternative with HTTPS when accessing the Web server (configuration of the CPU).

Table: Meaning of the column titles and entries

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

- **Protocol / function**
Protocols that the device supports.
- **Port number (protocol)**
Port number assigned to the protocol.
- **Default of the port**
 - Open
The port is open at the start of the configuration.
 - Closed
The port is closed at the start of the configuration.
- **Port status**
 - Open
The port is always open and cannot be closed.
 - Open after configuration
The port is open if it has been configured.
 - Open (login, when configured)
As default the port is open. After configuring the port, the communications partner needs to log in.
 - Closed after configuration
The port is closed because the CP is always client for this service.
- **Authentication**
Specifies whether or not the protocol authenticates the communications partner during access.

4.1 Security recommendations

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
DNP3	20000 (TCP/UDP)	Closed	Open after configuration	Yes, when Secure Authentication is enabled.
IEC	2404 (TCP)	Closed	Open after configuration	No
S7 and online connections	102 (TCP)	Closed	Open after configuration *	No
Online security diagnostics (if supported)	102 (TCP)	Open	Open after configuration *	No
Communication via SINEMA RC (if supported)	443 (TCP)	Closed	Open after configuration	Yes
HTTP	80 (TCP)	Closed	Open after configuration	Yes
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP (if supported)	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)
Syslog	514 (UDP)	Closed	Open after configuration	No

* Some service providers consider the opening of port 102 a security vulnerability. To avoid opening port 102 during online diagnostics, see section Online security diagnostics via port 8448 (Page 91).

Ports of communications partners and routers

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

These can be, if supported and used:

- TeleControl Basic / 55097 (TCP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- SINEMA RC Autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC
- IPSec / 500 (TCP)
- Syslog / 514 (UDP)

4.2 Configuration in STEP 7

Configuration in STEP 7

You configure the modules and networks in SIMATIC STEP 7. You will find the required version in the section Software requirements (Page 25).

You can configure a maximum of three CMs/CPs per station.

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 manuals /4/ (Page 106).

Overview of the configuration steps in STEP 7

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. Create an Ethernet network.
4. Connect the stations to the Ethernet subnet.
5. Configure the CPs including the messages (e-mail).
6. If required, create the program blocks for S7 communication and Open User Communication and configure them as needed.
7. Save and compile the project.
8. 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 more detailed information on configuring the CP in the Information system of STEP 7 and in the following sections.

Loading and storing the configuration data

When you load the station, the project data of the station including the configuration data of the CP is stored on the CPU.

You will find information on loading the station in the STEP 7 information system.

4.3 Communication types

"Communication types" parameter group

In this parameter group, you enable the communications services of the CP.

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

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.

- **Enable telecontrol communication**

Enables telecontrol communication on the CP.

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

- TeleControl Basic
- DNP3
- IEC 60870-5

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

You can find additional information in the configuration manuals /4/ (Page 106).

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

You can find additional information in the configuration manuals /4/ (Page 106).

For information on remote maintenance via SINEMA Remote Connect, see section SINEMA Remote Connect (Page 68).

- **Activate online functions**

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

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

- **Enabling S7 communication**

Enables the functions of S7 communication with the station CPU and S7 routing in the CP.

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

4.4 Time-of-day synchronization

Note**Time-of-day synchronization when using SINEMA RC**

When the CP obtains the time from the CPU, set the CPU time manually during commissioning when using SINEMA Remote Connect; see note in section Installing, connecting up and commissioning (Page 36).

Note**Time-of-day synchronization of the CP**

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

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

Note**Recommendation for setting the time**

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

Time-of-day synchronization with the S7-1200

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

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

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

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

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

Parameter groups for time-of-day synchronization

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

- **Ethernet interface**

Here you create the configuration under the following conditions:

- Telecontrol communication is disabled.
- The security functions are disabled.

- **Security**

Here is where you configure when the security functions are enabled.

Dependence of the synchronization method on the use of the CP

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

- **Telecontrol communication disabled, security disabled**

- NTP
- Time from CPU

- **Telecontrol communication disabled, security enabled**

- NTP
- NTP (secure)
- Time from CPU

- **Telecontrol communication and security enabled**

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

Synchronization method of the CP

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

- **NTP**

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

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

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

- **NTP (secure)**

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

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

On the CP you specify the servers used.

- **Time from CPU**

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

Parameters of the CPU:

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

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

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

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

- **Time from partner**

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

You will find the description in the configuration manual /4/ (Page 106).

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.

4.5 Ethernet interface

4.5.1 Ethernet addresses

Ethernet addresses

In the following parameter groups you network the Ethernet interface and configure the IP address parameters.

You configure the port interconnection and transmission properties in the parameter groups under Advanced options > Port [Xn P1].

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

4.5.2 IPv6

Manual configuration of IPv6 addresses

If you configure additional IPv6 addresses ("Manual configuration" option), make sure that the two IPv6 addresses belong to different subnets.

You will find information on configuration in the STEP 7 information system.

Communication partner and IPv6

Note

Internet communication via IPv6

If you want to use IPv6 addresses and connect the CP to the Internet, make sure that the router connected to the Internet and the providers of the Internet services used (e.g. e-mail) also support IPv6 addresses.

OUC communication via IPv6

When you use the Open User Communication blocks and activate IPv6, make sure that the communication partners support IPv6. In case of queries to the DNS server, the returned addresses primarily use IPv6 addresses before they use the IPv4 addresses.

4.5.3 CP identification

The parameter group is available only when telecontrol communication is enabled. You can find additional information in the configuration manuals /4/ (Page 106).

4.5.4 Time-of-day synchronization

Time-of-day synchronization

For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 47).

4.5.5 Advanced options

TCP connection monitoring

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

- **TCP connection monitoring time**

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

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

- **TCP keepalive timeout**

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

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

Transmission settings

The protocol-specific transmission settings are visible only when telecontrol communication is enabled. You can find additional information in the configuration manuals /4/ (Page 106).

4.5.6 Access to the Web server

Access to the Web server of the CPU

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

From a PC, you can access the Web server of the station via LAN.

You will find information on the Web server in the manual /1/ (Page 105).

Special features of access to the Web server when using the TeleControl Basic are explained in the configuration manual /4/ (Page 106).

You will find information on the Web server of the S7-1200 in the manual /1/ (Page 105).

4.6 Partner stations

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

4.7 DNS configuration

DNS server

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

When addressing a communications partner as FQDN, you need to configure a DNS server. The IP address (IPv4/IPv6) of the communications partner is then determined via the configured DNS server.

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

4.8 Communication with the CPU

4.8.1 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 47).

4.8.2 CP diagnostics

The functions are supported by a CP as of firmware version V3.

CP diagnostics

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

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

- **Enable advanced CP diagnostics**

Enable the option to use advanced CP diagnostics.

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

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

- **Diagnostics trigger tag**

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

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

Note

Fast setting of the diagnostics trigger tag

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

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

- **Frame memory overflow warning**
 - Only relevant for telecontrol communication -
- **Frame memory occupation**
 - Only relevant for telecontrol communication -
- **Current IP address**

PLC tag (data type String) for the current IP address of the interface of the CP.
- **Date of last successful logon to TCSB**
 - Only relevant for telecontrol communication -
- **Date of last unsuccessful logon to TCSB**
 - Only relevant for telecontrol communication -
- **TeleService status**
 - Only relevant for telecontrol communication -
- **VPN IPsec status**

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

 - 0 = No tunnel established
 - 1 = Tunnel established
- **Connection to SINEMA Remote Connect**

The PLC tag (BOOL) indicates whether an OpenVPN tunnel to SINEMA RC is established:

 - 0 = No tunnel established
 - 1 = Tunnel established

4.9 SNMP

SNMP

The CP supports the following SNMP versions:

- **SNMPv1**

Available with enabled and disabled security functions

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

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

In the default setting, the CP uses the following community strings to authenticate access to its SNMP agent via SNMPv1:

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

*) Note the use of lowercase letters!

Note

Security of the access

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

The community strings can be configured when the security functions are enabled.

- **SNMPv3**

Available only when security functions are enabled

For information on configuring SNMPv3, refer to the section SNMP (Page 61).

Configuration

- **"Enable SNMP"**

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

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

4.10 Security

The configurability of the individual options depends on the telecontrol protocol being used.

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

For the configuration limits of the security functions refer to the section Configuration limits and performance data (Page 20).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 57).

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 Standard" or "NET Administrator" in the area below "Assigned roles".

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

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

4.10.2 Parameter overview

Parameter groups

If the security functions of the CP are enabled, you will find the following parameter groups for configuring the CP:

- **CP identification**

Only with the TeleControl Basic protocol

Here, you configure parameters for authenticating the CP with the telecontrol server. You will find detailed information about the parameters below.

- **DNP3 security options**

Only with the DNP3 protocol

Here, you configure protocol-specific security functions. You will find detailed information about the parameters below.

- **Firewall**

See section Firewall (Page 58).

- **Time-of-day synchronization**

For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 47).

- **E-mail configuration**

See section E-mail configuration (Page 60).

- **Log settings**

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

See section Log settings - Filtering of the system events (Page 61).

- **SNMP**

Here you make the settings for the SNMP agent on the CP.

See section SNMP (Page 61).

- **Certificate manager**

See section Certificate manager (Page 71).

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

- **VPN groups**

Here you configure the VPN communication, refer to the section VPN (Page 63).

- **User management**

Here you configure the users, roles and rights.

4.10.3 Firewall

4.10.3.1 Pre-check of messages by the MAC firewall.

Each incoming or outgoing frame initially runs through the MAC firewall (layer 2). If the frame is discarded at this level, it will not be checked by the IP firewall (layer 3). This means that with suitable MAC firewall rules, IP communication can be restricted or blocked.

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

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

- Separate the two IP addresses only using a hyphen.

Correct: 192.168.10.0-192.168.10.255

- Do not enter any other characters between the two IP addresses.

Incorrect: 192.168.10.0 - 192.168.10.255

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

4.10.3.3 Firewall settings for configured connection connections via a VPN tunnel

IP rules in advanced firewall mode

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

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

See section Settings for online security diagnostics and downloading to station with the firewall activated (Page 59) for information on this.

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

Setting the firewall for online functions

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

Global security functions:

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

Local security functions of the CP:

Now select the CP in the S7 station.

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

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

Note

Additional services for online security diagnostics and download

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

4.10.4 E-mail configuration

Configuring e-mails in STEP 7

With special events, e.g. CPU STOP, the CP can send e-mails. It does not depend on whether telecontrol communication is used.

When using telecontrol communication, additionally configured events in the process image of the CPU can trigger the sending of e-mails. Along with the e-mail process data can also be sent.

You configure the individual e-mails in the message editor (entry "Messages"), see section Messages (Page 74)

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

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

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

- Port no. 587

By using STARTTLS, the module sends encrypted e-mails to the SMTP server of your e-mail service provider.

Recommendation: If your e-mail provider offers both options (STARTTLS / SSL/TLS), you should use STARTTLS with port 587.

- Port no. 465

By using SSL/TLS (SMTPS), the module sends encrypted e-mails to the SMTP server of your e-mail service provider.

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

Importing the certificate with encrypted transfer

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

Use the certificate by taking the following steps:

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

For the procedure, refer to the section Handling certificates (Page 71).

4.10.5 Log settings - Filtering of the system events

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

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

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

4.10.6 SNMP

SNMP

The range of functions of the CP for SNMP can be found in the section SNMP (Page 92).

If the security functions are enabled, you have the following selection and setting options.

SNMP

- **"Enable SNMP"**

If the option is enabled, communication via SNMP is released on the device. As default, SNMPv1 is enabled.

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

- **"Use SNMPv1"**

Enables the use of SNMPv1 for the CP. For information on the configuration of the required community strings see below (SNMPv1).

- **"Use SNMPv3"**

Enables the use of SNMPv3 for the CP. For information on the configuration of the required algorithms see below (SNMPv3).

SNMPv1

The community strings need to be sent along with queries to the CP via SNMPv1.

- **"Reading community string"**

The string is required for read access.

Leave the preset string "public" or configure a string.

- **"Allow write access"**

If the option is enabled write access to the CP is released and the corresponding community string can be edited.

- **"Writing community string"**

The string is required for write access and can also be used for read access.

Leave the preset string "private" or configure a string.

Note the use of lowercase letters with the preset community strings!

Note

Security of the access

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

SNMPv3

The algorithms need to be configured for encrypted access to the CP via SNMPv3.

- **"Authentication algorithm"**

Select the authentication method to be used from the drop-down list.

- **"Encryption algorithm"**

Select the encryption method to be used from the drop-down list.

Note the information on security of the possible algorithms in the online help.

User management

In the user management that you will find in the global security settings, assign the various users their role.

Below the properties of the roles you can see the rights list of the particular role, for example the various types of access using SNMP. For new roles, you can freely configure individual rights.

You will find information on users, roles and the password policy in the information system of STEP 7.

4.10.7 VPN

4.10.7.1 VPN (Virtual Private Network)

VPN - IPsec

Virtual Private Network (VPN) is a technology for secure transportation of confidential data in public IP networks, for example the Internet. With VPN, a secure connection (IPsec tunnel) is set up and operated between two secure IT systems or networks via a non-secure network.

The IPsec tunnel forwards all data even from protocols of higher layers (HTTP, FTP, etc.).

The data traffic between two network components is transported unrestricted through another network. This allows entire networks to be connected together via a neighboring or intermediate network.

Properties

- VPN forms a logical subnet that is embedded in a neighboring (assigned) network. VPN uses the usual addressing mechanisms of the assigned network, however in terms of the data, it transports its own frames and therefore operates independent of the rest of this network.
- VPN allows communication of the VPN partners with the assigned network.
- VPN is based on tunnel technology and can be individually configured.
- Communication between the VPN partners is protected from eavesdropping or manipulation by using passwords, public keys or a digital certificate (authentication).

Areas of application

- Local area networks can be connected together securely via the Internet ("site-to-site" connection).
- Secure access to a company network ("end-to-site" connection)
- Secure access to a server ("end-to-end" connection)
- Communication between two servers without being accessible to third parties (end-to-end or host-to-host connection)
- Ensuring information security in networked automation systems
- Securing the computer systems including the associated data communication within an automation network or secure remote access via the Internet
- Secure remote access from a PC/programming device to automation devices or networks protected by security modules via public networks.

Cell protection concept

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

- Access to individual devices and network segments protected by security modules is allowed.
- Secure connections via non-secure network structures becomes possible.

Due to the combination of different security measures such as firewall, NAT/NAPT routers and VPN via IPsec tunnels, security modules protect against the following:

- Data espionage
- Data manipulation
- Unwanted access

4.10.7.2 Creating a VPN tunnel for S7 communication between stations

Requirements

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

- The two stations have been configured.
- The CPs in both stations must support the security functions.
- The Ethernet interfaces of the two stations are located in the same subnet.

Note

Communication also possible via an IP router

Communication between the two stations is also possible via an IP router. To use this communications path, however, you need to make further settings.

Procedure

To create a VPN tunnel, you need to work through the following steps:

1. Creating a security user
If the security user has already been created: Log on as this user.
2. Enable the "Activate security features" option
3. Creating the VPN group and assigning security modules
4. Configure the properties of the VPN group
5. Configure local VPN properties of the two CPs

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

Select "Activate security features"

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

You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

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

Note

Current date and current time on the CP for VPN connections

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

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

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

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

Configure the properties of the VPN group

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

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

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

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

Note

Specifying the VPN properties of the CPs

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

Result

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

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

4.10.7.3 VPN communication with SOFTNET Security Client (engineering station)

Set up VPN tunnel communication between the SOFTNET Security Client and the CP as described in section Creating a VPN tunnel for S7 communication between stations (Page 64).

VPN tunnel communication works only if the internal node is disabled

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

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

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

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

Disable the node in the SOFTNET Security Client tunnel overview:

1. Remove the checkmark in the "Enable active learning" check box.

The lower-level node initially disappears from the tunnel list.

2. In the tunnel list, select the required connection to the CP.

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

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

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

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

4.10.7.4 Establishment of VPN tunnel communication between the CP and SCALANCE M

Create a VPN tunnel between the CP and a SCALANCE M router as described for the stations.

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

If the check box is not selected, the CP rejects establishment of the tunnel.

4.10.7.5 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

4.10.7.6 SYSLOG

Use of SYSLOG only with 1 VPN connection

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

4.10.7.7 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect Server

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

- Exporting the CA certificate (optional)

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

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

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

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

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

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

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- CA Certificate

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

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

- Fingerprint

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

Authentication

- Device ID

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

- Device password

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

Max. number of characters: 127

Optional settings

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

- **Update interval**

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

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

- **"Connection type"**

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

- Auto

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

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

- PLC trigger

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

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

Note

Connection abort

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

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

- **PLC tag for connection establishment**

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

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

4.10.8 Certificate manager

Assignment of certificates

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

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

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

For a description of the procedure, refer to the section Handling certificates (Page 71).

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

4.10.9 Handling certificates

Certificate for authentication

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

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

Note

No certificate with security functions disabled.

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

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

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

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

The steps are described in the following sections.

Importing third-party certificates from communications partners

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

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

Assigning certificates in the global security settings

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

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

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

Assigning certificates locally

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

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

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

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

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

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

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

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

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

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

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

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

Certificate for logging server

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

Change certificate: Subject Alternative Name

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

You can change this parameter of a certificate in the certificate manager of the global security settings. To do this, select 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

You will find a description of the telecontrol-specific parameters in the configuration manuals, see /4/ (Page 106).

4.12 Messages

Configuring e-mails

If important events occur, the CP can send messages. E-mails are configurable. The recipient can be a PC with an Internet connection 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 will find the characters permitted for message texts and additional parameters in the section Character set for messages (Page 79).

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.

Information required to use e-mails:

- Access data of the SMTP server: Address, port number, user name, password
- When using STARTTLS or SSL/TLS: Certificate of the e-mail service provider
- E-mail addresses of the recipients

You create the configuration in the following parameter groups.

- Enabling security functions

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

- Configuration of the service / protocol:
"E-mail configuration", see section E-mail configuration (Page 60).
- When using STARTTLS or SSL/TLS:
 - Import of the certificate of the e-mail service provider:
"Global security settings"
 - Using the imported certificate for the CP:
Parameter group "Security" > "Certificate manager"

Configuration in the message editor

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

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

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

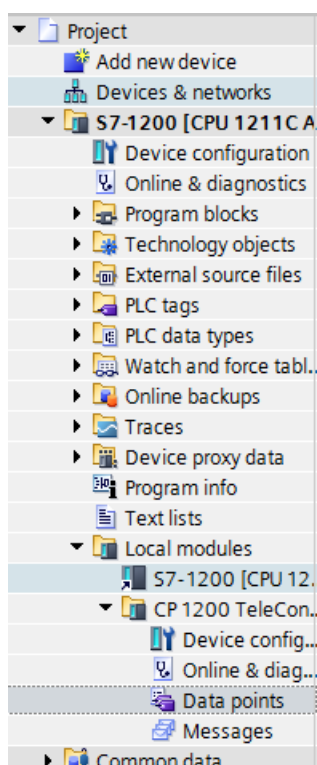


Figure 4-1 Opening the message editor via the project navigation

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



Figure 4-2 Switching over between the two editors

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

Creating objects

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

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

Arranging columns and rows, showing/hiding columns

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

- Arrange columns

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

- Sorting objects

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

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

- Adapting the column width

You can reach this function with the following actions:

- Using the shortcut menu that opens when you right-click on a column header:

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

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



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

- Showing/hiding columns

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

Copy messages

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

- Cut
- Copy
- Paste

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

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

- Delete

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

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

Tab for configuring the messages

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

"Message parameter"

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

"Trigger"

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

- **E-mail trigger**

Specifies the event for which the sending of the message is triggered:

- **Use PLC tag**

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

Resetting the trigger bit:

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

In all other cases, you need to reset the trigger bit with the user program.

Note

Fast setting of the diagnostics trigger tag

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

- **CPU changes to STOP**
- **CPU changes to RUN**
- **VPN connection established**

Triggers the sending of the message when the VPN connection is established or returns.
- **VPN connection terminated**

Triggers the sending of the message when the VPN connection is interrupted.
- **SINEMA RC connection established**

Triggers the sending of the message when the OpenVPN connection is established or returns.
- **SINEMA RC connection terminated**

Triggers the sending of the message when the OpenVPN connection is interrupted.
- **PLC tag for trigger**

PLC tag for the trigger "Use PLC tag"
- **Enable identifier for processing status**

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

The status is written to "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 e-mails (Page 93).
- **PLC tag for processing status**

PLC tag of the type DWORD for the processing status
- **Include value**

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

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

\$\$ as placeholder for the values of data points supports the following data types:
Bool, Byte, Char, Int, UInt, Word, DWord, UInt, DInt, Real, String,
arrays of the specified data types
- **PLC tag for value**

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

4.13 Character set for messages

Character set for message texts

The following ASCII character set (hexadecimal value and character name) is supported for the texts:

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

4.13 Character set for messages

Program blocks (OUC)

5.1 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

You can use the instructions (program blocks) listed below for direct communication between S7 stations.

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

Note**Different program block versions**

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

Requirements for Secure OUC

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

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

Supported program blocks for OUC

The following instructions in the specified minimum version are available for 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

- **TMAIL_C V4.0**

Sending e-mails

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

For changing configuration data of the CP during runtime:

- **T_CONFIG V1.0**

Program-controlled configuration of the IP parameters

Refer to the information on T_CONFIG and on the SDTs "IF_CONF_..." in the section Changing the IP address during runtime (Page 84).

Note

No feedback from the CP

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

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

Connection descriptions in system data types (SDTs)

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

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

Creating an SDT for the data blocks

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

The SDT type is not created by selecting an entry from the "Data type" drop-down list in the declaration table of the block, but by entering the name manually in the "Data type" box, for example "TCON_IP_V4".

The corresponding SDT is then created with its parameters.

Usable SDTs

- **TCON_IP_V4**

For transferring frames via TCP or UDP

- **TCON_QDN**

For TCP or UDP communication via the fully qualified domain name (FQDN) (IPv4 / IPv6)

- **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
- **TMail_V6**
For transferring e-mails addressing the e-mail server using an IPv6 address
- **TMail_FQDN**
For transferring e-mails addressing the e-mail server using its name (FQDN)
- **TCON_IP_V4_SEC**
For the secure transfer of data via TCP
- **TCON_QDN_SEC**
For the secure transfer of data via the host name
- **TMail_V4_SEC**
For secure transfer of e-mails addressing the e-mail server using an IPv4 address
- **TMail_V6_SEC**
For secure transfer of e-mails addressing the e-mail server using an IPv6 address
- **TMail_QDN_SEC**
For secure transfer of e-mails addressing the e-mail server using the host name

Note on TMail_Vx_SEC / TMail_QDN_SEC:

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

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

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.

5.2 Changing the IP address during runtime

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 Changing the IP address during runtime

Changing the IP address during runtime

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

- IP address
 - Subnet mask
 - Router address
-

Note

Changing the IP parameters with a dynamic IP address

Note the effects of program-controlled changes to the IP parameters if the CP obtains a dynamic IP address from the connected router: In this case, the CP can no longer be reached by communications partners.

Requirements - firmware version

Requirements for program-controlled changing of the IP parameters are as follows:

- CP firmware \geq V2.1.7x
and
- CPU firmware \geq V4.2

Requirements - program blocks / STEP 7 versions

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

Apart from the address parameters of the CP, with T_CONFIG the address parameters of DNS servers (IF_CONF_DNS) and NTP servers (IF_CONF_NTP) can also be changed program controlled.

Depending on the STEP 7 version, the following program blocks and system data types can be used:

- **STEP 7 Basic ≥ V14**

T_CONFIG

Along with:

- IF_CONF_V4
- IF_CONF_NTP
- IF_CONF_V6
- IF_CONF_DNS

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

Note**No feedback from the CP**

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

- **STEP 7 Basic ≤ V14**

TC_CONFIG

Along with:

- IF_CONF_V4

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

Requirements - CP programming

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

Diagnostics and upkeep

6.1 Diagnostics options

The following diagnostics options are available.

LEDs of the module

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

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

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

STEP 7 Basic: Diagnostics functions via 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 select the type of communication "Enable online functions"; see section Communication types (Page 46).

"Diagnostics" group

The diagnostics pages are divided into the following groups:

- **General**

This group displays general information on the module.

- **Diagnostics status**

This group displays status information of the module from the view of the CPU.

- Device-specific events

Information on internal module events is displayed here.

- **Ethernet interface**

Address and statistical information

- **Industrial Remote Communication**

The group has the following diagnostics pages:

- Partner

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

- Data point list

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

- Protocol diagnostics

With the button "Enable protocol trace", the frames received and sent by the module are logged for several seconds.

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

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

- **Time of day**

Information on the time on the device

- **Security**

The group has the following diagnostics pages:

- Status

This diagnostics page displays the most important security settings, the time of day, and data relating to the configuration.

- System log

You can start logging system entries on this diagnostics page if a connection to a SCALANCE S module is established. You can save the entries.

- Audit log

You can start logging the log data of the module on this diagnostics page. You can save the entries.

- Communication status

This diagnostics page shows the states of the known security modules of the VPN groups, their endpoints and the tunnel properties.

- SINEMA RC - automatic VPN configuration

This diagnostics page shows the status of the automatic OpenVPN configuration and the OpenVPN connections.

"Functions" group

- **Firmware update**

For a description, see section Downloading firmware (Page 95).

- **Assign IP address**

- **Assign PROFINET device name**
- **Save service data**

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

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

Diagnostics e-mail

If configurable events such as a CPU STOP occur, the CP can send a diagnostics e-mail. For information on configuration, see "Messages".

Partner status

When using telecontrol communication, the CP can signal the status of the connection to the communications partner to the CPU via a variable. You can display the status of the variable via the Web server of the CPU. You configure the variable in the following parameter group:

- TeleControl Basic: "Partner stations"
- DNP3 / IEC: "Communication with the CPU"

CP diagnostics

The CP can store extended diagnostic data in PLC tags. You can display the states of the PLC tags via the Web server of the CPU.

For information on the configuration, see section CP diagnostics (Page 54).

Web server of the CPU

Via the CP you can access the Web server of the CPU and the information available there. For access, refer to the section Access to the Web server (Page 52).

SNMP

For information on the functions, refer to the section SNMP (Page 92).

6.2 Web server S7-1200: Connection establishment

Establishing a connection to the Web server of the CPU

Follow the steps below to connect to the Web server of the CPU from a PC.

Requirements in the CPU configuration

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

The procedure for establishing a connection to the Web server depends on whether you have enabled or disabled the "Allow access only using HTTPS" option in the "General" parameter group:

- **Connection establishment with HTTP**

Procedure if the "Allow access only using HTTPS" option is disabled

- **Connection establishment with HTTPS**

Procedure if the "Allow access only using HTTPS" option is enabled

These two variants are described in the following sections.

You will find the requirements for access to the Web server of the CPU (permitted Web browser) and the description of the procedure in the STEP 7 information system under the keyword "Information about the Web server".

Connection establishment with HTTP

1. Connect the PC to the CPU via the Ethernet interface.
2. Enter the address of the CPU in the address box of your Web browser: `http://<IP address>`
3. Press the Enter key.
The start page of the Web server opens.
4. Click on the "Download certificate" entry at the top right of the window.
The "Certificate" dialog opens.

5. Download the certificate to your PC by clicking the "Install certificate ..." button.

The certificate is loaded on your PC.

You will find information on downloading a certificate in the help of your Web browser and in the STEP 7 information system under the key words "HTTPS" or "Access for HTTPS (S7-1200)".

6. When the connection has changed to the secure mode HTTPS ("https://<IP address>/..." in the address box of the Web server), you can continue as described in the next section.

When you terminate the connection to the Web server, the next time you can log in with the Web server without downloading the certificate using HTTP.

Connection establishment with HTTPS

1. Connect the PC to the CPU via the Ethernet interface.
2. Enter the address of the CPU in the address box of your Web browser: https://<IP address>
3. Press the Enter key.

The start page of the Web server opens.

4. Log in on the start page of the Web server as a user with the necessary rights.

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

5. After logging in, select the entry "Module status" in the navigation panel of the Web server.
6. Select the CP in the module list.

The CP-specific content is displayed.

6.3 Online security diagnostics via port 8448

Security diagnostics via port 8448

Requirements:

- Access to the Web server of the station is activated via HTTPS.
- With an activated firewall, access must be enabled.

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

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

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

See also

Settings for online security diagnostics and downloading to station with the firewall activated (Page 59)

6.4 SNMP

SNMP (Simple Network Management Protocol)

SNMP is a protocol for management and diagnostics of networks and nodes in the network. To transmit data, SNMP uses the connectionless UDP protocol.

The information on the properties of SNMP-compliant devices is stored in MIB files (MIB = Management Information Base).

Range of performance of the CP as an SNMP agent

The CP supports data queries in the following SNMP versions:

- SNMPv1 (standard)
- SNMPv3 (security)

It returns the contents of MIB objects of the standard MIB II according to RFC1213.

- **MIB II**

The CP supports the following groups of MIB objects:

- System
- Interfaces

The "Interfaces" MIB object provides status information about the CP interfaces.

- IP
- ICMP
- TCP
- UDP
- SNMP

The following groups of the MIB II standard are not supported:

- Address Translation (AT)
- EGP
- Transmission

- **LLDP MIB**

Traps are not supported by the CP.

For more detailed information about the MIB files and SNMP, refer to the manual /5/ (Page 106).

Configuration

For information on the configuration, refer to:

- With security functions disabled (SNMPv1): SNMP (Page 56)
- With security functions enabled (SNMPv1 / SNMPv3): SNMP (Page 61)

6.5 Processing status of e-mails

Configuration of the processing status of e-mails

The following status identifiers apply to e-mails configured with the message editor of the CP. The output of status identifiers is enabled by the option "Enable identifier for processing status". The status identifier is written to the "PLC tag for processing status" in the CPU.

For information on the configuration, refer to the section E-mail configuration (Page 60).

Outputting the processing status of e-mails

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

If there are problems delivering messages, you can determine the status via the Web server of the CPU.

Processing status of e-mails

The meaning of the status identifiers of the "PLC tag for processing status" is as follows:

Table 6- 1 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 message 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.

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

6.6 Downloading firmware

New firmware versions of the CP

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

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15922/dl>)

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

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

- Saving the firmware file on the memory card of the CPU

You will find a description of the procedure for loading on the memory card of the CPU on the Internet page of the Siemens Industry Online Support.

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

Note

Effects on the retentive memory of the CPU

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

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

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

Requirements:

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

Procedure:

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

6. Select the slot of the CP or the CPU.

Both methods are possible.


7. Connect using the "Connect" button.

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

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

6.7 Module replacement

Module replacement

 CAUTION
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 the CP without needing to download the project data to the station again.

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

Exception:

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

Technical data

7.1 Technical specifications of the CP 1243-1

Table 7- 1 Technical specifications of the CP 1243-1

Technical specifications		
Article number	6GK7 243-1BX30-0XE0	
Attachment to Industrial Ethernet		
Quantity	1	
Design	RJ-45 jack	
Properties	100BASE-TX, IEEE 802.3-2005, half duplex/full duplex, autocrossover, autonegotiation, galvanically isolated	
Transmission speed	10/100 Mbps	
Permitted cable lengths (Ethernet)	(Alternative combinations per length range) *	
0 ... 55 m	<ul style="list-style-type: none"> • Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180 • Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet 	
0 ... 85 m	<ul style="list-style-type: none"> • Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180 • Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet 	
0 ... 100 m	<ul style="list-style-type: none"> • Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180 • Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet 	
Electrical data		
Power supply	From the S7-1200 backplane bus	5 VDC
Current consumption (typical)	From the S7-1200 backplane bus	250 mA
Effective power loss (typical)	From the S7-1200 backplane bus	1.25 W
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally	-20 °C to +70 °C
	During operation with the rack installed vertically	-20 °C to +60 °C
	During storage	-40 °C to +70 °C
	During transportation	-40 °C to +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation

7.2 Pinout of the Ethernet interface

Technical specifications	
Design, dimensions and weight	
Module format	Compact module for S7-1200, single width
Degree of protection	IP20
Weight	122 g
Dimensions (W x H x D)	30 x 110 x 75 mm
Installation options	Standard DIN rail Switch panel
Product functions **	

* For details, refer to the IK PI catalog, cabling technology

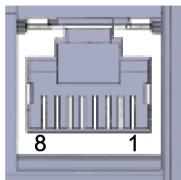
**You will find further characteristics and performance data in the section Application and functions (Page 13).

7.2 Pinout of the Ethernet interface

Pinout of the Ethernet interface

The table below shows the pin assignment of the Ethernet interface. The pin assignment corresponds to the Ethernet standard 802.3-2005, 100BASE-TX version.

Table 7- 2 Pin assignment of the Ethernet interface

View of the RJ-45 jack	Pin	Signal name	Assignment
	1	TD	Transmit Data +
	2	TD_N	Transmit Data -
	3	RD	Receive Data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive Data -
	7	GND	Ground
	8	GND	Ground

Approvals

Approvals issued

Note

Issued approvals on the type plate of the device

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

The CP has the following approvals and meets the following standards:

EC declaration of conformity



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

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

Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356

- **2014/30/EU (EMC)**

EMC directive of the European Parliament and of the Council of February 26, 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility.; official journal of the EU L96, 29/03/2014, pages. 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

The EC Declaration of Conformity is available for all responsible authorities at:

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

You will find the EC Declaration of Conformity for this product on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15922/cert>) > "EC Declaration of Conformity"

IECEX

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

IECEX classification:

- Ex ec IIC T4 Gc

Certificate: IECEx DEK 18.0019X

Applied standards:

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

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

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15922/cert>)

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 35).

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

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

ATEX



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

ATEX approval:

- II 3 G Ex ec IIC T4 Gc

Type Examination Certificate: DEKRA 18 ATEX 0027X

Applied standards:

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

 WARNING
Installation guidelines
The product meets the requirements if you keep to the following during installation and operation:
<ul style="list-style-type: none">• The notes in the section Important notes on using the device (Page 33)• The installation instructions in the document /1/ (Page 105)

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

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 35).

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

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

c(UL)us



Applied standards:

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

File Number: E223122

cULus Hazardous (Classified) Locations



Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

Applied standards:

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

APPROVED for Use in:

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

Report / UL file: E223122 (NRAG.E223122)

Observe the conditions for safe usage of the CP according to the section Notices regarding use in hazardous areas according to UL HazLoc (Page 35).

FM



Factory Mutual Approval Standard Class Number 3600, 3611, 3810, ANSI/ISA-61010-1

Equipment rating:

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

Report Number: 3049779, 3049925

Observe the conditions for safe usage of the CP according to the section Notices on use in hazardous areas according to FM (Page 36).

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

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/15922/cert>)

Dimension drawings

Note

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

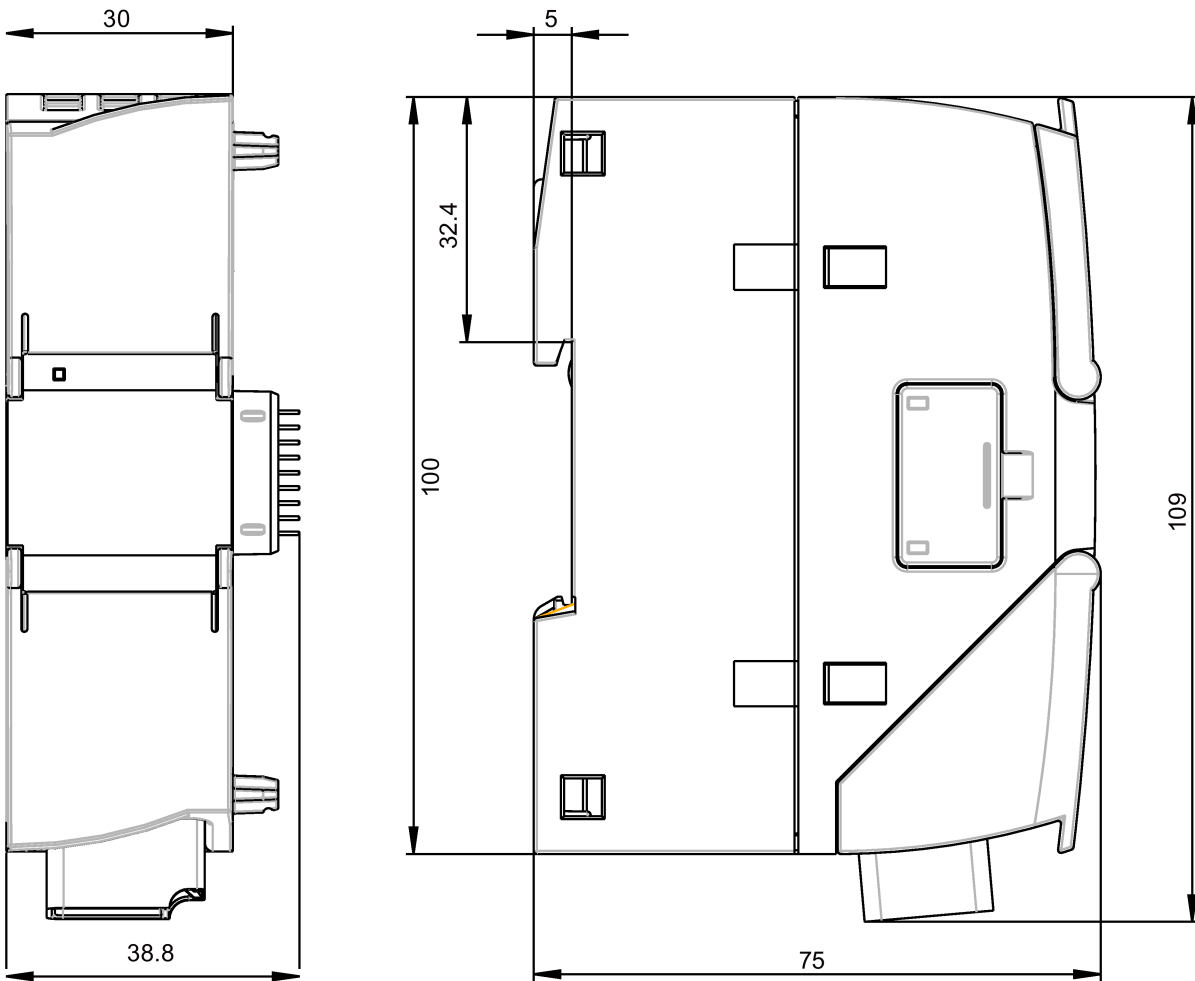


Figure B-1 Front view and side view left

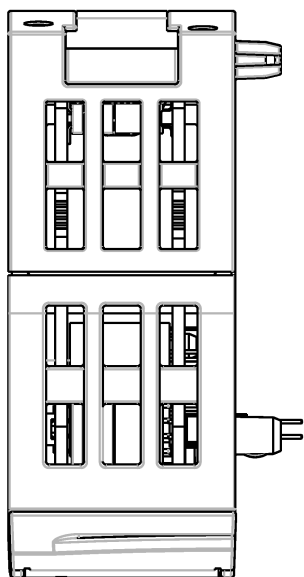


Figure B-2 From above

Documentation references

Where to find Siemens documentation

- Article numbers

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

- SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI
- SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70

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

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

- Manuals on the Internet

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

Link: (<https://support.industry.siemens.com/cs/ww/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.

/1/

SIMATIC
S7-1200 Automation System
system manual
Siemens AG

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/13683/man>)

/2/

/2/

SIMATIC NET
CP 1243-1
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/103948898>)

/3/

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

/4/

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>)

/5/

SIMATIC NET
Diagnostics and configuration with SNMP
Diagnostics manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15392/man>)

Index

A

Abbreviations, 4
Article number, 3

C

Connection resources, 20
CPU firmware, 25
Cross references (PDF), 6

D

Data buffering, 21
Dimensions, 37
Disposal, 7
DNS server - program-controlled change, 84

E

E-mail
 Configuration, 74
 Programming (OUC), 81
 Quantity, 21
Ethernet interface
 Assignment, 98

F

Firewall, 18
Firmware version, 3
Frame memory, 21

G

Gateway (VPN), 67
Glossary, 7

H

Hardware product version, 3

I

Importing a certificate - e-mail, 61
Instructions (OUC), 81
IP address - program-controlled change, 84
IP configuration
 IPv4, IPv6, 16
IP_CONF_V4, 84
IPsec, 63

L

Logging server, 73

M

MAC address, 3
MIB, 92

N

NTP, 49
NTP (secure), 49
NTP server - program-controlled change, 84
IPsec tunnel,

O

Online diagnostics, 87
Online functions, 17, 46, 88
Operating statuses (LED displays), 30
OUC (Open User Communication), 81
OUC connections
 Resources, 20

P

Passive VPN connection establishment, 67
PG/OP connections, 21
Port 8448, 91
Product name, 4
Program blocks, 14

R

Recycling, 7
Replacing a module, 96

S

S7 connections
 Enable, 46
 Resources, 20
S7 routing, 14
Safety notices, 33
Security, 18
Security diagnostics, 91
Send buffer, 21
Service & Support, 8
SIMATIC NET glossary, 7
SMS
 Programming (OUC), 81
SMTPS, 60
SNMP, 17, 56, 92
SNMPv3, 19, 61
SSL/TLS, 60
STARTTLS, 60
STEP 7 - version, 25
SYSLOG, 67

T

T_CONFIG, 84
TC_CONFIG, 84
Time-of-day synchronization, 16
Training, 8

V

VPN, 21, 63

W

Web server, 52