SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-1

Operating Instructions

07/2014

C79000-G8976-C365-01

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C365-01
℗ 08/2014 Subject to change

Preface

Validity of this manual

This document contains information on the following telecontrol product:

- **CP 1243-1**
  Article number6GK7 243-1BX30-0XE0
  Hardware product version 2
  Firmware version V2.0

  The CP 1243-1 is the communications processor for connecting the SIMATIC S7-1200 to a public infrastructure (e.g. DSL) to a control center with TELECONTROL SERVER BASIC (TCSB Version V3).

  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 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**

  The term "CP" is used below instead of the full product name CP 1243-1.

- **TCSB**

  This acronym 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.

Purpose of the manual

This manual describes the properties of this module and supports you when installing and commissioning it.

The required configuration steps are described as an overview and there are explanations of the relationship between firmware functions and configuration.

You will also find information about the diagnostics options of the device.

Current manual release on the Internet

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

89332514 (http://support.automation.siemens.com/WW/view/en/89332514)

Required experience

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

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

Requirements for use of the module

You will find the requirements for using the module in the section Hardware requirements (Page 17).

Sources of information and other documentation

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

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

License conditions

Note

Open source software

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

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

- DOC_OSS-S7CMCP_74.pdf
- DOC_OSS-CP1243-1_76.pdf

Security information

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

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

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

Training, Service & Support

You will find information on Training, Service & Support in the multi--language document "DC_support_99.pdf" on the data medium supplied with the documentation.

Table of contents

Application and properties

1

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 a control center with TELECONTROL SERVER BASIC (TCSB version V3).

With the combination of different security functions such as firewall and protocols for data encryption, the CP protects the station and even entire automation cells from unauthorized access and protects the communication between the remote S7 station and the master station (TCSB) from espionage and manipulation.

1.2 Communications services

Communications services

The following communications services are supported:

- **Telecontrol communication**

  The CP is a communications processor of the SIMATIC S7-1200 for system connection to control centers with the OPC server application TCSB.

  The communications protocol used allows IP-based data transmission for telecontrol applications. As an integrated (unconfigurable) Security function, the telecontrol protocol encrypts the data for transfer between the CP and telecontrol server.

  For a description of the configurable Security functions, refer to the section Other services and properties (Page 10).

- **S7 communication and PG/OP communication with the following functions:**
  - PUT/GET as client and server for data exchange with remote stations (S7-300/400/1200/1500)
  - PG functions
  - Operator control and monitoring functions (HMI)

1.3 Other services and properties

Other services and properties

- **Data point configuration**

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

- **IP configuration - IPv4 and IPv6**

  The essential features of IP configuration for the CP:

  – The CP supports IP addresses according to IPv4 and IPv6.

    For telecontrol applications 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**

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

    For information on the format of the time stamp, refer to the section Datapoint types (Page 34).

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

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

  For more information, refer to the section Time-of-day synchronization (Page 46).

- **Redundancy**

  The CP can communicate with a redundant installation of TCSB.

- **Storage of events**

  The CP can store events of different classes and transfer them together to the TCSB.

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

  The telecontrol communication with TCSB is triggered in two ways:

  – After a request by TCSB or an OPC client connected to TCSB

  – Triggered by various selectable criteria

- **Messages / e-mail**

  With configured events in the process image of the CPU, the CP can send messages as e-mails. The data sent by e-mail is configured using PLC tags.

- **Analog value processing**

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

- **Online functions**

  From an engineering station (ES) on which STEP 7 is installed, you can use the online functions of STEP 7 via the CP to access the S7-1200 CPU if the station is located in the same IP subnet. Online access via the telecontrol server is not possible.

  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 a remote station located in a different IP subnet or that can be reached via the Internet, these functions can only be used if the ES (with CP 1628 or via SCALANCE S) is connected to the station via a VPN tunnel.

- **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 47).

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 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 ("Bandwidth limitation")

  – Global firewall rules

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

  VPN tunnel communication allows the establishment of secure IPsec tunnels for communication with one or more security modules.

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

- **Logging**

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

- **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.

For information on configuring the security functions, refer to the section Security functions (Page 39).

You will find further information on the functionality and configuration of the security functions in the information system of STEP 7 and in the manual /4/ (Page 78).

1.4 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.

To use telecontrol communication, three CP 1243-1 modules can be plugged in per station that communicate with three telecontrol servers.

Connection resources

- **Telecontrol connections**

  The CP can establish corrections to non-redundant or redundant telecontrol servers (TCSB).

  In addition to this, inter-station communication with up to 4 S7 stations with a CP 1243-1 can be operated via the telecontrol server.

- **TCP connections**

  The CP can establish connections to up to 4 communications partners (S7 stations).

- **Online functions**

  1 connection resource is reserved for online functions.

- **S7 connections**

  8 connection resources for S7 connections (PUT/GET)

- **PG/OP connections**
  - 1 connection resource for PG connections
  - 3 connection resources for OP connections

Number of data points for the data point configuration

The maximum number of configurable data points is 200.

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. You will find details in the section Datapoint types (Page 34).

Frame memory (send buffer)

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

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, refer to the section Communication with the CPU (Page 55).

You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Types of transmission, event classes, triggers, status identifiers (Page 36).

Messages / e-mail

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

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")

1.5 Configuration examples

Telecontrol with a non-redundant master station (TCSB)

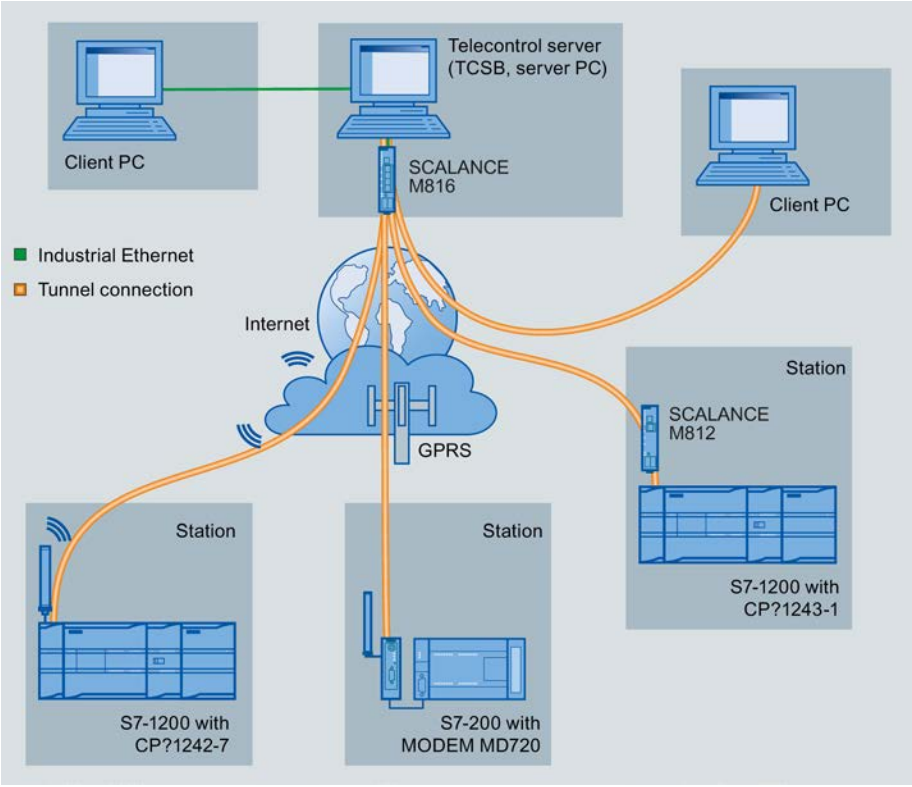


Figure 1-1 **Communication between S7 stations and a master station (TCSB)**

In the telecontrol applications of the example shown, SIMATIC S7 stations communicate with a non-redundant telecontrol server (TCSB) in the master station.

- Telecontrol communication between stations and master station

  The communication is via the following paths and communications modules:

  – Communication via the Internet: S7-1200 with CP 1243-1

  – Communication via the GSM network and the Internet: S7-1200 with CP 1242-7 or S7-200 with MODEM MD720

  The establishment of terminal connections with encryption is initiated automatically by the telecontrol protocol used by the various communications modules.

  The creation of VPN connections between the CP 1243-1 and telecontrol server is optional.

  The telecontrol server monitors the connections established by the remote stations.

- Inter-station communication

  Stations of the same type, for example S7-1200 with CP 1243-1, can communicate with each other by sending the frames via the telecontrol server.

Telecontrol with a redundant master station (TCSB)

The following figure shows a possible configuration with S7 stations communicating with a redundant master station (TCSB).

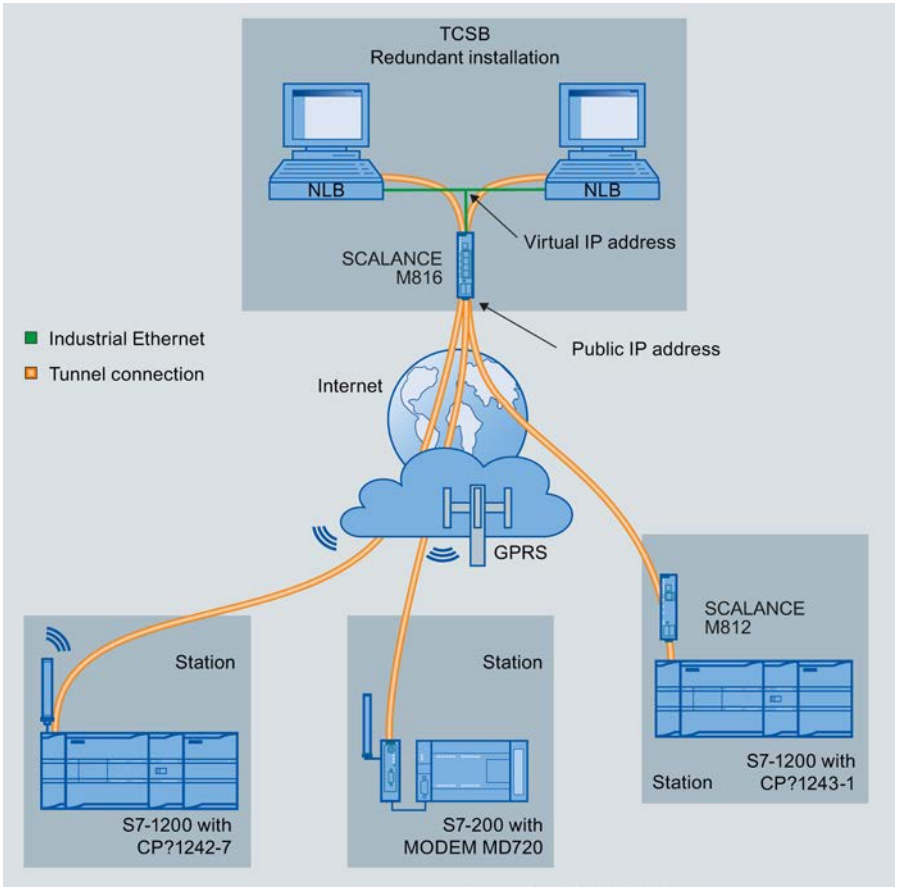


Figure 1-2 **S7 station communication with a redundant a master station**

Requirements for use 2

2.1 Hardware requirements

The following description relates to a configuration with telecontrol communication with TCSB.

Rails, housing, cabling and other accessories are not taken into account.

Depending on the configuration of your plant, you require the following devices and firmware versions.

Application example: Telecontrol communication with TCSB

In the S7-1200 station:

- CPU firmware version: 3.0, 4.0
- Mobile wireless router SCALANCE M812

In the master station:

- PC with TCSB (version V3)
- Mobile wireless router SCALANCE M816

For more detailed information on the structure of TCSB , refer to the section /3/ (Page 78).

- When using online functions: Engineering station with STEP 7 (refer to the section Software requirements (Page 17)).

For the configuration of the S7 station with CP:

Engineering station with STEP 7

2.2 Software requirements

Configuration software

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

- STEP 7 Basic / Professional V13.0 with support package 0093

Software for online functions

STEP 7 in the version specified above

LEDs and connectors

3

3.1 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.

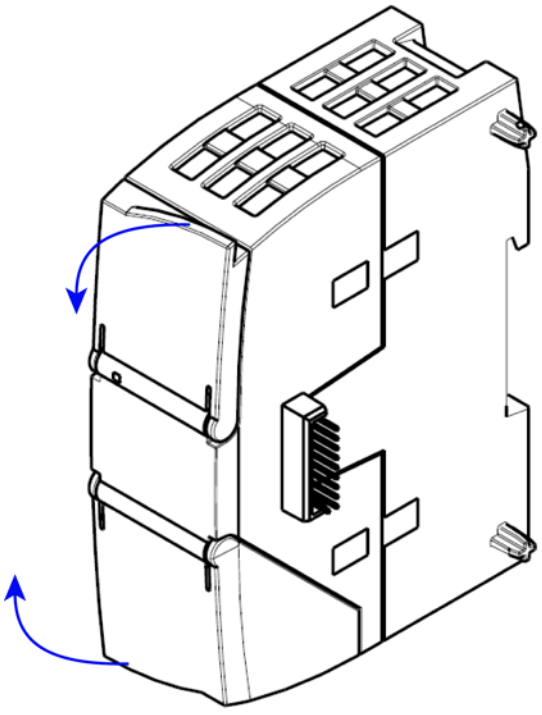


Figure 3-1 Opening the covers of the housing

3.2 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 3- 1 **LED on the front panel**

LED / colors	Name	Meaning
(red / green)	DIAG	Basic status of the module

Table 3- 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 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 3- 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 3- 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	
○	• Power OFF • Incorrect startup
● green	Running (RUN) without serious error
☼ flashing green	• Partner not connected • Firmware loaded successfully
☼ flashing red	• Starting up • Module fault • Invalid STEP 7 project data
◉ flashing red-green	Error loading firmware

Display of the operating and communications statuses

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

Table 3- 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

DIAG (red / green)	-	LINK (green)	CONNECT (green)	VPN (green)	SERVICE (green)	Meaning (if more than one point listed: alternative meaning)
flashing red		-	○	-	-	Missing STEP 7 project data
flashing red		●	☼	-	-	Backplane bus error
Connection to Industrial Ethernet						
-		●	-	-	-	Connection to Industrial Ethernet exists
green		☼	-	-	-	• 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, CPU in RUN mode
flashing green		●	☼	-	-	Partner not reachable, CPU in STOP mode
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 connection						
green		●	-	●	-	VPN connection configured on the CP
-		-	-	○	-	No VPN connection configured on the CP

DIAG (red / green)	-	LINK (green)	CONNECT (green)	VPN (green)	SERVICE (green)	Meaning (if more than one point listed: alternative meaning)
Loading firmware						
						Loading firmware. The DIAG LED flashes alternating red and green.
 flashing green						Firmware was successfully loaded.
 flashing red						Error loading firmware

3.3 Electrical connectors

3.3.1 Power supply

Power supply

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

3.3.2 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 69).

Installation, connecting up, commissioning 4

4.1 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

4.1.1 Notices on use in hazardous areas

⚠ WARNING
EXPLOSION HAZARD DO NOT OPEN WHEN ENERGIZED.

⚠ 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.

4.1.2 General notices on use in hazardous areas according to ATEX

WARNING

Requirements for the cabinet/enclosure

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

WARNING

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

WARNING

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

4.1.3 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.

4.2 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

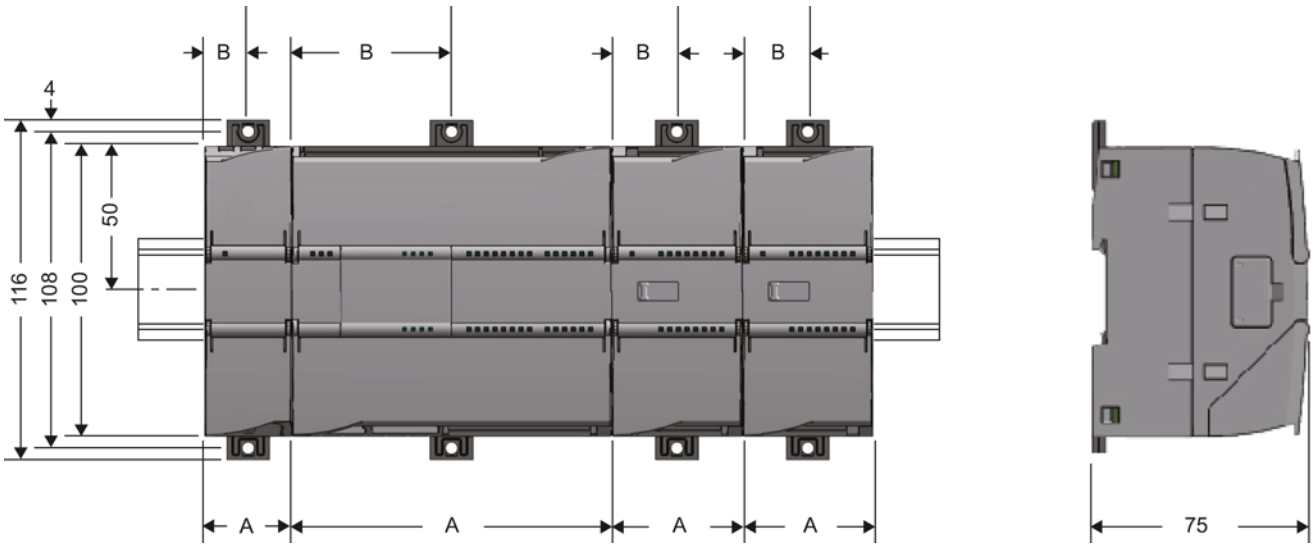


Figure 4-1 Dimensions for installation of the S7-1200

Table 4- 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 interfaces (examples)	CM 1241 RS-232 and CM 1241 RS-485	30 mm	15 mm
	CM 1243-5, CM 1242-5 (PROFIBUS master / slave)	30 mm	15 mm
	CP 1242-7	30 mm	15 mm
	CP 1243-1	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

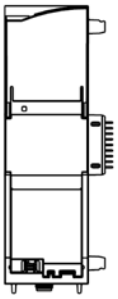
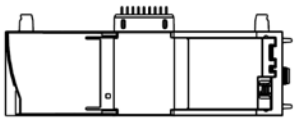
You will find detailed dimensions of the module in the section Dimension drawings (Page 75).

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.

Device position / permitted temperature range	Installation location
Horizontal installation of the rack: -20 °C to +70 °C	
Vertical installation of the rack: -20 °C to +60 °C	

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 4- 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 69).
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: • "Loading project data" • "Using online and diagnostics functions"
6	Close the front covers of the module and keep them closed during operation.	

Configuration and operation 5

5.1 Note on operation

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

5.2 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 17).

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

STEP 7 online help in "Support Packages"

The current online help topics dealing with the CP and the security functions are available in the STEP 7 information system under the entry "Support Packages".

Requirement for configuring the communication

One requirement for configuring communication between CP and TCSB is the programming of the assigned CPU and the input and output data of the station.

PLC tags must also be created to assign the user data to the data points.

For more detailed information, refer to the following sections.

How to configure telecontrol communication in STEP 7

Follow the steps below when configuring:

1. Create a STEP 7 project.
2. Insert the required SIMATIC stations.

   Configuration of TCSB and connections between CP and TCSB is neither possible nor necessary.
3. Insert the CPs and the required input and output modules in the stations.

4. Create an Ethernet network.
5. Connect the stations to the Ethernet subnet.
6. Configure the inserted CPs.

   For details on configuring the communication, refer to the following section.
7. Save the project.

You will find more detailed information on configuring the CP in the Information system of STEP 7 and in the following sections.

The configuration of the security functions is optional. You will find information in the section Security functions (Page 39).

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.

5.3 Address and authentication information

IP address of the CP

Since the CP always establishes the connection to TCSB, a dynamic IP address can be assigned to the CP by the Internet service provider.

Address and authentication information for communication with TCSB

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

- Parameters in the "Partner stations" parameter group
  - Partner IP address

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

5.4 Configuring the data points

Data point-related communication

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

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

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

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

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

Note

Number of PLC tags

Remember the maximum possible number of PLC tags the can be used for data point configuration in the section Configuration limits and performance data (Page 12).

The formats and S7 data types of the PLC tags that are compatible with the protocol-specific data point types of the CP can be found in the section Datapoint types (Page 34).

Access to the memory areas of the CPU

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

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

Configuring data points and messages in STEP 7

You configure the data points in STEP 7 in the Data point and alarm configuration. You can find this using the project tree:

Project > directory of the relevant station > Local modules > CP 1243-1

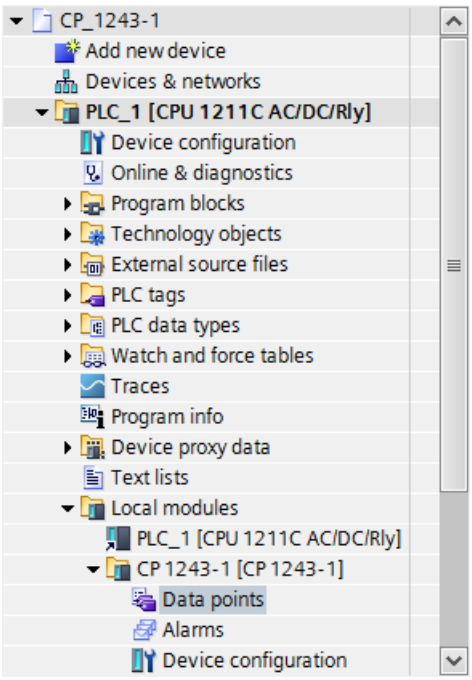


Figure 5-1 Configuring data points and messages (e-mails)

Here, you will find the editor for configuring messages.

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

5.5 Datapoint types

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

CP 1243-1: Supported data point types

Table 5- 1 Supported data point types and compatible S7 data types

Format (memory requirements)	Data point type	S7 data types	Address area
Bit	Digital input	BOOL	I, Q, M, DB
	Digital output	BOOL	I, Q, M, DB
	Command output	BOOL	I, Q, M, DB
Byte	Digital input	BYTE, CHAR	I, Q, M, DB
	Digital output	BYTE, CHAR	I, Q, M, DB
Integer with sign (16 bits)	Analog input	INT	I, Q, M, DB

Format (memory requirements)	Data point type	S7 data types	Address area
	Analog output	INT	I, Q, M, DB
Counter (16 bits)	Counter input	WORD	I, Q, M, DB
Integer with sign (32 bits)	Analog input	DINT	I, Q, M, DB
	Analog output	DINT	I, Q, M, DB
Counter (32 bits)	Counter input	DWORD, UDINT	I, Q, M, DB
Floating-point number with sign (32 bits)	Analog input	REAL	Q, M, DB
	Analog output	REAL	Q, M, DB
Floating-point number with sign (64 bits)	Analog input	LREAL	Q, M, DB
	Analog output	LREAL	Q, M, DB
Block of data (1 .. 64 bytes)	Data	ARRAY [1)]	DB
	Data	ARRAY [1)]	DB

[1)] For the possible formats of the ARRAY data type, refer to the following section.

Block of data (ARRAY)

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

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

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

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

Time stamp in UTC format

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

5.6 CPU scan cycle

Structure of the CPU scan cycle

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

- **High-priority read jobs**

  For data points of the type "Input", which are configured with the "High priority" setting in the data point configuration in "General > Priority in the scan cycle", the PLC tags are all read in one scan cycle.

- **Write jobs**

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

- **Low-priority read jobs - proportion**

  For data points of the type "Input", which are configured with the "Low priority" setting in the data point configuration in "General > Priority in the scan cycle", the values of a part of the PLC tags are read in every scan cycle.

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

- **Cycle pause time**

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

Duration of the CPU scan cycle

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

5.7 Types of transmission, event classes, triggers, status identifiers

Classification of the data points and storage of the values

The values of data points are stored in the image memory of the CP and transferred only when called by TCSB. Events are also stored in the send buffer and can be transferred unsolicited. All data points are therefore classified as follows:

- **No event (static value)**

  Data points that are not configured as an event ("Transfer after call") are entered in the image memory (process image of the CP).

- **Event**

  The values of data points configured as an event are also entered in the image memory of the CP. Of the value of the event is sent unsolicited to TCSB.

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

The image memory

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

The values are sent after being queried by the communications partner. Refer to "Transfer after call" in the section "Types of transmission".

The send buffer

The send buffer is the data buffer on the CP for storing the values of events. The send buffer has a maximum size of 64000 events. The configured number of events is divided equally among all configured and enabled communications partners. The "Data buffer size" parameter for the size of the send buffer is described in the section Communication with the CPU (Page 55).

If a connection to a communications partner is interrupted, the values of the events are retained in the buffer. When the connection returns, the buffered frames are sent.

The frame memory operates chronologically; in other words, the oldest frames are sent first (FIFO principle). When the maximum number of events is reached and the frames could not be sent, the oldest values are overwritten.

Types of transmission

Depending on your CP type, you have the following transmission types available:

- **Transfer after call**

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

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

- **Event class**

  The value is entered in the send buffer as an event and transferred unsolicited to the communications partner when the trigger fires.

  You will find details of the event classes and triggers in the following sections.

The type of transmission is specified for each data point in the data point configuration in STEP 7 with the "Type of transmission" or "Event class" parameter.

Event classes

The process data of the various event classes is handled as follows:

- **Every value triggered**

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

- **Current value triggered**

  Only the current value at the time the trigger condition was met is entered in the image memory and overwrites the last value stored there.

Trigger

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

- **Threshold value trigger**

  The value of the data point is transferred when this reaches a certain threshold. The threshold is calculated as the difference compared with the last stored value, refer to the section Threshold value trigger (Page 60).

- **Time trigger**

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

- **Event trigger**

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

Resetting the trigger bit in the bit memory area / DB

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

Generation of events if a data point status changes

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

Example: If the status "RESTART" of a data point configured as an event changes to "Value updated" when the station starts up, this causes an event to be generated.

Status IDs of data points

The status IDs listed in the following tables are transferred for each data point in each frame in 1 byte.

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

Table 5- 2 Byte assignment of the status byte for data points

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

5.8 Security functions

Note the range and application of the security functions of the CP, refer to the section Other services and properties (Page 10).

5.8.1 VPN

5.8.1.1 VPN (Virtual Private Network)

VPN tunnel

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

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

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

Properties

- VPN forms a logical subnet that is embedded in a neighboring (assigned) network. VPN uses the usual addressing mechanisms of the assigned network, however in terms of the data, it transports its own frames and therefore operates independent of the rest of this network.
- VPN allows communication of the VPN partners 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

5.8.1.2 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 a user.

2. Select the "Activate security features" check box

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

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

Creating a security user

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

1. In the local security settings of the CP, click the "User login" button.

   Result: A new window opens.
2. Enter the user name, password and confirmation of the password.
3. Click the "Logon" button.

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

With all further logons, log on as user.

Select the "Activate security features" check box

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

You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

1. In the global security settings, select the entry "Firewall" > "VPN groups" > "Add new VPN group".
2. Double-click on the entry "Add new VPN group", to create a VPN group.

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

Note

Current date and current time on the CP for VPN connections

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

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

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

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

Configure the properties of the VPN group

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

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

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

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

Note

Specifying the VPN properties of the CPs

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

Result

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

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

5.8.1.3 VPN communication with SOFTNET Security Client (engineering station)

Setting up VPN tunnel communication between the SOFTNET Security Client and CP 1243-1 is essentially the same as described in Procedure for S7-1200 stations (Page 40).

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 1243-1 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 1243-1.

To establish successful VPN tunnel communication to the CP 1243-1, 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 1243-1.
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 to the CP 1243-1 can be established.

5.8.1.4 Creating the VPN connection telecontrol server

Configuration of a VPN connection between CP and TCSB

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

To configure the communication between the CP 1243-1 and TCSB via a VPN connection, follow the steps below:

- Create a PC station as a substitute for the telecontrol server.

  This PC station serves as a placeholder for the telecontrol server only for configuration of the security group and it is not required for any other purpose.
- To set up the security functions you then have the following alternative options:
  - Install a CP 1628 (security module) on the computer of the telecontrol server and assign the CP 1243-1 and the CP 1628 to the same security group in the configuration.
  - Install the SOFTNET Security Client (license required) on the computer of the telecontrol server and configure the security functions in the STEP 7 project.

With both options you achieve the requirements at the TCSB end for secure communication between the CPs of the remote station and the telecontrol server via secure VPN connections.

Configure the security functions of the CPs as described above.

5.8.1.5 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.

5.8.1.6 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

5.8.2 Firewall

5.8.2.1 Firewall sequence when checking incoming and outgoing frames

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

5.8.2.2 Online diagnostics and downloading to station with the firewall activated

Firewall settings of the CP for an engineering station with Windows XP

On the engineering station with Windows XP, when there is online access from STEP 7 to the S7-1200 via the Ethernet interface of the CP, a ping is sent to the module. This checks the reachability of the partner.

To allow STEP 7 to establish an online connection via the Ethernet interface of the CP for diagnostics or downloading when the CP firewall is activated, access with ping commands must be allowed in the firewall.

If you use STEP 7 with Windows 7, no ping packet is sent.

Setting the firewall - steps involved

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

1. In the global security settings (see project tree), select the entry "Firewall > Services > Define services for IP rules".
2. Select the "ICMP" tab.
3. Insert a new entry of the type "Echo Reply" and another of the type "Echo Request".
4. Now select the CP in the S7-1200 station.
5. Enable the advanced firewall mode in the local security settings of the CP in the "Security > Firewall" parameter group.
6. Open the "IP rules" parameter group.
7. In the table, insert a new IP rule for the previously created global services as follows:
   - Action: Allow; "From external -> To station " with the globally created "Echo request" service
   - Action: Allow; "From station -> to external" with the globally created "Echo reply" service
8. For the IP rule for the Echo Request, enter the IP address of the PG/PC in "Source IP address". This ensures that only PING packets from your PG/PC can pass through the firewall.

5.8.2.3 Transmission speed < 1 Mbps not effective

In advanced firewall mode (parameter "Bandwidth"), it is not possible to limit the transmission speed to values < 1 Mbps.

The selection is restricted to the following range of values: 1 ... 100 Mbps

5.8.2.4 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 1243-1, 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.

5.8.2.5 Firewall settings for S7 connections via a VPN tunnel

IP rules in advanced firewall mode

If you set up S7 connections with a VPN tunnel between the CP 1243-1 and a communications partner, you will need to adapt the firewall settings of the CP 1243-1:

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

5.8.3 Filtering of the system events

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

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

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

5.9 Time-of-day synchronization

Procedure for time-of-day synchronization

Note

Recommendation for setting the time

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

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

- Time from partner

  In this case, the time of day is synchronized by the telecontrol server. This method is enabled automatically if telecontrol communication is enabled in "Communication types" in STEP 7.

- NTP

  If telecontrol communication is disabled, the time of day can only be synchronized by an NTP or NTP (secure) server. Here, configure the synchronization mode, the local time zone of the station, the synchronization interval and the addresses of the NTP servers.

Note

Special feature of time-of-day synchronization using NTP

If the option "Accept time from non-synchronized NTP servers" is not selected, the response is as follows:

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

NTP (secure) with security functions enabled

In the extended NTP configuration, you can create and manage additional NTP servers including those of the type NTP (secure).

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

Note

Ensuring a valid time of day

If you use security functions, a valid time of day is extremely important. If you do not obtain the time of day from the telecontrol server (telecontrol communication is not enabled), it is advisable to use the NTP (secure) method.

Configuration

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

5.10 SNMP

SNMP (Simple Network Management Protocol)

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

The information on the properties of SNMPcompliant devices is entered in MIB files (MIB = Management Information Base).

Range of performance of the CP as an SNMP agent

The CP supports data queries over SNMP in the following versions:

- SNMPv1 (standard)
- SNMPv3 (Security)

It returns the contents of MIB objects of the standard MIB II according to RFC 1213 and the Siemens Automation MIB.

- **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 (IPv4 and IPv6)

  – ICMP

  – TCP

  – UDP

  – SNMP

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

  – Address Translation (AT)

  – EGP

  – Transmission

- **Siemens Automation MIB**

  The following exceptions / restrictions apply to the CP.

  Write access is permitted only for the following MIB objects of the system group:

  – sysContact

  – sysLocation

  – sysName

    A set sysName is sent as the host name using DHCP option 12 to the DHCP server to register with a DNS server.

  For all other MIB objects / MIB object groups, only read access is possible for security reasons.

Traps are not supported by the CP.

Access permissions using community name

The CP uses the following community names to control the access rights in the SNMP agent:

Table 5- 3 Access rights in the SNMP agent

Type of access	Community name *)
Read access	public
Read and write access	private

*) Note the use of lowercase letters!

5.11 STEP 7 configuration of individual parameters

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

Note

Information in STEP 7 and in the manual

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

5.11.1 Communication types and SNMP

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

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

"Communication types" parameter group

- **Enable telecontrol communication**

  Enables communication with a Telecontrol server on the CP.

- **Activate online functions**

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

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

- **Enabling S7 communication**

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

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

"SNMP" parameter group

- **Enable SNMP**

  Enables communication using SNMP on the CP.

  If security functions are enabled, you will find the entry in "Security".

5.11.2 Ethernet interface (X1) > Advanced options

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

The setting made here applies globally to all TCP connections of the CP.

Note the option of overwriting the value configured here for individual communications partners, refer to the section Partner stations (Page 51).

TCP connection monitoring time

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

Permitted range: 0 to 65535 s. Default: 180 s. If you enter 0 (zero), the function is deactivated.

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

TCP keepalive monitoring time

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

Permitted range: 0 to 65535 s. Default: 1 s. If you enter 0 (zero), the function is deactivated.

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

Ethernet interface (X1) > Advanced options > Transfer settings

Reconnection delay

Basic value for the wait time until the next connection establishment following an unsuccessful attempt to establish a connection. After every 3 attempts, the basic value is

doubled up to a maximum of 900 s. Example: The basic value 20 results in the following wait times: 3 x 20 s, 3 x 40 s, 3 x 80 s etc. up to max. 3 x 900 s. If a substitute Telecontrol server exists, the CP changes servers after every 3 attempts: At the 4th attempt, the CP tries to establish a connection with the substitute server. If the substitute server cannot be reached, at the 7th attempt, the CP tries to connect to the main server, etc.

Send timeout

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

Permitted range: 1 to 65535 s. Default: 5 s.

Watchdog cycle

Interval at which a watchdog frame is sent to the Telecontrol server.

Permitted range: 0 to 65535 s. Default: 30 s

Watchdog monitoring time

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

Permitted range: 0 to 65535 s. If you enter 0 (zero), the function is deactivated.

Key exchange interval

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

5.11.3 Partner stations

5.11.3.1 Partner stations > Telecontrol server

Partner stations > "Telecontrol server"

- **Partner number**

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

- **Master station address**

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

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

The TCP connection monitoring time is set for all TCP connections of the CP in the parameter group of the Ethernet interface, see also the section Ethernet interface (X1) > Advanced options (Page 50). These settings apply to all TCP connections of the CP.

- **Partner IP address**

  IP address of the communications partner

- **Connection monitoring**

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

  The TCP connection monitoring time is set for all TCP connections of the CP in the parameter group of the Ethernet interface, see also the section TCP connection monitoring (page 10). The setting applies to all TCP connections of the CP.

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

- **TCP connection monitoring time**

  Only with TCP: If there is no data traffic within the connection monitoring time, the CP sends a keepalive to the communications partner. Permitted range: 0 to 65535 s. Default: 180 s. If you enter 0 (zero), the function is deactivated.

  The monitoring time is configured for the Ethernet interface as the default for all TCP connections. The default value can be adapted individually for each connection in "Partner stations" and this overwrites the global value for this partner that was set in the parameter group "Ethernet interface (X1) > Advanced options > TCP connection monitoring".

- **TCP keepalive monitoring time**

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

- **Connection establishment**

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

- **Partner port**

  Number of the listener port of the communications partner.

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

- **Redundancy mode**

  Do not configure a second IP address if you want to set up the telecontrol server redundantly. You should also read the section "Addressing in the redundant TCSB system (Page 53)".

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

- **Partner monitoring time**

  If the CP does not receive a sign of life from the communications partner within the configured time, the CP interprets this as a fault/error on the partner. If you enter 0, the function is deactivated.

- **Report partner status**

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

  – Bit 0 of "PLC tag for partner status" (data type WORD) is set to 1 if the partner can be reached.

  – Bit 1 is set to 1 if all the paths to the remote partner are OK (useful with redundant paths).

  – Bit 2 indicates the status of the send buffer (frame memory).
  The following values are possible:

  - 0: send buffer OK

  - 1: send buffer threatening to overflow (more than 80 % full).

  - 3: send buffer has overflowed (fill level 100 % reached).

  As soon as the fill level drops below 50%, bit 3 is reset to 0.

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

5.11.3.2 Addressing in the redundant TCSB system

Addressing of the redundant telecontrol server

- **Addressing of the TCSB redundancy group by the stations using one IP address**

  In the LAN in the master station to which the TCSB server PCs and the DSL router (e.g. SCALANCE M) are connected, the Network Load Balancing (NLB) of the computer operating system will assign a common virtual IP address to the two server PCs.

  This IP address is configured depending on the network setup:

  – If only CP 1243-1 modules without a DSL router are connected, the virtual address assigned by the NLB must be configured in the CPs as the IP address of the telecontrol server.

  – If a SCALANCE M DSL router is used, only one IP address will be configured to address the redundant telecontrol server in the stations, the public address of the SCALANCE M.

    Set the port forwarding on the SCALANCE M so that the virtual IP address of the TCSB server PCs (internal network) is led to the public IP address (external network). Only the public IP address is reachable from the Internet. The station does not therefore receive any information telling it which of the two computers of the redundancy group it is connected to.

  You should not configure the second IP address for the redundant telecontrol server for the CPs in STEP 7 since a second IP address cannot be reached. If there are connection

problems, after 3 unsuccessful attempts, the CP would attempt to establish a connection to the unreachable substitute server because only the public IP address of the DSL router can be reached.

- **Addressing the TCSB redundancy group by OPC clients**

  The individual server PCs are addressed by the OPC clients directly using the computer name or the IP address of the server PCs; these are assigned to the server PCs when setting up the system. The virtual IP address assigned by the NLB is not used by the OPC clients.

  This means that an OPC client always connects to a defined server PC of the redundancy group.

- **Addressing the server PCs by client PCs**

  If you have connected other client PCs to the redundancy group to allow configuration of TCSB, the connection partner is specified by the configuration of TCM1 and TCM2 in the CMT of the client PCs.

5.11.3.3 Partner for inter-station communication

Inter-station communication

In this table, you specify the S7 stations with which the current station will use inter-station communication. Connections for inter-station communication run via the telecontrol server.

Partner

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

For inter-station communication, the partner is addressed with the parameters "Project", "Station" and "Slot".

Project

Here, enter the project number of the CP in the partner station. (Parameter group "Security > CP identification" on the partner)

Station

Here, enter the station number of the CP in the partner station. (Parameter group "Security > CP identification" on the partner)

Slot

Here, enter the slot number of the CP in the partner station via which the connection will be established.

Send buffer

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

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

Access ID

The access ID displayed here is formed from the hexadecimal values of project number, station number and slot.

5.11.4 Communication with the CPU

Communication with the CPU > "Data buffer size"

- **Data buffer size**

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

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

You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Ethernet interface (X1) > Advanced options (Page 50).

5.11.5 E-mail configuration

E-mail configuration

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

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

- Port no. 587

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

- Port no. 465587

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

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

5.11.6 Data point configuration

5.11.6.1 Configuring the data point names

Character set for data point names

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

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

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

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

5.11.6.2 Threshold value trigger and Analog value preprocessing

Sequence of processing Threshold value trigger and Analog value preprocessing

Note

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

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

This affects the value that is configured for the threshold value trigger, refer to the section Threshold value trigger (Page 60).

Restricted preprocessing options if mean value generation is configured

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

- Unipolar transfer
- Error suppression time
- Smoothing

No Threshold value trigger if Mean value generation is configured

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

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

Sequence of analog value processing

1. Reading the data from the input area of the CPU
2. Analog value preprocessing (part 1)

   Processing involves the following steps:

   – Mean value generation

   - Mean value generation configured: Calculation and then continued at point 4.

   - No mean value generation configured: Continue with "Unipolar transfer".

   – Unipolar transfer (if configured)

   – Error suppression time (if configured)

   – Smoothing (if configured)
3. Threshold value calculation (if Threshold value trigger is configured)
4. Analog value preprocessing (part 2)

   – Adjustment to the start of measuring range and end of measuring range (if configured)
5. Storage of the value in the send buffer

   Transfer of the value to the partner if trigger and threshold value conditions are met.

5.11.6.3 Analog value preprocessing

Depending on the data point type, the functions for analog value preprocessing described below are supported.

Unipolar transfer

If unipolar transfer is enabled, negative values of analog inputs are corrected to zero.

Exception: The value -32768 / 8000_h as fault ID for wire break of live zero hardware analog inputs is transferred. With a software input, on the other hand, all values lower than zero are corrected to zero.

If mean value generation is active, this parameter has no effect.

Smoothing factor

Analog values that fluctuate quickly can be smoothed with this function.

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

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

where
y_n = smoothed value in the current cycle
x_n = value acquired in the current cycle n
k = smoothing factor

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

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

If mean value generation is active, this parameter has no effect.

Error suppression time

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

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

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

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

If mean value generation is active, this parameter has no effect.

Recommendation for finished values that were preprocessed by the CPU:

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

Mean value generation

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

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

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

Overflow range / underflow range

Acquisition of a value in the overflow or underflow range results in the mean calculation being stopped immediately. The value 32767 / 7FFF$_h$ or -32768 / 8000$_h$ is saved as an

invalid mean value for the current mean value calculation period and sent when the next analog value frame is triggered. The calculation of a new mean value is then started. If the analog value remains in the overflow or underflow range, this new value is again saved immediately as an invalid mean value and sent when the next frame is triggered.

Note

Fault suppression time > 0 configured

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

Set start of measuring range / Set end of measuring range

In these two input boxes, you set a limit value at the start of the measuring range and at the end of the measuring range and if these limits are violated, the transfer of a frame is triggered. Configuration of a threshold value trigger is necessary for this function.

The range of the value that can be configured as a decimal number corresponds to the measuring range of the analog module (-32768 ... 32767).

By configuring these two values, you specify that the values of this analog value are transferred as a frame only in the following situations:

- When called by TCSB
- When the threshold value trigger fires
- When the value of "Set start of measuring range" is exceeded
- When the value of "Set end of measuring range" is undershot

The parameters "Set start of measuring range" and Set end of measuring range" are pointless for measured values that have already been preprocessed in the CPU.

Note

Evaluation of the value even when the option is disabled

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

To disable the two options, delete the previously configured values "Start of measuring range" or "End of measuring range" from the input boxes and then disable the relevant option.

Recommendation for quickly fluctuating analog values:

If the analog value fluctuates quickly, it may be useful to smooth the analog value first if the "Set start of measuring range" and "Set end of measuring range" parameters are enabled. This avoids a frame being sent every time a limit value is violated if the analog value fluctuates close to one of the two limit values for a longer period of time.

5.11.6.4 Threshold value trigger

The CP calculates the value for the threshold value trigger after the analog value preprocessing, refer to the section Threshold value trigger and Analog value preprocessing (Page 56).

Threshold value trigger: How the integrattion calculation works

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

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

The calculation cycle

The integration threshold value calculation works with a cyclic comparison of the integrated current value with the last stored value. The calculation cycle in which the two values are compared is 500 milliseconds.
(Note: The calculation cycle must not be confused with the scan cycle of the CPU memory areas).

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

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

Table 5- 4 Example of the integration calculation of a threshold value configured with 2.0

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

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

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

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

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

5.11.6.5 Partner stations: Configuring the inter-station communication

Telecontrol server activated

If no partner was enabled for inter-station communication, the "Telecontrol server activated" option is selected automatically.

If the value of the data point is to be sent to an S7 station, select the option "Partner for inter-station communication".

The telecontrol server and an S7 station cannot be selected as the partner for a data point at the same time.

Enable partner for inter-station communication

If the value of the data point is to be sent to an S7 station, select the option "Partner for inter-station communication".

The telecontrol server and an S7 station cannot be selected as the partner for a data point at the same time.

Partner number for inter-station communication:

Here, select the partner for inter-station communication based on the access ID of the CP in the S7 station. You will find the access ID for the CP of the partner station in the "Security > CP identification" parameter group.

Data point index

data point index of the sending and receiving CP.

Note

The data pair of the sending and receiving CP must have an identical data point index. A receiving data point of CP 2 corresponds to a sending data point of CP 1 with the same data point index.

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

5.11.7 Configuring messages

Configuring e-mails

If important events occur, the CP can send e-mails to a communications partner.

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

Project > directory of the relevant station > Local modules > CP 1243-1

For the view in STEP 7, refer to the section Configuring the data points (Page 33).

Requirements and necessary information

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

- Enabling telecontrol communication ("Communication types") parameter group
- Configuring the "E-mail configuration" parameter group

  To do this, you require the following information:

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

  – Email address of the recipient

Triggering e-mail transfer

One of the following events triggers sending of the e-mail:

- CPU changes to STOP.
- CPU changes to RUN.
- The connection to the partner is interrupted.
- The connection to the partner is re-established.
- A trigger signal is fired.

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

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

Enable status identifier / External status

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

The meaning of the statuses returned in hexadecimal format is as follows:

Table 5- 5 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.
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): • Recipient address ("To" or "Cc").

Status	Meaning
8502	Syntax error. Check the following configuration data: Alarm configuration > E-mail data (Content): • Email address (sender)
8535	SMTP authentication incomplete. Check the "User name" and "Password" parameters in the CP configuration.
8550	SMTP server cannot be reached. You have no access rights. Check the following configuration data: • CP configuration > E-mail configuration: – User name – Password – Email address (sender) • Alarm configuration > E-mail data (Content): – 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.

Diagnostics and upkeep

6

6.1 Diagnostics options

The following diagnostics options are available.

LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 20).

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

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

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

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

Using the online functions, you can read diagnostics information from the CP from an engineering station on which the project with the CP is stored. You obtain the following static information on the selected module:

- General information on the module
- Diagnostics status
- Information on the Ethernet interface:
  - Network
  - Ethernet interface
  - Statistics

If you want to operate online diagnostics with the station via the CP, you need to select Activate online functions, see section Communication types and SNMP (Page 49).

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

6.2 Downloading firmware

New firmware versions of the CP

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

68853485 (http://support.automation.siemens.com/WW/view/en/68853485)

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

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

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

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

The last two methods are described below.

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

Requirements:

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

Procedure:

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

   Both methods are possible.
7. Connect using the "Connect" button.

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

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

Downloading the firmware via the Web server of the CPU

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

Requirements in the CPU configuration

1. Open the corresponding project on the engineering station.
2. Select the CPU of the station involved in STEP 7.

3. Select the "Web server" entry.
4. In the parameter group "General", select the "Enable Web server for this interface" option.
5. With a CPU version V4.0 or higher, create a user in the user management with the name "admin".

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

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

- **Connection establishment with HTTP**

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

- **Connection establishment with HTTPS**

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

These two variants are described in the following sections.

Requirement: The new firmware file is stored on your engineering station.

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

Connection establishment with HTTP

1. Connect the PC on which the new firmware file is located to the CPU via the Ethernet interface.
2. Enter the address of the CPU in the address box of your Web browser: **http**://<IP address>
3. Press the Enter key.

   The start page of the Web server opens.
4. Click on the "Download certificate" entry at the top right of the window.

   The "Certificate" dialog opens.
5. Download the certificate to your PC by clicking the "Install certificate ..." button.

   The certificate is loaded on your PC.

   You will find information on downloading a certificate in the help of your Web browser and in the STEP 7 information system under the key words "HTTPS" or "Access for HTTPS (S7-1200)".
6. When the connection has changed to the secure mode HTTPS ("**https**://<IP address>/..." in the address box of the Web server), you can continue as described in the next section "Downloading firmware".

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

Connection establishment with HTTPS

1. Connect the PC on which the new firmware file is located to the CPU via the Ethernet interface.
2. Enter the address of the CPU in the address box of your Web browser: **http**s://<IP address>
3. Press the Enter key.

   The start page of the Web server opens.
4. Continue as described in the following section "Downloading firmware".

Loading firmware

1. Log in on the start page of the Web server as an administrator.
   - User name: admin
   - Password: No password necessary
2. After logging in, select the entry "Module status" in the navigation panel of the Web server.
3. Select the CP in the module list.
4. Select the "Firmware" tab lower down in the window.
5. Browse for the firmware file on your PC using the "Browse..." button and download the file to the station using the "Run update" button.

6.3 Module replacement

Module replacement

⚠ 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.

Technical data

7

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	• 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	• 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	• 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 ℃ to +70 ℃
	During transportation	-40 ℃ to +70 ℃
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation

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 **	

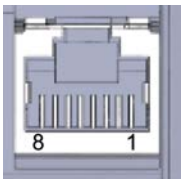
***** For details, refer to the IK PI catalog, cabling technology
******You will find further characteristics and performance data in the section Application and properties (Page 9).

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

A

Current approvals on the Internet

You will also find the current approvals for the product on the Internet pages of Siemens Automation Customer Support under the following entry ID:

68853485 (http://support.automation.siemens.com/WW/view/en/68853485)
→ "Entry list" tab, entry type "Certificates"

Other approvals

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

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

45605894 (http://support.automation.siemens.com/WW/view/en/45605894)

Under this entry, go to the relevant product and select the following settings: "Entry list" tab > entry type "Certificates".

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

CE

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

- EC directive 2006/95/EEC "Electrical Equipment Designed for Use within Certain Voltage Limits" (Low Voltage Equipment Directive)
- EN 60950-1 Information Technology Equipment - Safety

- EC Directive 2004/108/EC "Electromagnetic Compatibility" (EMC Directive)
  - Emission
    EN 61000-6-4:2007: Industrial area
  - Immunity
    EN 61000-6-2:2005: Industrial area

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

Siemens Aktiengesellschaft
Industry Automation
Industrielle Kommunikation SIMATIC NET
Postfach 4848
D-90327 Nürnberg
Germany

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

68853485 (http://support.automation.siemens.com/WW/view/en/68853485) → tab "Entry list"

Filter settings:
Entry type: "Certificates"
Certificate Type: "Declaration of Conformity"
Search items(s): <name of the module>

ATEX

ATEX approval: II 3 G Ex nA IIC T4 Gc

Relevant standards:

- EN 60079-0:2006: Potentially explosive atmosphere - general requirements
- EN 60079-15:2005: Electrical apparatus for explosive gas atmospheres; type of protection 'n'

The device is suitable for use in environments with pollution degree 2.

The device is suitable for use only in environments that meet the following conditions:

- Class I, Division 2, Group A, B, C, D and areas where there is no risk of explosion
- Class I, Zone 2, Group IIC and areas where there is no risk of explosion

WARNING

Installation guidelines

The product meets the requirements if you keep to the following during installation and operation:

- The notes in the section Important notes on using the device (Page 25)
- The installation instructions in the document /1/ (Page 77)

Over and above this, the following conditions must be met for the safe deployment of the CP:

- Install the modules in a suitable enclosure with degree of protection of at least IP54 to EN 60529 and take into account the environmental conditions for operation of the devices.
- If the rated temperatures of 70°C at the cable entry or 80°C at the branching point of the wires are exceeded, the permitted temperature range of the selected cable must be suitable for the actual measured temperatures.
- Measures must be taken to prevent the rated voltage being exceeded by more than 40% due to transient disturbances.

cULus HAZ.LOC.

Underwriters Laboratories Inc. meets

- Underwriters Laboratories, Inc.: UL 508 Listed (industrial control devices)
- UL 1604 (Hazardous Location)
- Canadian Standards Association: CSA C22.2 No 142 (process control equipment)
- CSA C22.2 No. 213 (Hazardous Location)

APPROVED for Use in:

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

FM

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

C-Tick

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

Dimension drawings

B

Note

All dimensions in the drawings are in millimeters.

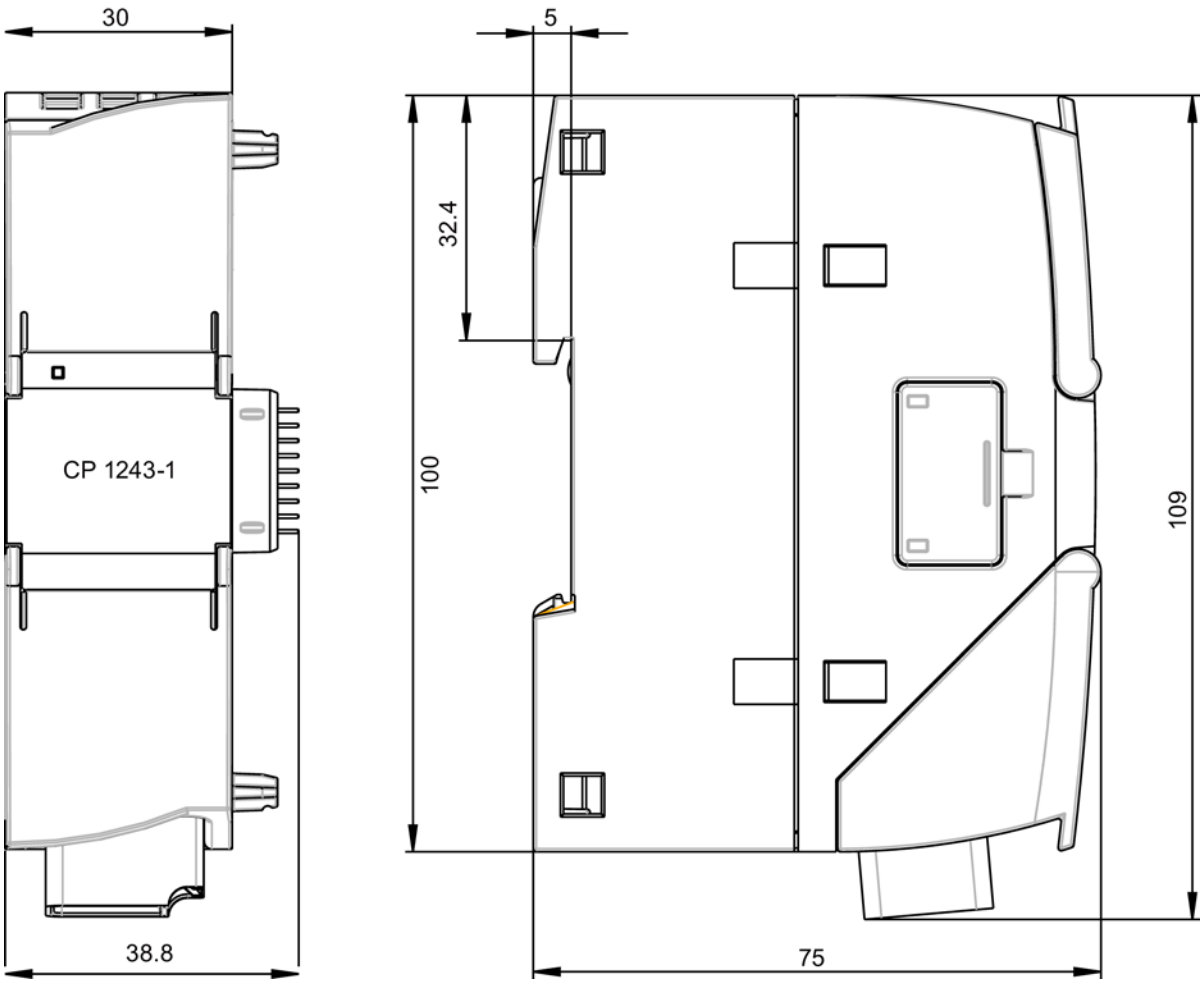


Figure B-1 CP 1243-1 DNP3 / CP 1243-1 IEC: Front view and side view left

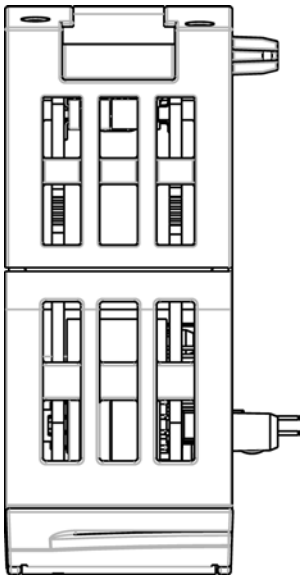


Figure B-2 CP 1243-1 DNP3 / CP 1243-1 IEC: View from above

Documentation references

C

Where to find Siemens documentation

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

  You can request the catalogs and additional information from your Siemens representative.
- You will find SIMATIC NET manuals on the Internet pages of Siemens Automation Customer Support:

  Link to Customer Support (http://support.automation.siemens.com/WW/view/en)

  Enter the entry ID of the relevant manual as the search item. The ID is listed below some of the reference entries in brackets.

  As an alternative, you will find the SIMATIC NET documentation on the pages of Product Support:

  10805878 (http://support.automation.siemens.com/WW/view/en/10805878)

  Go to the required product group and make the following settings:

  "Entry list" tab, Entry type "Manuals / Operating Instructions"
- You will find the documentation for the SIMATIC NET products relevant here on the data medium that ships with some products:
  - Product CD / product DVD or
  - SIMATIC NET Manual Collection

/1/

SIMATIC
S7-1200 Programmable Controller
System Manual
Siemens AG
order number: 6ES7298-8FA30-8BH0
Current issue under the following entry ID:
34612486 (http://support.automation.siemens.com/WW/view/en/34612486)

/2/

SIMATIC NET
CP 1243-1
Operating Instructions
Siemens AG
entry ID: 89332514 (http://support.automation.siemens.com/WW/view/en/89332514)

/3/

SIMATIC NET
TELECONTROL SERVER BASIC (Version V3)
Operating Instructions
Siemens AG
entry ID: 46635999 (http://support.automation.siemens.com/WW/view/en/46635999)

/4/

SIMATIC NET
Industrial Ethernet Security
Basics and Application
configuration manual
Siemens AG
Entry ID: 18701555 (http://support.automation.siemens.com/WW/view/en/18701555)

Index

S

T

V

W