SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-1

Operating Instructions

Preface

Application and properties 1

LEDs and connectors 2

Installation, connecting up, commissioning 3

Configuration 4

Program blocks 5

Diagnostics and upkeep 6

Technical data 7

Approvals A

Dimension drawings B

Documentation references C

04/2017

C79000-G8976-C365-03

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

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

C79000-G8976-C365-03
Ⓟ 05/2017 Subject to change

Preface

Validity of this manual

This document contains information on the following telecontrol product:

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

  The CP 1243-1 is the communications processor for connecting the SIMATIC S7-1200 to control center systems via the public infrastructure (e.g. DSL).

  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 / submodule / module**

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

- **TCSB**

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

- **STEP 7**

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

- **ES**

  PC with the STEP 7 project

Purpose of the manual

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

New in this issue

- New hardware product version 2
- New functions in the firmware version named above include:
  - Expansion of the telecontrol protocols DNP3 and IEC
  - Sending messages even without telecontrol communicaton
  - Changed behavior during time-of-day synchronization, see section Time-of-day synchronization (Page 42).
  - Expansion of the supported data types, refer to the section Datapoint types (Page 89).
- Functional improvement of data point configuration as of STEP 7 V14 SP1. see section Data point configuration (Page 82).
- Editorial revision

Replaced manual issue

Edition 12/2016

Current manual release on the Internet

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

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

Required experience

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

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

Cross references

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

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

Sources of information and other documentation

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

License conditions

Note

Open source software

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

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

- OSS-CP1243-1_86.pdf

Firmware

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

Security information

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

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

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

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

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

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

SIMATIC NET glossary

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

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

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

Recycling and disposal

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

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

Keep to the local regulations.

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

Training, Service & Support

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

Table of contents

Preface 3

1 Application and properties 11

1.1 Properties of the CP 11

1.2 Communications services 11

1.3 Other services and properties 12

1.4 Security functions 13

1.5 Configuration limits and performance data 15

1.6 Configuration examples 17
1.6.1 Sending e-mails 17
1.6.2 TeleControl Basic 18
1.6.3 DNP3 / IEC 20
1.6.3.1 Configuration with 1 subnet 20
1.6.3.2 Configuration with connections over the Internet 21
1.6.3.3 Configuration with a redundant control center 22

1.7 Requirements for use 23
1.7.1 Hardware requirements 23
1.7.2 Software requirements 23

2 LEDs and connectors 25

2.1 Opening the covers of the housing 25

2.2 LEDs 26

2.3 Electrical connectors 30
2.3.1 Power supply 30
2.3.2 Ethernet interface X1P1 30

3 Installation, connecting up, commissioning 31

3.1 Important notes on using the device 31
3.1.1 Notices on use in hazardous areas 31
3.1.2 Notices on use in hazardous areas according to IECEx / ATEX 32
3.1.3 Notices regarding use in hazardous areas according to UL HazLoc 33
3.1.4 Notices on use in hazardous areas according to FM 33

3.2 Installing, connecting up and commissioning 34

3.3 Note on operation 36

4 Configuration 37

4.1 Security recommendations 37

4.2 Configuration in STEP 7 40

4.3 Addressing and authentication 41
4.3.1 TeleControl Basic 41

4.3.2 DNP3 / IEC ... 41

4.4 Time-of-day synchronization ... 42

4.5 Communication types ... 45

4.6 Ethernet interface ... 46
4.6.1 CP identification ... 46
4.6.2 Time-of-day synchronization ... 46
4.6.3 Advanced options ... 47
4.6.4 Transmission settings – TeleControl Basic ... 48
4.6.5 Transmission settings – DNP3 ... 49
4.6.6 Transmission settings - IEC ... 51

4.7 SNMP ... 53

4.8 Partner stations ... 54
4.8.1 Partner stations > General parameters ... 54
4.8.2 TeleControl Basic ... 57
4.8.2.1 Addressing in the redundant TCSB system ... 57
4.8.2.2 Advanced settings ... 58
4.8.2.3 Partner for inter-station communication ... 58
4.8.3 DNP3 / IEC ... 59
4.8.3.1 Advanced settings (DNP3 / IEC) ... 59

4.9 Security ... 63
4.9.1 Parameter overview ... 63
4.9.2 CP iIdentifcation with the TeleControl Basic protocol ... 64
4.9.3 DNP3 security options ... 65
4.9.4 Firewall ... 67
4.9.4.1 Pre-check of messages by the MAC firewall. ... 67
4.9.4.2 Notation for the source IP address (advanced firewall mode) ... 68
4.9.4.3 Firewall settings for configured connection connections via a VPN tunnel ... 68
4.9.4.4 Settings for online security diagnostics and downloading to station with the firewall activated ... 68
4.9.5 E-mail configuration ... 69
4.9.6 Log settings - Filtering of the system events ... 70
4.9.7 SNMP ... 70
4.9.8 Certificate manager ... 72
4.9.9 Handling certificates ... 72
4.9.10 VPN ... 74
4.9.10.1 VPN (Virtual Private Network) ... 74
4.9.10.2 Creating a VPN tunnel for S7 communication between stations ... 76
4.9.10.3 VPN communication with SOFTNET Security Client (engineering station) ... 78
4.9.10.4 Creating the VPN connection telecontrol server ... 79
4.9.10.5 Establishment of VPN tunnel communication between the CP and SCALANCE M ... 79
4.9.10.6 CP as passive subscriber of VPN connections ... 79
4.9.10.7 SYSLOG ... 80
4.9.11 Configuration of the TeleService access ... 80

4.10 Data points ... 82
4.10.1 Data point configuration ... 82
4.10.2 Syntax of the data point names ... 88
4.10.3 Datapoint types ... 89
4.10.4 Configuration of the data point index ... 94
4.10.5 Status IDs of the data points ... 95

4.10.6 Read cycle 96
4.10.7 Process image, type of transmission, event classes, triggers 97
4.10.8 "Trigger“ tab 100
4.10.9 Threshold value trigger 101
4.10.10 Analog value preprocessing 103
4.10.11 Command outputs....109
4.10.12 Partner stations....112
4.10.12.1 Partner configuration for DNP3 and IEC data points....112
4.10.12.2 Partner configuration with TeleControl Basic data points. 112
4.11 Messages....113
4.12 Access to the Web server....115
5 Program blocks 117
5.1 Program blocks for OUC....117
5.2 Changing the IP address during runtime 119
6 Diagnostics and upkeep 121
6.1 Diagnostics options....121
6.2 Online security diagnostics via port 8448 123
6.3 Online functions and TeleService 123
6.4 SNMP....125
6.5 Processing status of e-mails....126
6.6 Downloading firmware 129
6.7 Module replacement 132
7 Technical data 133
7.1 Technical specifications of the CP 1243-1....133
7.2 Pinout of the Ethernet interface 134
A Approvals.... 135
B Dimension drawings.... 139
C Documentation references 141
Index.... 143

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 the following control center systems:

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

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 attachment to the control center systems named above. The CP can communicate with redundant control systems.

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

  You will find the usable security functions in the section Security functions (Page 13).

- **Messages / e-mail**

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

  You will find the requirements and functions in the section E-mail configuration (Page 69).

- **S7 communication and PG/OP communication with the following functions:**
  - PUT/GET as client and server for data exchange with S7 stations
  - 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**
  - IPv4 / IPv6

    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**

  The CP supports various methods of time-of-day synchronization. You will find information in the section Time-of-day synchronization (Page 42).

  For information on the format of the time stamp, refer to the section Datapoint types (Page 89).

- **Storage of events**

  The CP can store events of different classes chronologically and transfer them spontaneously or together to the telecontrol server.

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

  The telecontrol communication with the communications partner is triggered in two ways:
  - After a request by the master or an OPC client connected to TCSB
  - Unsolicited, triggered by various selectable criteria

- **Analog value processing**

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

- **Online functions / TeleService**

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

  The following online functions are available:

  – Downloading project or program data from the STEP 7 project to the station

  – Querying diagnostics data on the station

  – Downloading firmware files to the CP

  For information on the online functions, refer to the section Online functions and TeleService (Page 123).

- **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 125).

1.4 Security functions

Industrial Ethernet Security

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

- Data espionage
- Data manipulation
- Unauthorized access

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

The security functions can be used independently of telecontrol communication.

Security functions of the telecontrol protocols

- TeleControl Basic
  - Encrypted telecontrol communication

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

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

    To authenticate the CP with the telecontrol server
- DNP3

  The security functions specific to DNP3 can be used.
- IEC 60870-5

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

Further configurable security functions of the CP

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

- Firewall
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Firewall also for "non-IP" Ethernet frames according to IEEE 802.3 (layer 2)
  - Limitation of the transmission speed ("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.
- STARTTLS / SMTPS

  For the secure transfer of e-mails
- NTP (secure)

  For secure transfer during time-of-day synchronization

- **SNMPv3**

  For secure transmission of network analysis information safe from eavesdropping

- **Protection for devices and network segments**

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

Note

Plants with security requirements - recommendation

Use the following options:

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

See also section Security recommendations (Page 37).

For configuring the security functions refer to the section Security (Page 63).

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 142).

1.5 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.

Connection resources

- **Telecontrol connections**

  With the various telecontrol protocols the CP can establish connections to the following master station types:

  – To non-redundant or redundant telecontrol servers (TCSB).

  – To up to four non-redundant or redundant DNP3 masters

  – To up to four non-redundant or redundant IEC masters

  With the Telecontrol Basic protocol, in addition to this, inter-station communication with up to 15 S7 stations with a CP 1243-1 can be operated via the telecontrol server.

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

  Max. 14 connection resources, can be distributed as required for:

  – S7 connections (PUT/GET)

  – Connections via program blocks (OUC) to S7 stations
- **Online functions**

  1 connection resource is reserved for online functions.
- **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 89).

Frame memory (send buffer)

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

The send buffer has a maximum size of 64000 events divided into equal parts for all configured communications partners. The size of the frame memory can be set in STEP 7, refer to the section SNMP (Page 53).

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

Messages (e-mail)

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

IPsec tunnel (VPN)

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

Firewall rules

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

The firewall rules are divided up as follows:

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

1.6 Configuration examples

1.6.1 Sending e-mails

Configuration with sending of e-mails:

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

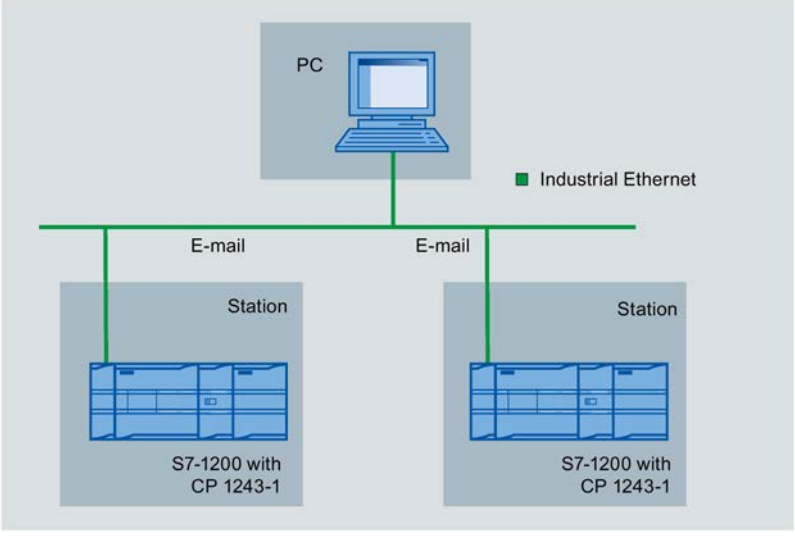


Figure 1-1 Sending e-mails

1.6.2 TeleControl Basic

Telecontrol with a non-redundant master station (TCSB)

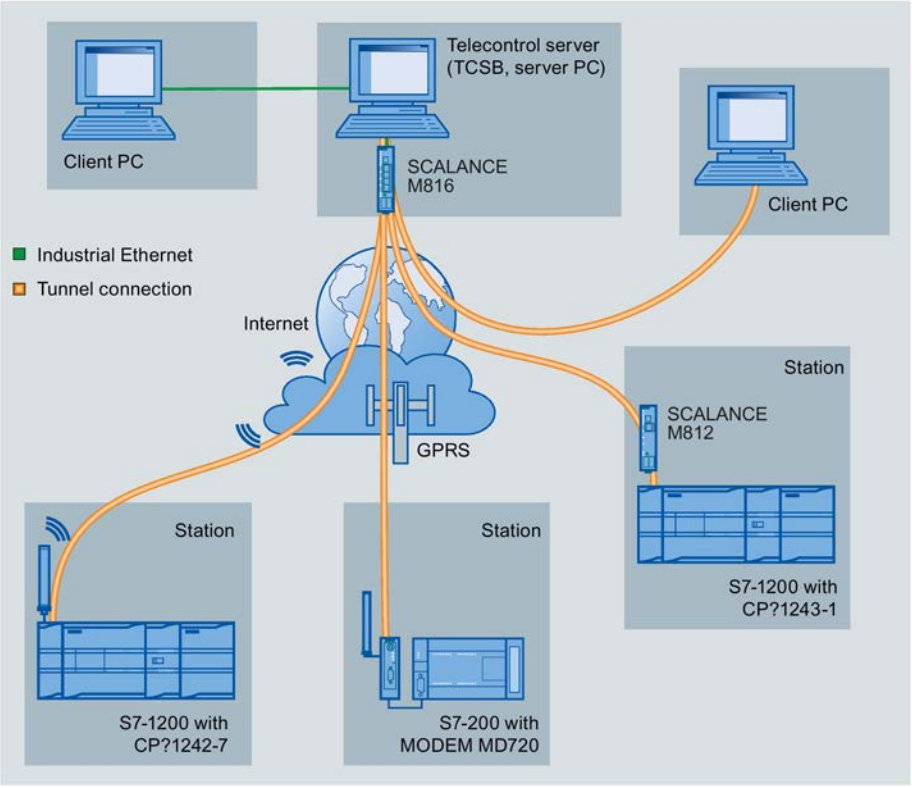


Figure 1-2 **Communication between S7 stations and a master station (TCSB)**

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).

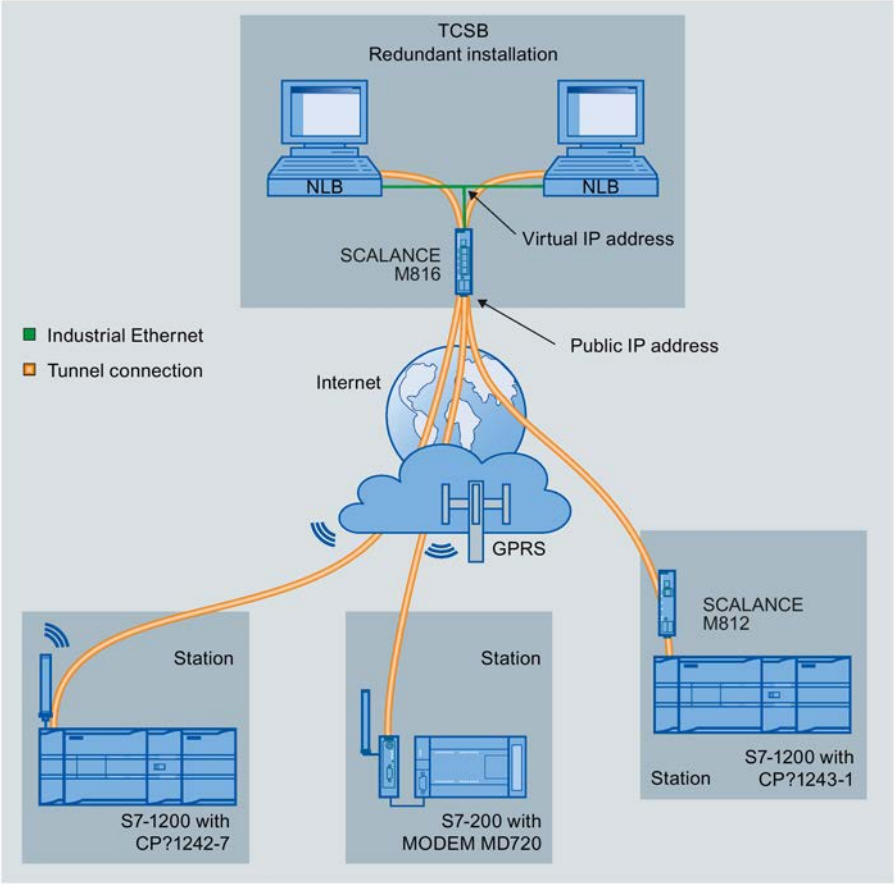


Figure 1-3 **S7 station communication with a redundant a master station**

1.6.3 DNP3 / IEC

1.6.3.1 Configuration with 1 subnet

Configuration example with a non-redundant control center

The following example describes a configuration with a non-redundant control center in which all nodes are located in 1 IP subnet.

In this example, the DNP3 protocol is used; in other words, the stations are equipped with a CP 1243-1.

A configuration in which the IEC protocol is used would have the same setup.

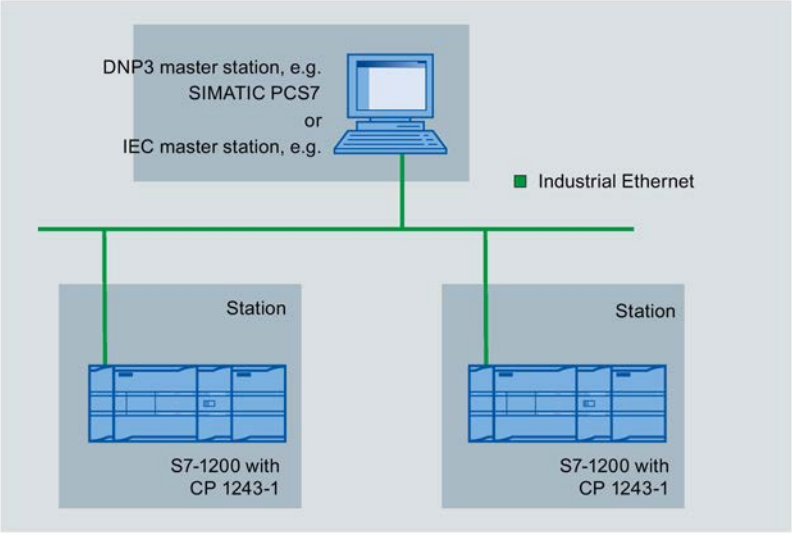


Figure 1-4 Configuration example with a non-redundant control center and stations in one IP subnet

The S7-1200 stations are connected to the Internet via the CP and connected to the control center.

When using the DNP3 protocol, for example, SIMATIC PCS 7 TeleControl or the system of a third-party provider can be used as the control center. If you use SIMATIC PCS 7 TeleControl as the DPN3 master in the control center, you require the necessary DPN3 driver.

1.6.3.2 Configuration with connections over the Internet

Configuration example with connections over the Internet

The following example contains a configuration with a non-redundant control center.

In this example, the DNP3 protocol is used. A configuration in which the IEC protocol is used would have the same setup.

The S7-1200 stations are connected to the Internet via the CP and connected to the control center.

When using the DNP3 protocol, for example, SIMATIC PCS 7 TeleControl or the system of a third-party provider can be used as the control center. If you use SIMATIC PCS 7 TeleControl as the DPN3 master in the control center, you require the necessary DPN3 driver.

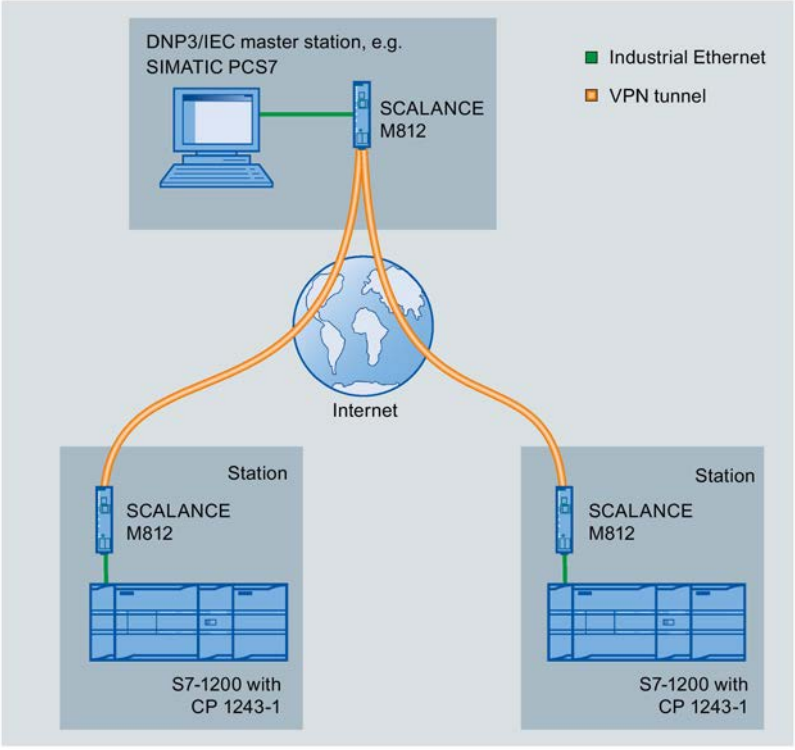


Figure 1-5 Configuration example with connections over the Internet

As an alternative to the router SCALANCE 812, you can also use a standard DSL modem and establish the VPN connection with a security module SCALANCE S.

Addressing

Refer to the information in the section DNP3 / IEC (Page 41).

1.6.3.3 Configuration with a redundant control center

Configuration example with a redundant control center

The following example contains a configuration with a redundant control center and connections via the Internet.

In this example, the DNP3 protocol is used. A configuration in which the IEC protocol is used would have the same setup.

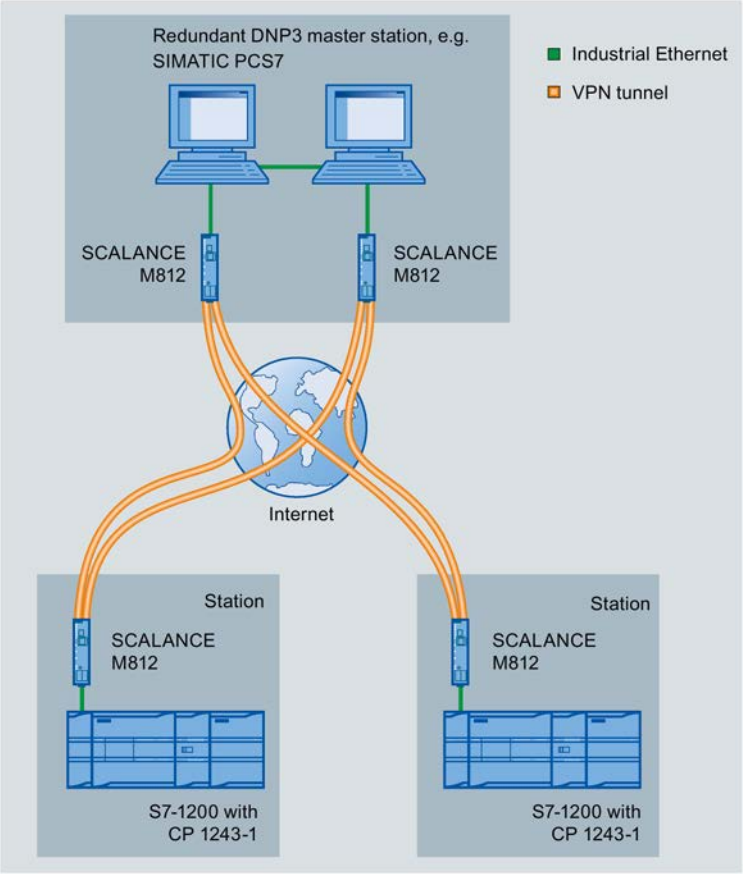


Figure 1-6 Configuration example with a redundant DNP3 master station

Addressing of the redundant DNP3 master

The two devices of the redundant DNP3 master in the control center are addressed by the CP using one DNP3 address but two different IP addresses.

1.7 Requirements for use

1.7.1 Hardware requirements

The following description relates to a configuration with telecontrol communication.

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 a control center

In the S7-1200 station:

- CPU with firmware version as of V3

  The full functionality of the CP is only available with a CPU as of V4.2.
- DSL router SCALANCE M812

In the master station:

- PC with control center application (alternative):
  - TCSB (version V3)

    For more detailed information on the structure of TCSB , refer to the section /3/ (Page 142).
  - DNP3 master
  - IEC master
- DSL router SCALANCE M812
- When using online functions: Engineering station with STEP 7 (refer to the section Software requirements (Page 23)).

For the configuration of the S7 station with CP:

Engineering station with STEP 7

1.7.2 Software requirements

Software for configuration and online functions

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

- STEP 7 Basic / Professional V14.0 SP1

LEDs and connectors

2

2.1 Opening the covers of the housing

Location of the display elements and the electrical connectors

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

The Ethernet connector is located behind the lower hinged cover of the module.

Opening the covers of the housing

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

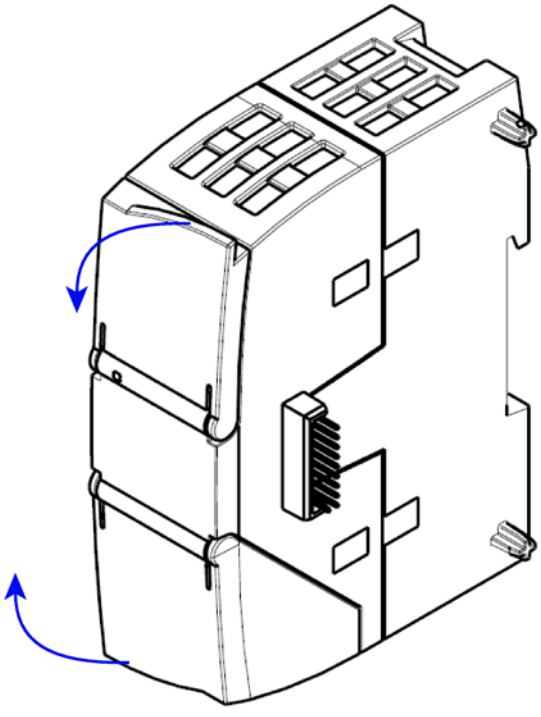


Figure 2-1 Opening the covers of the housing

2.2 LEDs

LEDs of the module

The module has various LEDs for displaying the status:

- **LED on the front panel**

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

- **LEDs below the upper cover of the housing**

  The LEDs below the upper cover provide more detailed information on the module status.

Table 2- 1 **LED on the front panel**

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

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

LED (color)	Name	Meaning
(green)	LINK	Status of the connection to Industrial Ethernet
(green)	CONNECT	Status of the connections to the communications partner
(green)	VPN	Status of the VPN configuration
(green)	SERVICE	Status of a connection for online functions

LED colors and illustration of the LED statuses

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

Table 2- 3 **Meaning of the LED symbols**

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

Note

LED colors when the module starts up

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

Display of the basic statuses of the CP ("DIAG" LED)

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

DIAG (red / green)	Meaning (if more than one point listed: alternative meaning)
Basic statuses of the CP	
	• 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 2- 5 Display of the operating and communications statuses

DIAG (red / green)	-	LINK (green)	CONNECT (green)	VPN (green)	SERVICE (green)	Meaning (if more than one point listed: alternative meaning)
Module startup (STOP → RUN) or error statuses						
○		○	○	○	○	Power OFF
● red		●	●	●	●	Startup - phase 1
☼ flashing red		-	○	○	○	Startup - phase 2
● green		-	-	-	-	Running (RUN) without serious error
○			●	●	●	Incorrect startup
● red		-	☼	-	-	Invalid STEP 7 project data
☼ flashing red		-	○	-	-	Missing STEP 7 project data
☼ flashing red		●	☼	-	-	Backplane bus error
Connection to Industrial Ethernet						
-		●	-	-	-	Connection to Industrial Ethernet exists
● green		☼	-	-	-	• Connection to Industrial Ethernet being established. • IP address being obtained.
-		○	-	-	-	No connection to Industrial Ethernet
Connection to communications partners						
● green		●	●	-	-	Connection established to at least one partner
● green		●	☼	-	-	Partner reachable, CPU in STOP mode
☼ flashing green		●	○	-	-	Partner not reachable

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

2.3 Electrical connectors

2.3.1 Power supply

Power supply

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

2.3.2 Ethernet interface X1P1

Ethernet interface

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

The pin assignment and other data relating to the Ethernet interface can be found in the section Technical data (Page 133).

Installation, connecting up, commissioning 3

3.1 Important notes on using the device

Safety notices on the use of the device

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

Overvoltage protection

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

3.1.1 Notices on use in hazardous areas

⚠ WARNING
EXPLOSION HAZARD DO NOT OPEN WHEN ENERGIZED.

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

WARNING

The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS).

This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the equipment power supply must comply with NEC Class 2, as described by the National Electrical Code (r) (ANSI / NFPA 70).

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

WARNING

EXPLOSION HAZARD

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

WARNING

EXPLOSION HAZARD

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

WARNING

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

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

WARNING

Requirements for the cabinet/enclosure

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

WARNING

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

WARNING

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

3.1.3 Notices regarding use in hazardous areas according to UL HazLoc

WARNING

EXPLOSION HAZARD

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

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

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

3.1.4 Notices on use in hazardous areas according to FM

WARNING

EXPLOSION HAZARD

Do not connect or disconnect while the circuit is live or unless the area is known to be free of ignitible concentrations.

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

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

WARNING

EXPLOSION HAZARD

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

3.2 Installing, connecting up and commissioning

Prior to installation and commissioning

⚠ CAUTION
Read the system manual "S7-1200 Programmable Controller" Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller", refer to the documentation in the Appendix. When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".

Pulling/plugging the module

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

Dimensions for installation

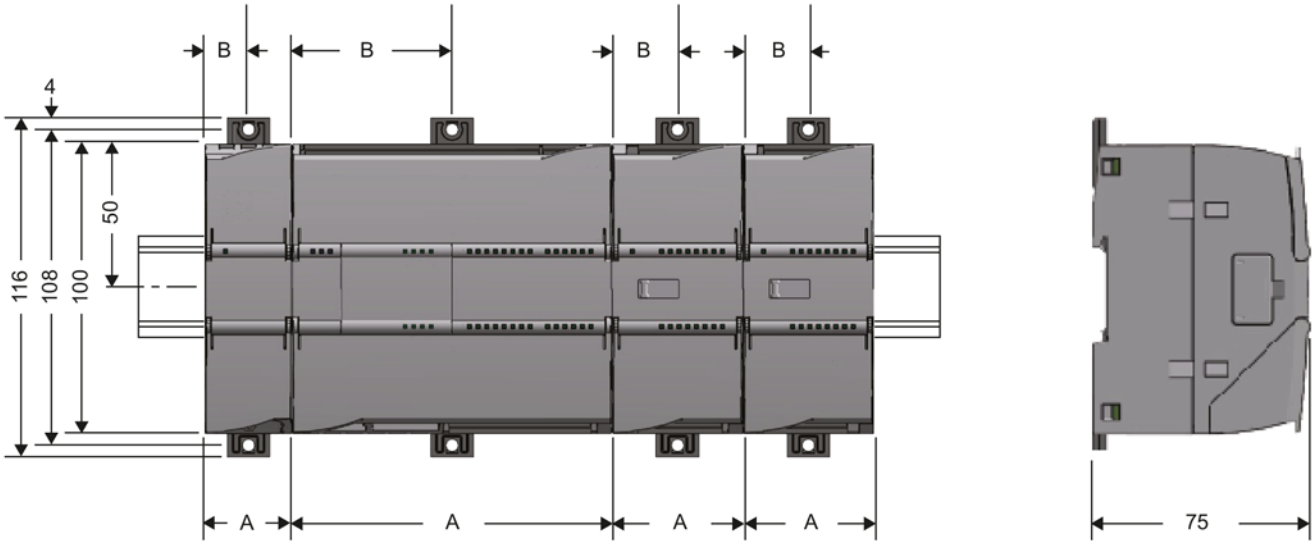


Figure 3-1 Dimensions for installation of the S7-1200

Table 3- 1 Dimensions for installation (mm)

S7-1200 devices		Width A	Width B *
CPU (examples)	CPU 1211C, CPU 1212C	90 mm	45 mm
	CPU 1214C	110 mm	55 mm
Communications interfaces (examples)	CM 1241, CM 1243-5, CM 1242-5	30 mm	15 mm
	CP 1242-7, CP 1243-1, CP 1243-7, CP 1243-8 IRC	30 mm	15 mm

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

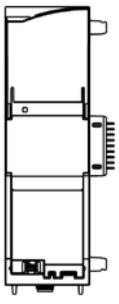
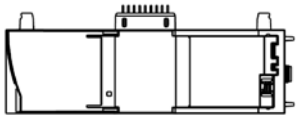
You will find detailed dimensions of the module in the section Dimension drawings (Page 139).

DIN rail clamps, control panel installation

All CPUs, SMs, CMs and CPs can be installed on the 35 mm DIN rail in the cabinet. Use the pull-out DIN rail mounting clips to secure the device to the rail. These mounting clips also lock into place when they are extended to allow the device to be installed in a switching panel. The inner dimension of the hole for the DIN rail mounting clips is 4.3 mm.

Installation location

NOTICE
Installation location The module must be installed so that its upper and lower ventilation slits are not covered, allowing adequate ventilation. Above and below the device, there must be a clearance of 25 mm to allow air to circulate and prevent overheating. Remember that the permitted temperature ranges depend on the position of the installed device. You will find the permitted temperature ranges in the section Technical specifications of the CP 1243-1 (Page 133).

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

Requirement: Configuration prior to commissioning

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

Installing, connecting up and commissioning the module

Note

Connection with power off

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

Table 3- 2 Procedure for installation and connecting up

Step	What to do	Notes and explanations
1	Mount the CP on the DIN rail and connect it to the module to its right.	Use a 35 mm DIN rail. The slots to the left of the CPU are permitted.
2	Secure the DIN rail.	
3	Connect the Ethernet cable to the CP.	You will find the pinout of the interface in the section Technical data (Page 133).
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.	

3.3 Note on operation

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

Configuration 4

4.1 Security recommendations

Keep to the following Security recommendations to prevent unauthorized access to the system.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
- Check regularly for new features on the Siemens Internet pages.
  - Here you will find information on network security:

    Link: (http://www.siemens.com/industrialsecurity)
  - Here you will find information on Industrial Ethernet security:

    Link: (http://w3.siemens.com/mcms/industrial-communication/en/ie/industrial-ethernet-security/Seiten/industrial-security.aspx)
  - You will find an introduction to the topic of industrial security in the following publication:

    Link: (http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP02-0BA4_BR_Network_Security_en_112015.pdf)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the PC directly to the Internet. If a connection from the CP to the Internet is required, arrange for suitable protection before the CP, for example a SCALANCE S with firewall or use the CP 1543SP-1.

Security functions of the product

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

- Protection levels

  Configure a protection level of the CPU.

  You will find information on this in the information system of STEP 7.

- Security function of the communication
  - Enable the security functions of the CP and set up the firewall.

    If you connect to public networks, you should use the firewall. Think about the services you want to allow access to the station via public networks. By using the "bandwidth limitation" of the firewall, you can restrict the possibility of flooding and DoS attacks.
  - Use the secure protocol variants NTP (secure) and SNMPv3.
  - Using the security functions of the telecontrol protocols.
  - Leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CP disabled.
- Logging function

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

Passwords

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

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

Protocols

Secure and non-secure protocols

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

Table: Meaning of the column titles and entries

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

- **Protocol / function**

  Protocols that the device supports.
- **Port number (protocol)**

  Port number assigned to the protocol.
- **Default of the port**
  - Open

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

    The port is closed at the start of the configuration.
- **Port status**
  - Open

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

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

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

    The port is closed because the CP is always client for this service.
- **Authentication**

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

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
DNP3 listener port	20000 (TCP)	Closed	Open after configuration	No
IEC listener port	102 (TCP)	Closed	Open after configuration	No
S7 and online connections	2404 (TCP)	Open	Open after configuration *	No
Online security diagnostics	8448 (TCP)	Closed	Open after configuration	No
HTTP	80 (TCP)	Closed	Open after configuration	No
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)

* For information on avoiding opening the port during diagnostics, see section Online security diagnostics via port 8448 (Page 123).

4.2 Configuration in STEP 7

Configuration in STEP 7

You configure the modules and networks in SIMATIC STEP 7. You will find the required version in the section Software requirements (Page 23).

Fitting CPs in a rack

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

Requirement for configuring the communication

One requirement for configuring communication between the CP and the communications partner 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 control center devices and applications and connections between the CP and partner 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.

Loading and storing the configuration data

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

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

4.3 Addressing and authentication

4.3.1 TeleControl Basic

IP address of the CP

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

To change the IP address during operation, refer also to the section Changing the IP address during runtime (Page 119).

Address and authentication data 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

    IP address or host name of the DSL router via which the telecontrol server is connected to the Internet.

    A fixed IP address is recommended.
  - Partner port (port number of the listener port of TCSB)
- Parameters in the "Security > CP identification" parameter group
  - Project number
  - Station number
  - Password (for authentication)

4.3.2 DNP3 / IEC

To configure and commission the CP, the following information is required:

Address information of the master

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

- Address of the master
  - IP address

    or
  - Name that can be resolved with DNS

    If you use DNS, there must be a DNS server (see below) and this must be reachable for the CP.

- Port number of the listener port of the master
- DNS server address(es)

  You require the DNS server address if you address the master using a name that can be resolved by DNS.

Configurations with connections over the Internet: VPN connections

For connections running via the Internet, dynamic IP addresses can be used.

To allow communication in both directions and to ensure that the data is protected during transfer, a connection with a VPN tunnel is necessary. For this the security modules of the SCALANCE S or SCALANCE M series are available.

Remember the following points when configuring:

- You configure the master IP address as normal.
- When configuring the CP interface, configure the IP address of the router.
- You create the VPN configuration with SCALANCE S/M both for the station end and for the control center end in STEP 7.

4.4 Time-of-day synchronization

Synchronization method of the CP

Note

Time-of-day synchronization of the CP

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

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

Note

Recommendation for setting the time

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

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

- **Time from partner**

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

  Only when telecontrol communication is enabled.

- **NTP**

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

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

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

- **NTP (secure)**

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

  On the CP you specify the servers used.

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

- **Time from the CPU**

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

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

Parameter groups for time-of-day synchronization

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

- **Ethernet interface**

  Here you create the configuration under the following conditions:

  – Telecontrol communication is disabled.

  – The security functions are disabled.

- **Security**

  Here you create the configuration under the following condition:

  – The security functions are enabled.

Dependence of the synchronization method on the use of the CP

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

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

Time-of-day synchronization with the S7-1200

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

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

Note

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

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

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

Time-of-day synchronization of the CPU

The following synchronization methods are possible for the CPU:

- **NTP**

  Only this option can be configured actively for the CPU:

- **Time from CP**

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

Forwarding the time from the CP to the CPU

Note

Forwarding the time to the CPU

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

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

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

- **CP firmware ≤ V2.1.6x**

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

  In the parameter group "Communication with the CPU", you can set whether or not the current time of day of the CP will be made available to the CPU via a PLC tag. For TLC tags, see parameter group "Communication with the CPU" of the CP.

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

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

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

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

4.5 Communication types

In this parameter group, you enable the communication types 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**
  - TeleControl Basic
  - DNP3
  - IEC 60870-5

  Note that if you change the telecontrol communication type later, all specific parameters are deleted. These also include data point and partner information among other things.

- **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.

4.6 Ethernet interface

4.6.1 CP identification

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

CP addressing

The parameter group is used for addressing and identification of the CP in the network.

- TeleControl Basic

  You will find the parameters for the TeleControl Basic protocol in "Security", refer to the section CP iIdentifcation with the TeleControl Basic protocol (Page 64).

- DNP3

  The station address is the DNP address.

  Entry of the station address (digits only). Permitted range of values: 1...65519.

- IEC

  The station address is the “common address of the ASDU" or the address of the information object.

  Entry of the station address (digits only). Permitted range of values: 1...65534.

4.6.2 Time-of-day synchronization

Time-of-day synchronization

For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 42).

4.6.3 Advanced options

TCP connection monitoring

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

With TeleControl Basic and DNP3:
Note the option of overwriting the values configured here for individual communications partners, refer to the section Partner stations (Page 54).

- **TCP connection monitoring time**

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

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

  - **The parameter below the Ethernet interface**

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

  - **The parameter below "Partner stations"**

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

    If for any reason you want to change the value of the TCP connection monitoring time for individual partners, you can adapt the value for every partner individually in "Partner stations". If. for example, you want to check the connection at shorter intervals, reduce the value.

- **TCP keepalive monitoring time**

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

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

  - **The parameter below the Ethernet interface**

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

  - **The parameter below "Partner stations"**

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

4.6.4 Transmission settings – TeleControl Basic

Transmission settings – TeleControl Basic

- **Connection establishment delay**

  The settings made here apply to the connection to the telecontrol server.

  The reconnection delay is the waiting time between repeated attempts to establish the connection by the CP when the telecontrol server is not reachable or the connection has aborted.

  This waiting time avoids continuous connection establishment attempts at short intervals if there are connection problems.

  A basic value is configured for the waiting time before the next connection establishment attempt. Starting at the basic value, the current waiting time is doubled after every 3 unsuccessful retries up to a maximum value of 900 s.

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

  Example:
  A configured basic value 20 results in the following intervals (waiting times) between the attempts to re-establish a connection:

  – three times 20 s
  – three times 40 s
  – three times 80 s
  – etc. up to max. 900 s

  Note

  If the partner cannot be reached, connection establishment via the mobile wireless network can take several minutes. This may depend on the particular network and current network load.

  Depending on your contract, costs may result from each connection establishment attempt.

- **Send monitoring time**

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

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

- **Watchdog monitoring time**

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

The value configured in TCSB is transferred by the telecontrol server to the CP the first time the connection is established.

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

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

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

- Key exchange interval

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

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

4.6.5 Transmission settings – DNP3

Transmission settings – DNP3

- Disturbance bit

  The disturbance bit can be used as bit 1.6 (IIN1.6) of the "Internal Indication Bytes" to indicate to the master when the CPU is in STOP mode.

- Max. time between Select and Operate

  Max. duration (seconds) between Select and Operate. For a Select command to be transferred to the CPU and to take effect, no other frame may be sent to the station between Select and Operate.

  Permitted range: 1..65535

  Default setting: 1

- Frame repetitions

  Number of frame repetitions at the Data Link Layer if no acknowledgement is received from the master.

  Permitted range: 0 ... 255

  Default setting: 0

  If you enter 0 (zero), the function is disabled.

- Connection confirmation

  Condition for the CP to request a connection confirmation from the master (never, always, only with segmented frames).

- **Connection monitoring time**

  Time (in seconds) within which an acknowledgement is expected from the master.

  Permitted range: 0...65535

  Default setting: 2

  If you enter 0 (zero), the function is disabled.

- **Transfer mode "Unsolicited"**

  Transfer mode for events

  – Spontaneous

    Event frames are transferred immediately.

  – Conditional spontaneous

    Event messages are only sent when spontaneous frames are sent or the partner establishes the connection.

- **Max. number of unsolicited frames**

  Maximum number of repetitions of unsolicited frames if no acknowledgement is received from the communications partner .

  Permitted range: 0...255

  Default setting: 3

- **Monitoring time for unsolicited frames**

  Time (in seconds) within which an acknowledgement of unsolicited frames is expected from the master.

  Permitted range: 1...65535

  Default setting: 5

- **Buffer for class 1 / 2 / 3 events**

  Here, for each of the three event classes you specify the number of events after which the stored events are sent to the communications partner.

  Permitted range: 1 ... 255.

- **Delay time class 1 / 2 / 3 events**

  Here, for each of the three event classes you specify the maximum time in seconds the events can be stored in the send buffer before they are sent to the communications partner.

  Permitted range: 0 ... 65535

  If you enter 0 (zero), the function is disabled.

- **Event class for image memory**

  Selection of an event class in which only the last current values are stored in the send buffer.

  In the default setting all values of events of classes 1 and 2 are stored in the send buffer, of class 3 only the current values (image memory procedure).

You will find details of how the image buffer and send buffer work as well as the options for transferring data in the section Process image, type of transmission, event classes, triggers (Page 97).

4.6.6 Transmission settings - IEC

Transmission settings - IEC 60870-5

- **Max. time between Select and Operate**

  Max. duration (seconds) between Select and Operate. For a Select command to be transferred to the CPU and to take effect, no other frame may be sent to the station between Select and Operate.

  Permitted range: 1..65535

  Default setting: 1

- **Monitoring time for connection establishment** (t_0)

  Monitoring time for the connection establishment (t_0) in seconds. If the communications partner does not confirm connection establishment within the monitoring time, the CP attempts to establish the connection again.

  Permitted range: 1..255

  Default setting: 30

- **Frame monitoring time** (t_1)

  Monitoring time in seconds for the acknowledgement of frames sent by the CP by the communications partner. The monitoring time applies to all frames sent by the CP in I, S and U format.

  If the partner does not send an acknowledgment during the monitoring time, the CP terminates the connection to the partner.

  Permitted range: 1..255

  Default setting: 15

Note

Settings on the master

When configuring the monitoring times t_1 and t_2 make sure that you make the corresponding settings on the master so that there are no unwanted error messages or connection aborts.

- **Monitoring time for S and U frames** (t_2)

  Monitoring time in seconds for the acknowledgment of data frames of the master by the CP.

  After receiving data from the master, the CP acknowledges the received data as follows:

  – If the CP sends data to the master itself within t_2, it acknowledges the data frames received from the master during t_2 at the same time along with the sent data frame (I format).

  – The CP sends an acknowledgment frame (S format) to the master of the latest when t_2 elapses.

  Permitted range: 1 ... 255

  Default setting: 10

  The value of t_2 should be less than that of t_1.

- **Idle time for test frames** (t_3)

  Monitoring time in seconds during which the CP has not received any frames from the master.

  When t_3 elapses, the CP sends a test/control frame (U format) to the master.

  This parameter is intended for situations in which longer idle periods occur; in other words, times when there is no data traffic.

  Permitted range: 1 ... 255

  Default setting: 30

- **Difference between send sequence number N(S) and receive sequence number N(R)** (k)

  The difference between the send sequence number and receive sequence number of a frame.

  The master returns the send sequence number of a frame from the CP that the sending CP then saves as the receive sequence number. Frames whose send sequence number is lower than the receive sequence number after the difference configured here is added are evaluated as having been successfully transferred and are deleted from the send buffer of the CP.

  Permitted range: 1 ... 64

  Default setting: 12

- **Max. number of unacknowledged data frames** (w)

  w: Maximum number of received data frames (I-APDUs), after which the oldest frame received from the master must be acknowledged.

  Permitted range: 1..8

  Default setting: 8

  The value must be less than the value of "Difference between send and receive sequence number" (k).

Acknowledgment mechanism for the IEC protocol

With each sent data frame, the CP sends a continuous send sequence number. The data frame remains initially stored in the send buffer.

When it receives the data frame, the master sends the send sequence number from this or (if several frames are received) the last frame as an acknowledgement to the CP. The CP saves the send sequence number returned by the master as a receive sequence number and uses it as an acknowledgement.

Frames whose send sequence number is equal to or lower than the current receive sequence number are evaluated as having been successfully transferred and are deleted from the send buffer of the CP.

Recommendations of the specification:

- w should not be higher than 2/3 of k.
- Recommended value for k: 12
- Recommended value for w: 8

4.7 SNMP

SNMP

The CP supports the following SNMP versions:

- SNMPv1

  Available with security functions disabled.

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

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

  The CP uses the following community strings to authenticate access to its SNMP agent via SNMPv1:

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

  *) Note the use of lowercase letters!

- SNMPv3

  Available only when security functions are enabled

  For information on the configuring SNMPv3, refer to the section SNMP (Page 70).

Configuration

- **"Enable SNMP"**

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

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

4.8 Partner stations

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

4.8.1 Partner stations > General parameters

Listener port

Only with DNP3 / IEC

Here the listener port of the module, port for connection requests of the communications partner are displayed.

- Default for the DNP3 protocol: 20000
- Default for the IEC protocol: 2404

You can change the port number for the module. Keep in mind the settings on the communications partner (master).

Permitted range: 1024...65535

Partner'X' / telecontrol server

- **Activate partner**
  - TeleControl Basic

    The telecontrol server is enabled as the only possible partner in the default settings.
  - DNP3 / IEC

    By enabling the option the master that can then be configured is enabled for communication.
- **Partner number**

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

- **Station address / Master station address**
  - TeleControl Basic

    The station address of the telecontrol server is assigned automatically by the system if telecontrol communication is enabled.
  - DNP3

    For identification the station address mut be configured on the master.
  - IEC

    Common ASDU address

Connection to partner

- **Partner IP address**

  IP address or host name (FQDN) of the partner. This can, for example, also be the FQDN of a DynDNS service.
  - Note on TeleControl Basic

    If the CP is connected to a TCSB redundancy group (TCSB V3), here configure the public IP address of the DSL router via which the telecontrol server can be reached from the Internet. Set the port forwarding on the DSL router so that the public IP address (external network) is led to the virtual IP address of the TCSB server PCs (internal network). The station does not therefore receive any information telling it which of the two computers of the redundancy group it is connected to.

    See also section Addressing in the redundant TCSB system (Page 57).
- **Connection monitoring**

  Only for TeleControl Basic and DNP3

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

  The TCP connection monitoring time is set for all TCP connections of the CP in the parameter group of the Ethernet interface. The setting applies to all TCP connections of the CP.

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

- **TCP connection monitoring time**

  Only for TeleControl Basic and DNP3

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

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

  The monitoring time is specified at a higher level for the Ethernet interface as the default for all configured TCP connections.

  – **The parameter below the Ethernet interface**

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

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

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

    If for any reason you want to change the value of the TCP connection monitoring time for individual partners, you can adapt the value for every partner individually in "Partner stations". If. for example, you want to check the connection at shorter intervals, reduce the value.

- **TCP keepalive monitoring time**

  Only for TeleControl Basic and DNP3

  If the value configured here differs from the value configured in the Ethernet interface parameter group, the monitoring time of the "Partner stations" parameter group is used.

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

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

  – **The parameter below the Ethernet interface**

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

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

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

- **Connection mode**

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

  The CP only supports this connection mode.

- **Connection establishment**

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

- **Protocol type**

  Only for DNP3

  Selection of the protocol type on the transport layer: TCP / UDP

- **Partner port**

  Only with TeleControl Basic

  Number of the listener port of the telecontrol server.

4.8.2 TeleControl Basic

4.8.2.1 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 one CP without a DSL router is connected, the virtual address assigned by the NLB must be configured in the CP as the IP address of the telecontrol server.

  – If a 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 DSL router.

    Set the port forwarding on the DSL router so that the public IP address (external network) is led to the virtual IP address of the TCSB server PCs (internal network). 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.

4.8.2.2 Advanced settings

Telecontrol server > Advanced settings

- **Report partner status**

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

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

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

  – Bits 2-3 indicate the status of the send buffer (frame memory).
  The following values are possible:

  - 0: Send buffer OK

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

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

  As soon as the fill level drops below 50%, bits 2 and 3 are reset to 0.

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

4.8.2.3 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.

Frame memory

Activate the option for enabling inter-station communication.

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.

Access ID

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

- Bits 0 - 7: Slot
- Bits 8 - 20: Station number
- Bits 21 - 31: Project number

4.8.3 DNP3 / IEC

4.8.3.1 Advanced settings (DNP3 / IEC)

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. The CP aborts the connection and attempts to re-establish it.

  If you enter 0, the function is deactivated.

- **DNP3 level**

  Only for DNP3

  Indicates the DNP3 implementation level supported by the CP

  In the DNP3 specification, various levels of protocol conformity are and they describe the supported range of functions (subset) of a master or a station. These levels (implementation levels) are known as "DNP3 Application Layer protocol Level" and abbreviated with DNP3-L1 to DNP3-L4.

  For the communication between the CP and the master, the DNP3 level supported by the master must be known.

  The selection of the level used by the DNP3 CP which must correspond to that of the connected master is set separately in STEP 7 for each individual communications partner (DNP3 master).

The CP supports the following implementation levels:

– Level 1
– Level 2
– Level 3
– Level 4
– Level 4+

The implementation level known here as Level 4+ that is not specified in the standard contains the range of functions of Level 4 and in addition support of the following DNP3 data types / variations:

– 64-bit analog value as floating-point number without time of day
– 64-bit analog value as floating-point number with time of day
– Counter event with time of day in 16-bit format
– Counter event with time of day in 32-bit format

- **Event transmission mode**

  Only for DNP3

  Mode with which DNP events are transferred to this communications partner:

  – Chronological transfer of individual frames

    or

  – Transfer of collected frames per data point as a block.

- **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 3 to 15 of the PLC tags are not used and do not need to be evaluated in the program.

Communication with the CPU

Using the first three parameters you specify the CPU access by the CP in the CPU scan cycle. You will find the structure of the CPU scan cycle in the section Read cycle (Page 96).

The fourth parameter "Frame memory size" decides the size of the send buffer on the CP for frames of data points that are configured as an event.

- Cycle pause time

  Wait time between two scan cycles of the CPU memory area

- Max. number of write jobs

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

- Max. number of read jobs

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

- Frame memory size

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

  The size of the frame memory is divided equally among all configured communications partners. You will find the size of the frame memory in the section Configuration limits and performance data (Page 15).

  You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Process image, type of transmission, event classes, triggers (Page 97).

Watchdog bit

- CP monitoring

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

CP time of day

- CP time to CPU

  Using this function, the CP can make its time of day available to the CPU.

  You will find details in the STEP 7 information system.

CP diagnostics

With the parameter group, you have the option of reading out advanced diagnostics data from the CP using PLC tags.

- **Enable advanced CP diagnostics**

  Enable the option to be able to use advanced CP diagnostics.

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

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

- **Diagnostics trigger tag**

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

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

  Note

  Fast setting of the diagnostics trigger variable

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

- **Frame memory overflow**

  PLC tag (data type byte) for the send buffer overflow pre-warning. Bit 0 is set to 1 when 80% of the fill level of the send buffer is reached.

- **Frame memory size**

  PLC tag (data type DWord) for the occupation of the send buffer. The number of saved frames is displayed.

- **Date of last successful logon to TCSB**

  Only for the TeleControl Basic protocol

  PLC tag (data type DTL) for the date on which the CP last logged in to the telecontrol server.

- **Date of last unsuccessful logon to TCSB**

  Only for the TeleControl Basic protocol

  PLC tag (data type DTL) for the date on which the CP was last unable to log in to the telecontrol server.

- **TeleService status**

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

  – 0 = No TeleService session active

  – 1 = TeleService session active

- **VPN status**

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

  – 0 = No VPN tunnel established

  – 1 = VPN tunnel established

4.9 Security

You will find an overview of the range and use of the security functions in section Security functions (Page 13).

For the configuration limits of the security functions refer to the section Configuration limits and performance data (Page 15).

4.9.1 Parameter overview

Parameter groups

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

- **CP identification**

  Only with the TeleControl Basic protocol

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

- **DNP3 security options**

  Only with the DNP3 protocol

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

- **Firewall**

  See section Firewall (Page 67).

- **Time synchronization**

  For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 42).

- **E-mail configuration**

  See section E-mail configuration (Page 69).

- **Log settings**

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

  See section Log settings - Filtering of the system events (Page 70).

- **SNMP**

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

  See section SNMP (Page 70).

- **Certificate manager**

  See section Certificate manager (Page 72).

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

- **VPN groups**

  Here you configure the VPN communication, refer to the section VPN (Page 74).

- **User management**

  Here you configure the users, roles and rights for the TeleService access, refer to the section Configuration of the TeleService access (Page 80).

4.9.2 CP iIdentifcation with the TeleControl Basic protocol

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

- Project number

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

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

- Station number

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

- Telecontrol password

  Password for the authentication of the CP on the telecontrol server

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

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

- Access ID

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

  – Bits 0 - 7: Slot
  – Bits 8 to 20: Station number
  – Bits 21 to 31: Project number

4.9.3 DNP3 security options

Partner'X'

Preliminary remarks: Authentication and key exchange

If the security function is enabled, the DNP3 master and CP authenticate themselves with a secret key, the pre-shared key.

With the help of the common pre-shared key, after the first connection establishment between master and CP session keys are agreed that are then renewed cyclically. Renewal of the session keys is normally initiated by the master. The criteria for renewing the key are specified in the following parameters.

- Key exchange interval
- Authentication requests before key exchange

As soon as one of these conditions is met, the session key is renewed.

Parameters

- **Enable DNP3 security options**

  Enable the option if you want to use the security mechanisms.

- **IKE mode**

  Selection of the mode for key exchange. Range of values:

  – Aggressive Mode

    The Aggressive Mode is somewhat faster but transfers the identity unencrypted.

  – Main Mode

    The Main Mode is the standard mode.

  Default setting: Aggressive Mode

- **Security statistics**

  Specifies whether the statistics of security events are sent to the master. Security events are authentication requests to the CP. If the option is enabled, all authentication requests with date, time and result are saved on the CP and sent to the master for further evaluation.

  Range of values:

  – Do not send security statistics

  – Send security statistics

  Default setting: Do not send security statistics

- **SHA-1 interlock**

  Setting to select whether the CP may use the secure hash algorithm SHA-1 if "SHA-256" was configured as the Secure hash algorithm and the master does not support SHA-256.

  Range of values:

  – SHA-1 mode not allowed

    The CP may not use SHA-1. If the master does not support SHA-256, no connection will be established.

  – SHA-1 mode allowed

    The CP can use SHA-1 if the master does not support SHA-256.

  Default setting: SHA-1 mode not allowed

- **Secure hash algorithm (SHA)**

  Selection of the Secure Hash Algorithm (SHA)

  Range of values:

  – SHA-1

  – SHA-256

  Default setting: 256

- **Key wrap algorithm**

  Selection of the Advanced Encryption Standard (AES)

  Range of values:

  – AES-128

  – AES-256

  Default setting: AES-128

- **Key length**

  Specifies the length of the pre-shared key in bytes.

  Permitted range: 16 - 128 Depending on the secure hash algorithm configured in STEP 7 above, the following lengths are preset:

  – For SHA-1: 16

  – For SHA-256: 32

  The value 0 (zero) is not permitted.

- **Max. number of statistics queries**

  If the configured number of statistics queries of the master is exceeded within the key exchange interval, the CP enters a message in the diagnostics buffer of the CPU.

  Range of values: 2...255 Default setting: 5

- **Authentication requests before key exchange**

  Maximum number of authentication requests of the CP with the master. When this number is reached, the session key is renewed.

  Range of values: 1...10000 Default setting: 1000

  Recommendation: Set the number for the CP twice as high as for the master.

- **Key exchange interval**

  Period after which the key is exchanged again between the CP and the master. The interval must be matched up on both communications partners.

  Range of values: 0...65535 min. at 0 (zero), the key is never changed (function disabled). Default setting: 15 min.

  Recommendation: Set the key exchange interval for the CP twice as high as for the master.

- **Authentication timeout**

  Maximum waiting time for the response from the master to an authentication request of the CP.

  Exceeding the wait time is evaluated as an error by the CP. In this case, the CP generates a security event and sends this to the master.

  Range of values: 1... 65535 s Default setting: 5

- **Pre-shared key**

  The pre-shared key can be configured in two ways:

  – Manual configuration

    Enter the pre-shared key in STEP 7 manually as a hexadecimal value.

  – Import as file

    Import the pre-shared key from the file system of the engineering station if the pre-shared key was generated by the master or another engineering system.

  The pre-shared key of the CP must be identical to the pre-shared key of the master.

4.9.4 Firewall

4.9.4.1 Pre-check of messages by the MAC firewall.

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

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

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

- Separate the two IP addresses only using a hyphen.

  Correct: 192.168.10.0-192.168.10.255

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

  Incorrect: 192.168.10.0 - 192.168.10.255

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

4.9.4.3 Firewall settings for configured connection connections via a VPN tunnel

IP rules in advanced firewall mode

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

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

See also

Settings for online security diagnostics and downloading to station with the firewall activated (Page 68)

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

Setting the firewall for online functions

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

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

7. In the table, insert a new IP rule for the previously created global services as follows:
   – Action: Allow; "From external -> To station " with the globally created "Echo request" service
   – Action: Allow; "From station -> to external" with the globally created "Echo reply" service
8. For the IP rule for the Echo Request, enter the IP address of the engineering station in "Source IP address". This ensures that only ICMP frames (ping) from your engineering station can pass through the firewall.

4.9.5 E-mail configuration

Configuring e-mails in STEP 7

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

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

You configure the individual e-mails in the message editor (entry "Messages"), see section Messages (Page 113)

Requirements

The following requirements must be met in the configuration for sending e-mails:

- The security functions are enabled.
- The time of the CP is synchronized.
- In the "E-mail configuration" entry, the protocol to be used and the data for access to the e-mail server are configured.

E-mail configuration

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

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

- Port no. 587

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

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

- Port no. 465

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

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

Importing the certificate with encrypted transfer

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

Use the certificate by taking the following steps:

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

For the procedure, refer to the section Handling certificates (Page 72).

4.9.6 Log settings - Filtering of the system events

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

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

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

4.9.7 SNMP

SNMP

The range of functions of the CP for SNMP can be found in the section SNMP (Page 125).

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

SNMP

- **"Enable SNMP"**

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

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

- "Use SNMPv1"

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

- "Use SNMPv3"

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

SNMPv1

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

- "Reading community string"

  The string is required for read access.

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

- "Allow write access"

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

- "Writing community string"

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

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

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

SNMPv3

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

- "Authentication algorithm"

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

- "Encryption algorithm"

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

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

User management

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

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

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

4.9.8 Certificate manager

Assignment of certificates

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

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

For a description of the procedure, refer to the section Handling certificates (Page 72).

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

4.9.9 Handling certificates

Certificate for authentication

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

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

Note

No certificate with security functions disabled.

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

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

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

1. Importing third-party certificates from communications partners

   ⇒ Global security settings of the project (certificate manager)

2. Assigning certificates locally

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

These two steps are described in the next two sections.

Importing third-party certificates from communications partners

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

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

   Global security settings > Certificate manager

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

Assigning certificates locally

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

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

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

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

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

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

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

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

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

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

   Global security settings > Certificate manager

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

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

Certificate for logging server

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

Change certificate: Subject Alternative Name

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

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

4.9.10 VPN

4.9.10.1 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

4.9.10.2 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.

4.9.10.3 VPN communication with SOFTNET Security Client (engineering station)

Setting up VPN tunnel communication between the SOFTNET Security Client and the CP is essentially the same as described in Creating a VPN tunnel for S7 communication between stations (Page 76).

VPN tunnel communication works only if the internal node is disabled

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

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

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

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

Disable the node in the SOFTNET Security Client tunnel overview:

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

   The lower-level node initially disappears from the tunnel list.
2. In the tunnel list, select the required connection to the CP.
3. With the right mouse button, select "Enable all members" in the shortcut menu.

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

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

4.9.10.4 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.

4.9.10.5 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.

4.9.10.6 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

4.9.10.7 SYSLOG

Use of SYSLOG only with 1 VPN connection

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

4.9.11 Configuration of the TeleService access

Configuration for using TeleService

To meet the requirements for using the TeleService functions for the CP, you need to make the necessary settings at the following points in STEP 7.

"Communication types" parameter group of the CP

Select the following options:

- Enable telecontrol communication
- Activate online functions

Telecontrol server under "Partner stations" of the CP

You configure the following information here:

- Address of the telecontrol server

  IP address or name of the telecontrol server that can be resolved by DNS.
- Port

  Port number of the telecontrol server

Users and roles in the global security settings

1. Open the following page in the project tree:

   Global security settings > User management

2. Role

   Open the "Roles" tab

   The two tables "Roles" and "Rights of the role" become visible.

   If necessary open the "Roles view" if this is hidden by the "Rights of the role" table.

   In the "Roles" table (at the top) create a new user-defined role for TeleService.

3. In the "User" tab create a user that will later be allowed to execute the TeleService functions for the CP.

   Configure the following parameters:

   – User name

     Assign the name of the user that will have TeleService rights.

     You require the user name at the start of a TeleService session.

   – Authentication method

     Select the authentication method "Password" for this user.

   – Password

     Assign the password.

     You require the password at the start of a TeleService session.

     Note:
     You specify the password properties of the security functions in the "Password policies" tab.

     You enter the password on the engineering station when starting a TeleService session.

   – Maximum time of the session

     The time that can be configured here is only required for access to SCALANCE S modules. If the user is set up only for TeleService sessions, you can leave the default value unchanged.

4. Click on the "Roles" tab.
5. Select the CP in the lower list "Rights of the role" under the "Module rights" group.
6. The available rights are displayed in the "List of rights" table.

   The right "Use TeleService" is displayed.

7. Enable the "Use TeleService" right for the module.
8. Following this, set the S7 protocol to "allow" in Firewall.

4.10 Data points

4.10.1 Data point configuration

Data point-related communication with the CPU

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

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

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

PLC tags or DBs must first be created 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 15).

The formats and S7 data types of the PLC tags that are compatible with the protocol-specific data point types of the module can be found in the section Datapoint types (Page 89).

Access to the memory areas of the CPU

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

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

Configuring the data points and messages in STEP 7

You configure the data points in STEP 7 in the data point and message editor. You can find this using the project tree:

Project > directory of the relevant station > Local modules > CP

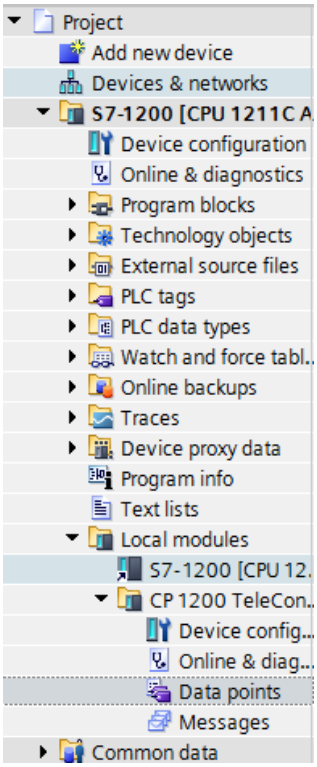


Figure 4-1 Configuring data points and messages

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

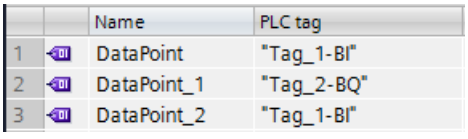
Using the two entries to the right above the table, you can switch over between the data point and message editor.

Figure 4-2 Switching over between the two editors

Creating obects

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

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



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

Figure 4-3 Data point table

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

Assigning data points to their data source

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

For the assignment you have the following options:

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

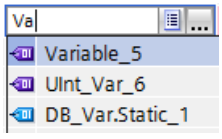
  All configured PLC tags and the tags of the created data blocks are displayed. Select the required data source with the mouse or keyboard.

- Click the symbol ...

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

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

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

  Select the required data source.

Note

Assignment of parameter values to PLC tags

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

Arranging and copying objects

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

- Arrange columns

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

- Sorting objects

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

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

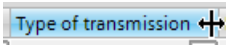
- Adapting the column width

  You can reach this function with the following actions:

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

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

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

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

- Showing / hiding columns

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

- Copying, pasting, cutting and deleting objects

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

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

Exporting and importing data points

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

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

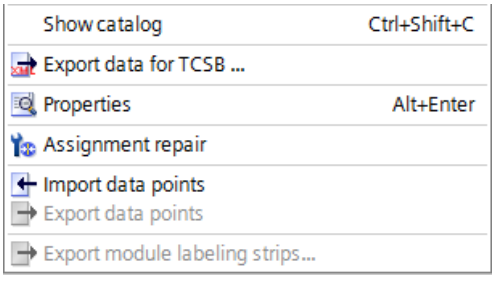


Figure 4-4 Shortcut menu of the module

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

Export

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

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

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

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

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

Editing the data point information

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

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

The lines of the CSV file have the following content:

- Line 1: ,Name,Type,

  This line must not be changed.
- Line 2: PLC,<CPU name>, <CPU type>,

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

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

  The CPU type must correspond exactly to the name of the CPU in the catalog.
- Line 3: Module,<module name>, <module type>,

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

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

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

  The module type must correspond exactly to the name of the module in the catalog.
- Line 4: Parameter names (English) of the data points

  This line must not be changed.
- Lines 5..n: Values of the parameters according to line 4 of the individual data points

  You can change the parameter values for the particular station.

Importing into a module

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

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

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

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

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

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

Importing into several modules

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

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

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

Restrictions for the import of data points

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

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

  Example: If a data point to be imported uses a time trigger, the import will be aborted if no time-of-day synchronization was configured for the module.
- The telecontrol protocol used by the module differs from that of the original module.

Only when importing into several modules:

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

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

- TeleControl Basic

  All SIMATIC NET modules with the TeleControl Basic protocol:

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

- ST7

  CP 1243-8 IRC, TIM modules capable of ST7

- DNP3

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

- IEC

  CP 1243-1, CP 1243-8 IRC

Data points can be imported and exported between compatible modules.

Assignment repair

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

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

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

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

4.10.2 Syntax of the data point names

Character set for data point names

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

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

Forbidden characters:

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

4.10.3 Datapoint types

Configure the user data to be transferred from the CPU that is referenced via PLC tags of the CPU on the CP as data points.

The data point types supported by the CP along with the compatible S7 data types are listed below for the various telecontrol protocols.

The direction relates to the direction of transfer:

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

Note

Effect of the change of arrays for data points

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

Data point types of the "TeleControl Basic" protocol

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

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

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

Block of data (ARRAY)

With the ARRAY data type, contiguous memory areas up to a size of 64 bytes can be transferred. The following S7 data types are compatible components of ARRAY:

- Byte, USInt (total of up to 64 per data block)
- Char (total of up to 64 per data block) - CP as of firmware version 2.1.77

- Int, UInt, Word (total of up to 32 per data block)
- DInt, UDInt, DWord (total of up to 16 per data block)

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

Format of the time stamp

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

Data point types of the "DNP3" protocol

Table 4- 2 Supported data point types, DNP3 object groups, variants and compatible S7 data types

Format (memory requirements)	Data point type CP [Data point type TIM]	DNP3 object group [variations]	Direction	S7 data types	Operand area
Bit	Binary Input	**1** [1, 2]	in	Bool	I, Q, M, DB
	Binary Input Event	**2** [1, 2]	in	Bool	I, Q, M, DB
	Binary Output [1)]	**10** [2]	out	Bool	Q, M, DB
	Binary Output Event [1)]	**11** [1, 2]	out	Bool	Q, M, DB
	Binary Command	**12** [1]	out	Bool	Q, M, DB
Integer (16 bits)	Counter Static	**20** [2]	in	UInt, Word	I, Q, M, DB
	Frozen Counter [2)]	**21** [2, 6]	in	UInt, Word	I, Q, M, DB
	Counter Event	**22** [2, 6]	in	UInt, Word	I, Q, M, DB
	Frozen Counter Event [3)]	**23** [2, 6]	in	UInt, Word	I, Q, M, DB
	Analog Input	**30** [2]	in	Int	I, Q, M, DB
	Analog Input Event	**32** [2]	in	Int	I, Q, M, DB
	Analog Output Status [4)]	**40** [2]	out	Int	Q, M, DB
	Analog Output	**41** [2]	out	Int	Q, M, DB
	Analog Output Event [4)]	**42** [2, 4]	out	Int	Q, M, DB
Integer (32 bits)	Counter Static	**20** [1]	in	DWord	I, Q, M, DB
	Frozen Counter [2)]	**21** [1, 5]	in	DWord	I, Q, M, DB
	Counter Event	**22** [1, 5]	in	DWord	I, Q, M, DB
	Frozen Counter Event [3)]	**23** [1, 5]	in	DWord	I, Q, M, DB
	Analog Input	**30** [1]	in	DInt	Q, M, DB
	Analog Input Event	**32** [1]	in	DInt	Q, M, DB
	Analog Output Status [4)]	**40** [1, 3]	out	DInt	Q, M, DB
	Analog Output	**41** [1]	out	DInt	Q, M, DB
	Analog Output Event [4)]	**42** [1]	out	DInt	Q, M, DB

Format (memory requirements)	Data point type CP [Data point type TIM]	DNP3 object group [variations]	Direction	S7 data types	Operand area
Floating-point number (32 bits)	Analog Input	**30** [5]	in	Real	Q, M, DB
	Analog Input Event	**32** [5, 7]	in	Real	Q, M, DB
	Analog Output Status [4]	**40** [3]	out	Real	Q, M, DB
	Analog Output	**41** [3]	out	Real	Q, M, DB
	Analog Output Event [4]	**42** [5, 7]	out	Real	Q, M, DB
Floating-point number (64 bits)	Analog Input	**30** [6]	in	LReal	Q, M, DB
	Analog Input Event	**32** [6, 8]	in	LReal	Q, M, DB
	Analog Output	**41** [4]	out	LReal	Q, M, DB
	Analog Output Event [4]	**42** [6, 8]	out	LReal	Q, M, DB
Data block (1...64 bytes) [5]	Octet String / Octet String Output	**110** [-]	in, out	[5]	DB
	Octet String Event [5]	**111** [-]	in, out	[5]	DB

[1] This object group can be configured in the Data point editor of STEP 7 using the substitute object group 12.

[2] This object group can be configured in the Data point editor of STEP 7 using the substitute object group 20.

[3] This object group can be configured in the Data point editor of STEP 7 using the substitute object group 22.

[4] This object group can be configured in the Data point editor of STEP 7 using the substitute object group 41.

[5] With these data point types, contiguous memory areas up to a size of 64 bytes can be transferred. All S7 data types with a size between 1 and 64 bytes are compatible.

Substitute object groups (of the table footnotes [1], [2], [3], [4])

The initial data point types of the following object groups can be configured using the substitute object groups listed above:

- 10 [2]
- 11 [1, 2]
- 21 [1, 2, 5, 6]
- 23 [1, 2, 5, 6]
- 40 [1, 2, 3]
- 42 [1, 2, 4, 5, 6, 7, 8]

To configure the DNP3 CP, use the specified substitute object group.

Assign each data point on the master using the configurable data point index in STEP 7. The data point of the DNP3 CP is then assigned to the corresponding data point on the master.

Example of configuring the data point Binary Output (10 [2])
The data point is configured as follows:
On the DNP3 CP as Binary Command (12 [1])
On the master as Binary Output (10 [2])

With the data point types Binary Output Event (11) and Analog Output Event (42), you also need to enable mirroring; refer to the next section.

Configuration of the mirroring back for output events (object groups 11 and 42)

You first create the data point types Binary Output Event (object group 11) and Analog Output Event (object group 42) as described above as data points of the object groups 12 or 41.

The local values of these two object groups can be monitored for change and the changes transferred to the master (). Changing a local value can, for example, be caused by manual operator input on site.

To allow the value resulting from local events or interventions to be transferred to the master, the data point in question requires a channel for mirroring back. You configure this mirroring back function is configured using the "Value monitoring" option in data point configuration, General tab.

Remember that to use the mirror back function, you need to interconnect the local values in the controller with the relevant PLC tag of the data point.

Format of the time stamp

Time stamps are transferred in UTC format (48 bits) and contain milliseconds.

Data point types of the "IEC" protocol

Table 4- 3 Supported data point types, IEC types and compatible S7 data types

Format (memory requirements)	Data point type	IEC type	Direction	S7 data types	Operand area
Bit	Single-point information	<1>	in	Bool	I, Q, M, DB
	Single-point information with time tag CP56Time2a 1)	<30>	in	Bool	I, Q, M, DB
	Single command	<45>	out	Bool	Q, M, DB
	Single command with time tag CP56Time2a 1)	<58>	out	Bool	Q, M, DB
	Double command with time tag CP56Time2a 1)	<59>	out	Bool	Q, M, DB
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag CP56Time2a 1)	<32>	in	Byte, USInt	I, Q, M, DB
	Regulating step command with time tag CP56Time2a 1)	<60>	out	Byte, USInt	Q, M, DB
Integer (16 bits)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag CP56Time2a 1)	<34>	in	Int	I, Q, M, DB
	Measured value, scaled value	<11>	in	Int	I, Q, M, DB
	Measured value, scaled value with time tag CP56Time2a 1)	<35>	in	Int	I, Q, M, DB
	Set point command, normalised value	<48>	out	Int	Q, M, DB
	Set point command, scaled value	<49>	out	Int	Q, M, DB
	Set point command, normalised value with time tag CP56Time2a 1)	<61>	out	Int	Q, M, DB
	Set point command, scaled value with time tag CP56Time2a 1)	<62>	out	Int	Q, M, DB

Format (memory requirements)	Data point type	IEC type	Direction	S7 data types	Operand area
Integer (32 bits)	Bitstring of 32 bits	<7>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a [1]	<33>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals	<15>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals with time tag CP56Time2a [1]	<37>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits	<51>	out	UDInt, DWord	Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a [1]	<64>	out	UDInt, DWord	Q, M, DB
Floating-point number (32 bits)	Measured value, short floating point number	<13>	in	Real	Q, M, DB
	Measured value, short floating point number with time tag CP56Time2a [1]	<36>	in	Real	Q, M, DB
	Set point command, short floating point number	<50>	out	Real	Q, M, DB
	Set point command, short floating point with time tag CP56Time2a [1]	<63>	out	Real	Q, M, DB
Data block (1...2 Bit) [2]	Double-point information	<3>	in	[2]	DB
	Double-point information with time tag CP56Time2a [1]	<31>	in	[2]	DB
	Double command	<46>	out	[2]	DB
	Regulating step command	<47>	out	[2]	DB
	Double command with time tag CP56Time2a [1]	<59>	out	[2]	DB
	Regulating step command with time tag CP56Time2a [1]	<60>	out	[2]	DB
Data block (1...32 Bit) [3]	Bitstring of 32 bits [3]	<7>	in	[3]	DB
	Bitstring of 32 bits with time tag CP56Time2a [1] [3]	<33>	in	[3]	DB
	Bitstring of 32 bits [3]	<51>	out	[3]	DB
	Bitstring of 32 bits with time tag CP56Time2a [1] [3]	<64>	out	[3]	DB

[1] For the format of the time stamp, see the following section.

[2] For these data point types, create a data block with an array of precisely 2 bool.

[3] With these data point types, contiguous memory areas up to a size of 32 bits can be transferred. Only the S7 Bool data type is compatible.

Format of the time stamp

Time stamps are transferred according to the IEC specification in the "CP56Time2a" format. Note that in the frames only the first 3 bytes for milliseconds and minutes are transferred.

4.10.4 Configuration of the data point index

Configuration of the data point index

Below you will find the rules for configuring the data point index.

Data point index with the TeleControl Basic protocol

Within a CP, the indexes of the data point classes must comply with the following rules:

- Input

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

- Output

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

Note

Index for data points with inter-station communication

Note that for inter-station communication with a CP in another S7 station, the indexes of the two corresponding data points (data point pair) must be identical on the sending and receiving CP.

For information on the configuration, refer to the section Partner configuration with TeleControl Basic data points. (Page 112).

Data point index with the DNP3 protocol

On a CP, data point indexes must be unique within each of the following object groups:

- Binary Input / Binary Input Event
- Binary Output / Binary Command
- Counter / Counter Event
- Analog Input / Analog Input Event
- Analog Output
- Octet String / Octet String Event

Indexes of two data points in different object groups can be identical.

Data point index with the IEC protocol

The data point indexes must be unique in a CP.

Data point indexes assigned twice are indicated as errors in the consistency check and prevent the project being saved.

4.10.5 Status IDs of the data points

Status identifiers

The status identifiers of the data points listed in the following tables are transferred along with the value in each frame to the communications partner. They can be evaluated by the communications partner.

The entries in the table row "Significance" relate to the entry in the table row "Bit status".

Generation of events if a data point status changes

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

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

Status identifiers with the TeleControl Basic protocol

Depending on their status, the status bits (see table) are converted to the OPC quality code by TCSB.

- Quality = BAD

  Bit 2 or 7 = 1
- Quality = UNCERTAIN

  Bit 1 or 3 or 5 = 1
- Quality = GOOD

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

Table 4- 4 Bit assignment of status byte 0

Bit	7	6	5	4	3	2	1	0
Flag name	-	NON_ EXISTENT	Substituted	LOCAL_ FORCED	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	Limit value of the analog preprocessing overshot / undershot	Value not yet updated after start	Value is valid
Bit status	*(always 0)*	1	1	1	1	1	1	1

Status identifiers with the DNP3 protocol

The status IDs correspond to the following elements of the specification:

OBJECT FLAGS - DNP3 Specification, Volume 6, Data Object Library - Part 1

Table 4- 5 Bit assignment of the status byte

Bit	7	6	5	4	3	2	1	0
Flag name	-	-	-	LOCAL_ FORCED	DISCONTI NUITY	OVER_ RANGE	RESTART	ONLINE
Meaning	-	-	-	Local opera-tor control	Counted value over-flow before reading the value	Limit value of the analog prepro-cessing over-shot / undershot	Value not yet updated after start	Value is valid
Bit status	*(always 0)*	*(always 0)*	*(always 0)*	1	1	1	1	1

Status identifiers with the IEC protocol

The status IDs correspond to the following elements of the specification:

Quality descriptor - IEC 60870 Part 5-101

Table 4- 6 Bit assignment of the status byte

Bit	7	6	5	4	3	2	1	0
Flag name	-	-	SB substituted	-	CY carry	OV overflow	NT not topical	IV invalid
Meaning	-	-	Substitute value	-	Counted value over-flow before reading the value	Value range exceeded, analog value	Value not updated	Value is valid
Bit status	*(always 0)*	*(always 0)*	1	*(always 0)*	1	1	1	0

4.10.6 Read cycle

Priority of the data points

The cyclic reading of the values of input data points from their assigned PLC tags on the CPU can be prioritized.

Less important input data points do not need to be read in every CPU scan cycle. Important input data points, on the other hand, can be prioritized for updating in every CPU scan cycle.

You can prioritize the data points in STEP 7 in the data point configuration in the "General" tab with the "Read cycle" parameter. There you will find the two following options for input data points:

- Fast cycle
- Normal cycle

The data points are read according to the method described below.

Structure of the CPU scan cycle

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

- **High-priority read jobs**

  The values of input data points with the scan priority "High-priority" are read in every scan cycle.

- **Low priority read jobs**

  Some of the values of input data points with the scan priority "Low-priority" are read in every scan cycle.

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

- **Write jobs**

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

- **Cycle pause time**

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

4.10.7 Process image, type of transmission, event classes, triggers

Saving the data point values

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

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

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

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

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

- **Triggered: event**

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

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

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

The image memory, the process image of the CP

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

The values are sent after querying the communications partner, see "Transfer after call" in the section "Types of transmission" below.

The send buffer (frame memory)

The send buffer of the CP is the memory for the individual values of data points that are configured as an event. The maximum size of the send butter can be found in the section Configuration limits and performance data (Page 15).

The configured number of events is divided equally among all configured and enabled communications partners. For information on the configuration, refer to the parameter "Frame memory size" in the section SNMP (Page 53).

If the connection to a communications partner is interrupted, the individual values of the events are stored in the RAM of the CP. When the connection returns, the buffered values are sent. The frame memory operates chronologically; in other words, the oldest frames are sent first (FIFO principle).

If a frame was transferred to the communications partner, the transferred values are deleted from the send buffer.

If frames cannot be transferred for a longer period of time and the send buffer is threatening to overflow, the response is as follows:

The forced image mode with TeleControl Basic

If the send buffer reaches a fill level of 80%, the CP changes to the forced image mode. New values of events are no longer added to the send buffer but rather they overwrite older existing values in the image memory.

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

Types of transmission / event classes

The following types of transmission are possible:

- **Transfer after call**

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

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

- **Triggered (event)**

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

  The values of events are saved in the following situations:

  – The configured trigger conditions are fulfilled (data point configuration > "Trigger" tab, see below)

  – The value of a status bit of the status identifiers of the data point changes see also the section Status IDs of the data points (Page 95).

    Example: When the value of a data point configured as an event is updated during startup of the station by reading the CPU data for the first time, the status "RESTART" of this data point changes (bit status change 1 → 0). This leads to generation of an event.

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

  – **Every value triggered**

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

  – **Current value triggered**

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

Trigger

Trigger types

Various trigger types are available for 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 101).

- **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. As 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 tag in the bit memory area / DB:

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

Transmission time of the frame (Transmission mode)

Whether the value of a data point is transferred to the communications partner immediately after the trigger fires or after a delay depends on the setting of the parameter "Transmission mode" in the "Trigger" tab of the data point:

- **Spontaneous**

  The value is transferred immediately.

- **Conditional spontaneous**

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

  – The telecontrol server queries the station.

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

4.10.8 "Trigger“ tab

Trigger

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

Saving the value of a data point configured as an event

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

- **Threshold value trigger**

  The value of the data point is saved when this reaches a certain threshold. The threshold is calculated as the difference compared with the last stored value, refer to the section Threshold value trigger (Page 101).

- **Time trigger**

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

- **Event trigger (Trigger tag)**

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

Resetting the trigger tag in the bit memory area / DB:

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

Note

Fast setting of triggers

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

Note

Hardware trigger

You need to reset hardware triggers via the user program

Transferring the value of a data point configured as an event

You specify whether the value of a data point is transferred to the communications partner immediately after the trigger fires or after a delay in the "Transmission mode" parameter.

Transmission mode

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

- Immediate transfer - Spontaneous

  The value is transferred immediately.

- Buffered transfer - Conditionally spontaneous

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

  – The communications partner queries the station.

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

4.10.9 Threshold value trigger

Note

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

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

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

Note

No Threshold value trigger if Mean value generation is configured

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

For the time sequence of the analog value preprocessing refer to the section Analog value preprocessing (Page 103).

Threshold value trigger

Function

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

Two methods are used to calculate the threshold value deviation:

- **Absolute method**

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

- **Integrative method**

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

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

Absolute method

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

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

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

Integrative method

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

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

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

Table 4- 7 Example of the integration calculation of a threshold value configured with 2.0

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

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

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

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

4.10.10 Analog value preprocessing

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

Requirements and restrictions

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

Note

Restrictions due to configured triggers

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

Sequence of the analog value preprocessing options

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

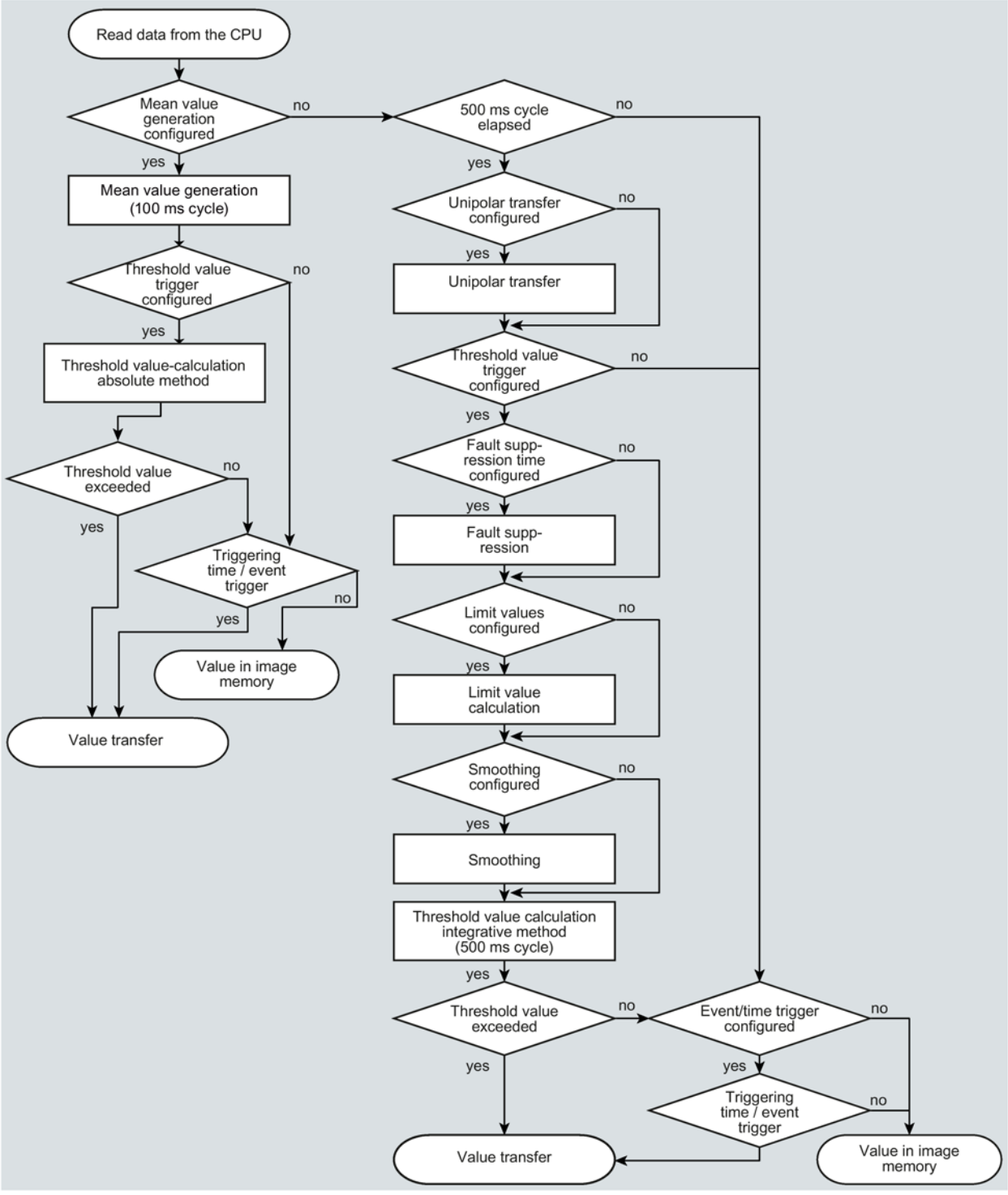


Figure 4-5 Sequence of the analog value preprocessing

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

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

Mean value generation

Note

Restricted preprocessing options if mean value generation is configured

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

- Unipolar transfer
- Fault suppression time
- Smoothing

Function

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

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

The current values of an analog data point are read in a 100 millisecond cycle and totaled. The number of read values per time unit depends on the read cycle of the CPU and the CPU scan cycle of the CP.

The mean value is calculated from the accumulated values as soon as the transfer is triggered by a trigger. Following this, the accumulation starts again so that the next mean value can be calculated.

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

Input modules: Overflow range / underflow range

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

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

Note

Fault suppression time > 0 configured

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

Unipolar transfer

Restrictions

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

Function

With unipolar transfer, negative values are corrected to zero. This can be desirable if values from the underrange should not be transferred as real measured values.

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

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

Fault suppression time

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

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

Function

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

The transmission of an analog value in the overflow ($7FFF_h$) or underflow range (8000_h) is suppressed for the specified time. The value $7FFF_H$ or 8000_H is only sent after the fault suppression time has elapsed, if it is still pending.

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

Input modules

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

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

Recommendation for finished values that were preprocessed by the CPU:

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

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

Smoothing factor

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

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

Function

Analog values that fluctuate quickly can be evened out using the smoothing function.

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

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

where
y_n = smoothed value in the current cycle
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

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

Requirements for the function

- Configuration of the threshold trigger for this data point
- PLC tag in the bit memory operand area or data area

  The analog value data point must be linked to a PLC tag in the bit memory or data area (data block). For PLC tags of hardware modules (input operand area) limit value configuration is not possible.

The configuration of limit values is pointless for measured values that have already been preprocessed on the CPU.

Function

In these two input boxes, you can set a limit value in the direction of the start of the measuring range or in the direction of the end of the measuring range. You can also evaluate the limit values, for example as the start or end of the measuring range.

Status identifier "OVER_RANGE" / "overflow"

With protocols that support status identifiers, if the limit value is overshot or undershot, the status identifier of the data point is set for measured range violation known below as the identifier "OV". This status identifiers are described in the section Status IDs of the data points (Page 95).

The "OV" bit of the status identifier of the data point is set as follows when the relevant analog value is transferred:

- Limit value 'high':
  - If the limit value is exceeded: OV = 1
  - If the value then falls below the limit value: OV = 0
- Limit value 'low':
  - If the value falls below the limit value: OV = 1
  - If the value then exceeds the limit value: OV = 0

Configuration of the limit value

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

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

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

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

Note

Evaluation of the value even when the option is disabled

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

To disable the two options, delete the previously configured values limit values from the input boxes and then disable the relevant option.

Recommendation for quickly fluctuating analog values:

If the analog value fluctuates quickly, it may be useful to smooth the analog value first if limit values are configured.

4.10.11 Command outputs

Parameters for command outputs

With the DNP3 and IEC protocols, the following parameters can be configured for command outputs:

- LATCH_ON / LATCH_OFF
- PULSE_ON

The parameters can be configured for the following data point types:

- DNP3

  Binary Command Output
- IEC

  Single command

Configuration

The data point types allow receipt of a command with the following control information (control code):

- LATCH_ON / LATCH_OFF

  or
- PULSE_ON

  When the byte "Control Code" is received with the function "PULSE_ON" information sent with it by the master "Count", "On-time" and "Off-time" is evaluated and compared to the object parameters "Max. pulse duration", "Pulse duration replacement time" and "Max. number of pulses" (see below).

The following control codes sent by the master station are evaluated.

Table 4- 8 Functions of the data object

Receipt of:			Reaction of the object depends on the configuration	
Control Code	TCC *	Op Type **	Output mode = Pulse on	Output mode = Latch on/off
0x01	NUL	PULSE_ON	The output is set to 1 for the duration of “On-time“.	The command is rejected.
0x03	NUL	LATCH_ON	The command is rejected.	The output is set permanently to 1.
0x04	NUL	LATCH_OFF	The command is rejected.	The output is set permanently to 0.
0x41	CLOSE	PULSE_ON	The output is set permanently to 1 (as with LATCH_ON).	The command is rejected.
0x81	TRIP	PULSE_ON	The output is set permanently to 0 (as with LATCH_OFF).	The command is rejected.

* Trip-Close Code field

** Operation Type field

Parameter

Name:	Max. number of pulses
Range of values:	0 ... 255

Default:	0
Explanation:	Monitors the number of pulses sent by the master station (Count). If the number of pulses received from the master station exceeds the value configured here, the command is rejected. If you enter 0 (zero), the monitoring is disabled.

Name:	**Max. pulse duration**
Range of values:	0 ... 65535
Default:	0
Explanation:	Monitors the pulse duration sent by the master (On-time). If the duration of the pulse received from the master exceeds the value configured here, the configurable "Pulse duration replacement time" is used. If the "Pulse duration replacement time" is configured with zero, the command is rejected. With 0 (zero) the "Pulse duration replacement time" is used for every pulse.

Name:	**Pulse duration equivalent time**
Range of values:	0 ... 65535
Default:	0
Explanation:	Replacement value for the pulse duration If the pulse duration received from the master exceeds the value configured in “Max pulse duration“. The parameter is only used when “Max. pulse duration“ is configured. If the value is 0 (zero), no replacement value is used. If the ""Max. pulse duration" and "Pulse duration replacement time" are configured with zero, the command is rejected.

4.10.12 Partner stations

4.10.12.1 Partner configuration for DNP3 and IEC data points

Enabling the partners for data points - DNP3 / IEC

Enable all configured partners with which the selected data point will exchange data. You specify the communications partners of the CP in the "Partner stations" parameter group.

- **Partner 1 enabled**

  In the overview table of the data points, as default Partner 1 is set as the partner of a data point.

  In the "Partner stations" tab, in this case Partner 1 is enabled, the option grayed out.

- **Partner n enabled**

  If you enable a different partner or more partners for this data point in the overview table, these will be enabled in the "Partner stations" tab and all 4 partners can be selected or deselected.

4.10.12.2 Partner configuration with TeleControl Basic data points.

Enabling the partner for data points - TeleControl Basic

Enable the partner with which the selected data point will exchange data.

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

The communications partner may be:

- The telecontrol server

  Since the telecontrol server is always enabled as a communications partner of the CP, it is adopted as default in this tab.

  The option "Telecontrol server enabled" is selected and grayed out.

- An S7 station

  The station must be reachable via the "TeleControl Basic" protocol.

  You specify the communications partners of the CP in the "Partner stations" parameter group.

Activate one of the two options.

- **Telecontrol server enabled**

  Only the telecontrol server is a communications partner of the data point.

- **Partner for inter-station communication**

  Only the S7 station is a communications partner of the data point.

Partner number (inter-station communication)

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

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

Data point index

Index of the corresponding data point on the communications partner.

Note:

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

4.11 Messages

Configuring e-mails

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

For the requirements for using e-mails, see section E-mail configuration (Page 69).

You configure the e-mail in STEP 7 in the editor for the data point and message configuration. You can find this using the project tree:

Project > directory of the relevant station > Local modules > CP

For the view in STEP 7, refer to the section Data point configuration (Page 82).

General functions of the message editor such as copying or column settings correspond to those of the data point editor.

Requirements and necessary information

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

- Configuring the "E-mail configuration" parameter group (see "Security" parameter group)

  To do this, you require the following information:

  – Access data of the SMTP server: Address, port number, user name, password
  – CP's own e-mail address
  – Email address of the recipient

"Message parameter"

Here you configure the recipient, the subject and the text of the message.

"Trigger"

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

- **E-mail trigger**

  Specifies the event for which the sending of the e-mail is triggered.

  – Use PLC tag

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

  – CPU changes to STOP

  – CPU changes to RUN

  – Connection to a partner interrupted

    Triggers the sending of the e-mail when the connection to a partner is interrupted.

  – Connection to a partner established

    Triggers the sending of the e-mail when the connection returns.

  Following triggers only with TeleControl Basic:

  – Connection establishment to partner failed

    Triggers the sending of the e-mail when the connection to a partner could not be established.

  – Teleservice session started

  – Teleservice session ended

- **PLC tag for trigger**

  PLC tag for the e-mail trigger "Use PLC tag"

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

- **Enable identifier for processing status**

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

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

  For the significance of the status output in hexadecimal, refer to the section Processing status of e-mails (Page 126).

- **PLC tag for processing status**

  PLC tag of the type DWORD for the processing status

- **Include value**

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

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

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

- **PLC tag for value**

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

4.12 Access to the Web server

Access to the Web server of the CPU

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

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

For the requirements, refer to the manual /3/ (Page 142).

You will find information on the Web server in the manual /1/ (Page 141).

Program blocks 5

5.1 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

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

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

Note

Different program block versions

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

Supported program blocks for OUC

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

- TSEND_C V3.0 / TRCV_C V3.0

  Compact blocks for:

  – Connection establishment / termination and sending data

  – Connection establishment / termination and reception of data

Use as an alternative:

- TCON V4.0 / TDISCON V2.1

  Connection establishment / connection termination

- TUSEND V4.0 / TURCV V4.0

  Sending and receiving data via UDP

- TSEND V4.0 / TRCV V4.0

  Sending and receiving data via TCP or ISOonTCP

- TMAIL_C V4.0

  Sending e-mails

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

For changing configuration data of the CP during runtime:

- T_CONFIG V1.0

  Program-controlled configuration of the IP parameters

The program block can be found in STEP 7 in the "Instructions > Communication > Open User Communication" window.

Connection descriptions in system data types (SDTs)

For the connection description, the blocks listed above use the parameter CONNECT (or MAIL_ADDR_PARAM with TMAIL_C). The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

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

You generate the SDT type by entering the name e.g. "TCON_Param" in the "Data type" box manually in the declaration table of the block instead of selecting an entry from the "Data type" drop-down list. The corresponding SDT is then created with its parameters.

Using the SDT

- TCON_IP_v4

  For transferring frames via TCP

- TADDR_Param

  For transferring frames via UDP

- TCON_IP_RFC

  For transferring frames via ISO-on-TCP (direct communication between two S7-1200 stations)

- TMail_V4

  For transferring e-mails addressing the e-mail server using an IPv4 address

- TMail_V6

  For transferring e-mails addressing the e-mail server using an IPv6 address

- TMail_FQDN

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

- TMail_V4_SEC

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

- TMail_V6_SEC

  For secure transfer of e-mails addressing the e-mail server using an IPv6 address

- TMail_QDN_SEC

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

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

Connection establishment and termination

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

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

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

Note

Connection abort

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

5.2 Changing the IP address during runtime

Changing the IP address during runtime

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

- IP address
- Subnet mask
- Router address

Note

Changing the IP parameters with a dynamic IP address

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

Requirements - firmware version

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

- CP firmware ≥ V2.1.7x

  and

- CPU firmware ≥ V4.2

Requirements - program blocks / STEP 7 versions

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

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

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

- STEP 7 Basic ≥ V14

  T_CONFIG

  Along with:

  – IF_CONF_V4
  – IF_CONF_NTP
  – IF_CONF_V6
  – IF_CONF_DNS

- STEP 7 Basic ≤ V14

  TC_CONFIG

  Along with:

  – IF_CONF_V4

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

Requirements - CP programming

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

Diagnostics and upkeep

6

6.1 Diagnostics options

The following diagnostics options are available.

LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 26).

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

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

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

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

If you want to operate online diagnostics with the station via the CP, you need to activate the online functions in the parameter group "Communication types" see the section Communication types (Page 45).

"Diagnostics" group

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

- General information on the module

  General information on the module
- Diagnostics status

  Information on the diagnostics status
- Ethernet interface

  Address and statistical information

- Industrial Remote Communication

  Here, you obtain specific information on the WAN interface and other parameters of the CP. The entry has the following subentries:

  – Partner

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

  – Data point list

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

  – Protocol diagnostics

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

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

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

  – Device-specific events

    Information on CP-internal events

- Time

  Information on the time on the device

"Functions" group

- Saving service data

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

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

STEP 7: The partner status

The CP can signal the status of the connection to the communications partner to the CPU via a PLC tag. You can display the status of the PLC tag via the Web server of the CPU

For information on the configuration, refer to the section Partner stations (Page 54).

Web server of the CPU

Via the CP you can access the Web server of the CPU and the information available there. For access, refer to the section Access to the Web server (Page 115).

SNMP

For information on the functions, refer to the section SNMP (Page 125).

6.2 Online security diagnostics via port 8448

Security diagnostics without opening port 102

If you want to perform security diagnostics without opening port 102, follow the steps below:

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

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

See also

Settings for online security diagnostics and downloading to station with the firewall activated (Page 68)

6.3 Online functions and TeleService

Online functions and TeleService

Along with STEP 7 on the engineering station (ES) the CP provides various diagnostics and maintenance functions under the following terms:

- Online functions

  Access from the ES to the station via LAN

  Requirement: The ES and the CP are located in the same subnet.

- TeleService

  Access from the ES to the station via WAN (Internet)

  Requirement: The CP is connected to the telecontrol server and can be reached via this path Refer to the information in section Access to the Web server (Page 115).

  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.

  Connections between a CP and telecontrol server for transferring user data are not interrupted by a TeleService-connection.

The functions and the connection establishment are largely the same with the online functions and TeleService.

Note

Transmission time with TeleService

Note that transferring larger amounts of data via WAN (Internet) can take a very long time.

If there are disruptions or interruptions of the transmission path this can lead to the data transmission being aborted.

Connection establishment to use the online functions via Ethernet

Procedure:

1. Connect the ES to the network.
2. Open the relevant STEP 7 project on the ES.
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, go to the Choose the entry "TeleService via telecontrol" in the "Type of PG/PC interface" drop-down list.
6. In the "PG/PC interface" drop-down list select the entry "TeleService board".
7. In the table select the CP if it is not already selected.

   The path both via the CP or the CPU is possible.
8. Click on the icon next to the "PG/PC interface" drop-down list.

   The "Establish remote connection via telecontrol" dialog box opens.
9. Make the necessary entries in this dialog (see below) and click on "Connect".

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

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

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

  Selection whether the TeleService switching station is located on the PC of the engineering station or in the network or can be reached via the Internet.

  A TeleService gateway cannot be used as a switching station only the telecontrol server.

  – Enter the address of the telecontrol server.

    IP address or name and port number of the telecontrol server that can be resolved by DNS

  – Own server password

    Enter the telecontrol password to authenticate the CP with the telecontrol server

    The telecontrol password for the CP is configured under "CP identification" in the security settings, see also the section CP iIdentifcation with the TeleControl Basic protocol (Page 64).

- **Authentication ...**
  - Teleservice user name and password

    Here, enter the data for the TeleService user that you configured in STEP 7 in the global Security settings, see also section Configuration of the TeleService access (Page 80).

Terminate online connection

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

6.4 SNMP

SNMP (Simple Network Management Protocol)

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

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

Range of performance of the CP as an SNMP agent

The CP supports data queries in the following SNMP versions:

- SNMPv1 (standard)
- SNMPv3 (Security)

It returns the contents of MIB objects of the standard MIB II according to 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
  - ICMP
  - TCP
  - UDP
  - SNMP

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

For more detailed information about the MIB files and SNMP, refer to the manual /5/ (Page 142).

Configuration

For information on the configuration, refer to:

- With security functions disabled (SNMPv1): SNMP (Page 53)
- With security functions enabled (SNMPv1 / SNMPv3): SNMP (Page 70)

6.5 Processing status of e-mails

Configuration of the processing status of e-mails

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

For information on the configuration, refer to the section Messages (Page 113).

Outputting the processing status of e-mails

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

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

Processing status of e-mails

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

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

Status	Meaning
0000	Transfer completed free of errors
82xx	Other error message from the e-mail server Apart from the leading "8", the message corresponds to the three-digit error number of the SMTP protocol.
8401	No channel available. Possible cause: There is already an e-mail connection via the CP. A second connection cannot be set up at the same time.
8403	No TCP/IP connection could be established to the SMTP server.
8405	The SMTP server has denied the login request.
8406	An internal SSL error or a problem with the structure of the certificate was detected by the SMTP client.
8407	Request to use SSL was denied.
8408	The client could not obtain a socket for creating a TCP/IP connection to the mail server.
8409	It is not possible to write via the connection. Possible cause: The communications partner reset the connection or the connection aborted.
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.

6.6 Downloading firmware

New firmware versions of the CP

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

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

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

When you have saved the new firmware file on your engineering station (ES), the following methods are available to you for loading the firmware file:

- Saving the firmware file on the memory card of the CPU (recommended method)

  You will find a description of the procedure in the S7-1200 system manual.
- Loading the firmware with the online functions of STEP 7 via Ethernet

  You will find a description of connecting the ES to the station in the section Online functions and TeleService (Page 123).
- Downloading the firmware via the Web server of the CPU (as of CPU firmware version V4.0)

  This method is described below.

Note

Effects on the retentive memory of the CPU

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

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 ES and to download the CP's new firmware file to the station.

Requirements in the network configuration

- The CP is connected to the telecontrol server and can be reached via this path

  Refer to the information in section Access to the Web server (Page 115).

Requirements in the CPU configuration

1. Open the corresponding project on the ES.
2. Select the CPU of the station involved in STEP 7.
3. Select the "Web server" entry.

4. In the parameter group "General", select the "Enable Web server for this interface" option.
5. With a CPU version V4.0 or higher, create a user in the user administration with the required rights.

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

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

- Connection establishment with HTTP

  Procedure if the "Allow access only using HTTPS" option is disabled
- Connection establishment with HTTPS

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

These two variants are described in the following sections.

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

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

Connection establishment with HTTP

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

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

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

   The certificate is loaded on your PC.

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

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

Connection establishment with HTTPS

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

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

Loading firmware

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

   Use the user data configured in the user administration of the Web server of the CPU.
2. After logging in, select the entry "Module status" in the navigation panel of the Web server.
3. Select the CP in the module list.
4. Select the "Firmware" tab lower down in the window.
5. Browse for the firmware file on your PC using the "Browse..." button and download the file to the station using the "Run update" button.

Note

Closing the Web server

If you close the Web server during the firmware update, you cannot change the operating status of the CPU to RUN. In this case you need to turn the CPU off and on again to change the CPU to the operating status RUN.

6.7 Module replacement

Module replacement

CAUTION

Read the system manual "S7-1200 Programmable Controller"

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

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

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

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

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

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 °C to +70 °C
	During transportation	-40 °C to +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Design, dimensions and weight		
Module format	Compact module for S7-1200, single width	
Degree of protection	IP20	
Weight	122 g	

Technical specifications	
Dimensions (W x H x D)	30 x 110 x 75 mm
Installation options	Standard DIN rail Switch panel
Product functions **	

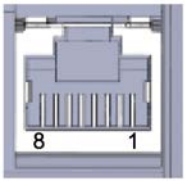
* For details, refer to the IK PI catalog, cabling technology
**You will find further characteristics and performance data in the section Application and properties (Page 11).

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

Approvals issued

Note

Issued approvals on the type plate of the device

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

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

EC declaration of conformity

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

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

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

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

  EMC directive of the European Parliament and of the Council of February 26, 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility.; official journal of the EU L96, 29/03/2014, pages. 79-106

- **2011/65/EU (RoHS)**

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

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

Siemens Aktiengesellschaft
Division Process Industries and Drives
Process Automation
DE-76181 Karlsruhe
Germany

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

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

IECEx

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

IECEx classification: Ex nA IIC T4 Gc

IECEx certificate: IECEx DEK 14.0088X

The CP meets the requirements of the following standards:

- EN 60079-0

  Hazardous areas - Part 0: Equipment - General requirements

- EN 60079-15

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

You can see the current versions of the standards in the IECEx certificate that you will find on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15922/cert)

The conditions must be met for the safe deployment of the CP according to the section Notices on use in hazardous areas according to IECEx / ATEX (Page 32).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find on the Internet at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013)

ATEX

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

ATEX approval: II 3 G Ex nA IIC T4 Gc

Type Examination Certificate: KEMA 10ATEX0166 X

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 31)
- The installation instructions in the document /1/ (Page 141)

Note the conditions for the safe deployment of the CP according to the section Link: (https://support.industry.siemens.com/cs/ww/en/ps/15922/cert).

You should also note the information in the document "Use of subassemblies/modules in a Zone 2 Hazardous Area" that you will find on the Internet at the following address: Link: (https://support.industry.siemens.com/cs/ww/en/view/78381013)

c(UL)us

Applied standards:

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

File Number: E223122

cULus Hazardous (Classified) Locations

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

Applied standards:

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

APPROVED for Use in:

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

Report / UL file: E223122 (NRAG.E223122)

Note the conditions for the safe deployment of the CP according to the section Notices regarding use in hazardous areas according to UL HazLoc (Page 33).

FM

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

Equipment rating:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

Report Number: 3049779, 3049925

Note the conditions for the safe deployment of the CP according to the section Notices on use in hazardous areas according to FM (Page 33).

Australia - RCM

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

EAC (Eurasian Conformity)

Customs union of Russia, Belarus and Kazakhstan

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

Current approvals

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

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

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

Dimension drawings

B

Note

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

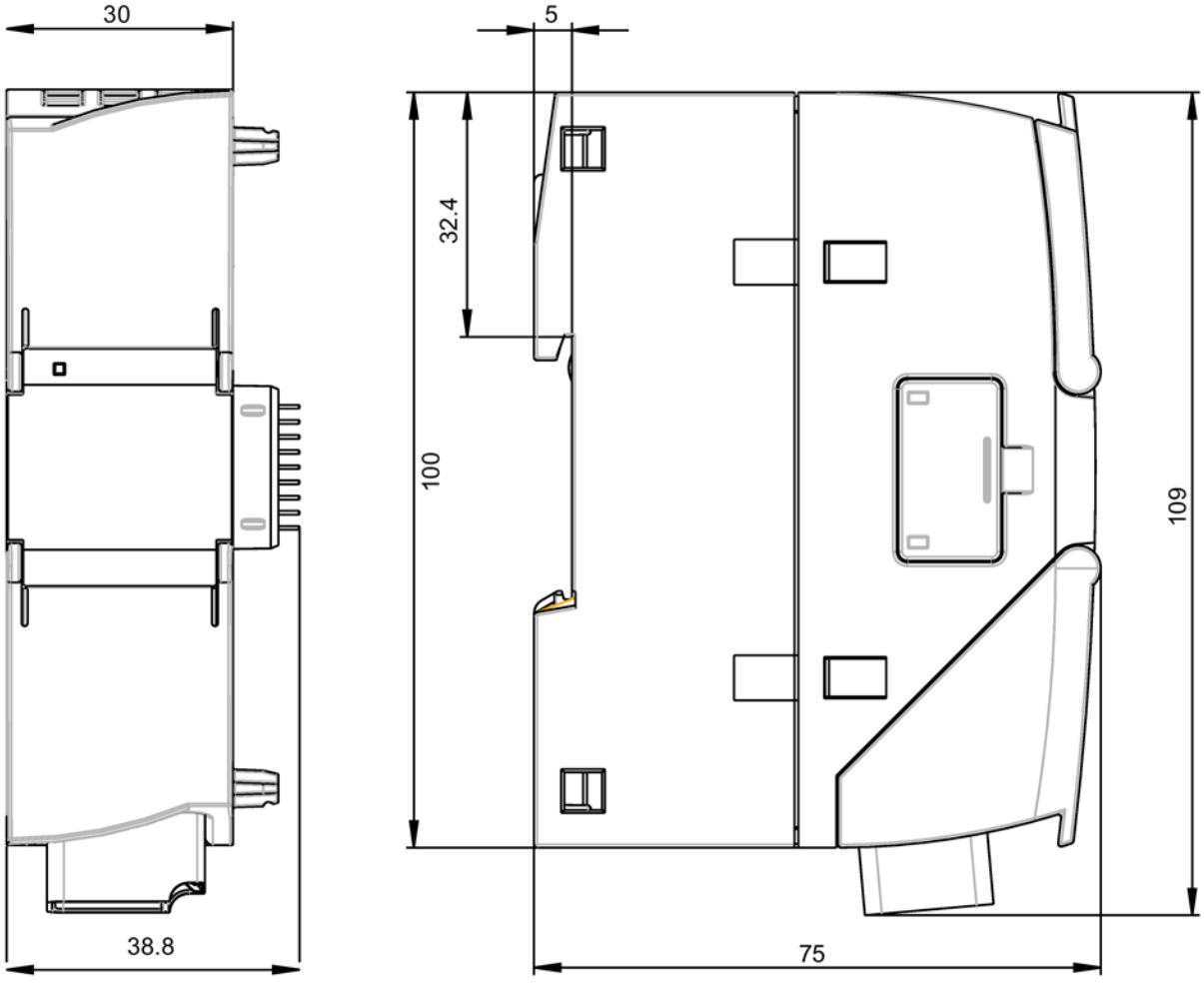


Figure B-1 Front view and side view left

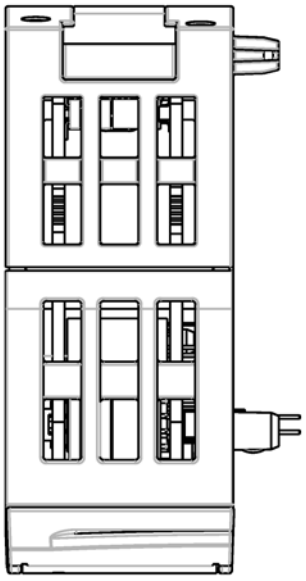


Figure B-2 From above

Documentation references

C

Where to find Siemens documentation

- Article numbers

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

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

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

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

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

- Manuals on the Internet

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

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

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

  Entry type “Manuals”

- Manuals on the data medium

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

/1/

SIMATIC
S7-1200 Programmable Controller
System Manual
Siemens AG
Current release at the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/13683/man)

/2/

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

/3/

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

/4/

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

/5/

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

Index

A

Abbreviations/acronyms, 4
Article number, 3

C

Conditional spontaneous, 100, 101
Connection resources, 15
CPU firmware, 23
Cross references (PDF), 5

D

Data buffering, 16
Data point configuration, 82
Data point type, 89
Dimensions, 35
Disposal, 6
DNP3 addressing, 41
DNP3 implementation level, 65
DNP3 master, addressing via the Internet, 21
DNS server, 42
DNS server - program-controlled change, 119

E

E-mail
    Configuration, 113
    Programming (OUC), 117
    Quantity, 16
Encryption, 11
Ethernet interface
    Assignment, 134
Events, 98

F

Firewall, 14
Firmware version, 3
Forced image mode, 98
Frame memory, 16, 98

G

Gateway, 79
Glossary, 6

H

Hardware product version, 3

I

IEC addressing, 41
Image memory, 98
Importing a certificate - e-mail, 70
Instructions (OUC), 117
Internet connections, 42
Inter-station communication, 94
IP address - program-controlled change, 119
IP address (master), 41
IP configuration
    IPv4, IPv6, 12
IP_CONF_V4, 119

L

Logging server, 73

M

MAC address, 3
MIB, 125
Mirroring, 92

N

NTP, 43
NTP (secure), 43
NTP server - program-controlled change, 119
IPsec tunnel,

O

Online diagnostics, 46, 121
Online functions, 13, 121

OPC quality code, 95
Operating statuses (LED displays), 28
OUC (Open User Communication), 117
OUC connections
    Resources, 16

P

Passive VPN connection establishment, 79
PG/OP connections, 16
Port 8448, 123
Process image, 98
Product name, 4
PUT/GET, 16

R

Recycling, 6
Redundant DNP3 master, addressing, 22
Replacing a module, 132
Reset trigger bit, 99

S

S7 connections
    Enable, 46
    Resources, 16
Safety notices, 31
Security, 13
Security diagnostics without port 102, 123
Send buffer, 16, 98
Service & Support, 6
SIMATIC NET glossary, 6
SMS
    Programming (OUC), 117
SMTPS, 69
SNMP, 13, 53, 125
SNMPv3, 15, 70
SSL/TLS, 69
STARTTLS, 69
Static values, 98
STEP 7 - version, 23
SYSLOG, 80

T

T_CONFIG, 119
TC_CONFIG, 119
TeleService, 13
Time stamp, 90
Time-of-day synchronization, 12
Training, 6
Transmission mode, 100, 101
Trigger tag - resetting, 100

U

Unsolicited, 100, 101

V

Virtual IP address, 57
VPN, 16, 42, 74

W

Web server, 115