SIEMENS

SIMATIC NET

ET 200SP - Industrial Ethernet CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1

Operating Instructions

Preface

Application and functions 1

LEDs and connectors 2

Installation and connecting up 3

Configuration and operation 4

Programming (OUC) 5

Diagnostics and maintenance 6

Technical specifications 7

Approvals A

Dimension drawings B

Accessories C

Documentation references D

01/2017

C79000-G8976-C426-03

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-C426-02
℗ 01/2017 Subject to change

Copyright © Siemens AG 2016.
All rights reserved

Preface

Validity of this manual

This document contains information on the following modules:

- **CP 1542SP-1**
  Article number **6GK7542-6UX00-0XE0**
  Hardware version 1
  Firmware version V1.0
  Communications processor for connecting a SIMATIC ET 200SP CPU to Industrial Ethernet
- **CP 1542SP-1 IRC**
  Article number **6GK7542-6VX00-0XE0**
  Hardware version 1
  Firmware version V1.0
  Communications processor for connecting a SIMATIC ET 200SP CPU via Industrial Ethernet to a control room (TCSB, DNP3, IEC 60870-5-104)
- **CP 1543SP-1**
  Article number **6GK7543-6WX00-0XE0**
  Hardware version 1
  Firmware version V1.0
  Communications processor for connecting a SIMATIC ET 200SP CPU to Industrial Ethernet, Security



Figure 1 CP 1542SP-1 with plugged in bus adapter (here 2xRJ-45)

On the front of the module at the right edge, the hardware version is 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.

Directly below, you will find the firmware version of the CP as it shipped.

The MAV address is printed on the front at the bottom left, above the connectors for the power supply.

Product names, terms and abbreviations/acronyms

Below you will find terms and abbreviations/acronyms used often in this manual.

- **CP**

  When the property being described is valid in the current context for all three CP types or if the CP type being used is clear from the context, the abbreviation "CP" will be used instead of the three following product designations

  – CP 1542SP-1

  – CP 1542SP-1 IRC

  – CP 1543SP-1

  If information applies only to a certain product variant. the full module name is specified.

- **TCSB**

  Control center software "TeleControl Server Basic"

- **Telecontrol server**

  PC with installed software "TeleControl Server Basic"

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.

Required experience

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

- Automation engineering
- Setting up the SIMATIC ET 200SP
- SIMATIC STEP 7 Professional

New in this issue

Editorial revision (MSIP approval)

Replaced edition

Release 11/2016

Current manual release on the Internet

You will also find the current version of this manual on the Internet pages of Siemens Industry Online Support under at the following addresses:

- CP 1542SP-1 / CP 1543SP-1
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/22144/man)
- CP 1542SP-1 IRC
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man)

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

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_CP-ET200SP_86.pdf

Security information

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

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

Firmware

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

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following address:

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

Training, Service & Support

You will find information on training, service and support in the multilanguage document "DC_support_99.pdf" on the Internet pages of Siemens Industry Online Support:

Link: (https://support.industry.siemens.com/cs/ww/en/view/38652101)

Table of contents

Preface **3**

1 Application and functions **11**

1.1 Components of the product 11

1.2 Application 11

1.3 Communications services 12

1.4 Telecontrol communication of the CP 1542SP-1 IRC 13

1.5 Other services and properties 14

1.6 Security functions (CP 1542SP-1 IRC, CP 1543SP-1) 15

1.7 Configuration limits and performance data 17

1.8 Requirements for use 19
1.8.1 Hardware requirements 19
1.8.2 Software requirements 20

1.9 Configuration examples 20

2 LEDs and connectors **25**

2.1 LEDs 25

2.2 Power supply 26

2.3 Connector for the BusAdapter 27

3 Installation and connecting up **29**

3.1 Important notes on using the device 29
3.1.1 Notes on use in hazardous areas 29
3.1.2 Notes on use in hazardous areas according to ATEX / IECEx 31
3.1.3 Notes on use in hazardous areas according to UL HazLoc 31
3.1.4 General notices on use in hazardous areas according to FM 32

3.2 Installing the CP 32

3.3 Connecting the CP 36

4 Configuration and operation **39**

4.1 Security recommendations 39

4.2 Configuration in STEP 7 42

4.3 Ethernet interface 43
4.3.1 IPv6 43
4.3.2 Time-of-day synchronization 43

4.4 SNMP 45

4.5 Telecontrol communication (CP 1542SP-1 IRC) 45
4.5.1 Configuration 45

4.5.2 Communication types ... 46
4.5.3 Address and authentication information ... 47
4.5.4 Ethernet interface (X1) > Advanced options ... 48
4.5.5 Partner stations ... 52
4.5.5.1 Partner configuration ... 52
4.5.5.2 Addressing of single and redundant communications partners ... 55
4.5.5.3 Partner for inter-station communication ... 55
4.5.6 Communication with the CPU ... 56
4.5.7 Data point configuration ... 57
4.5.7.1 Configuring the data points ... 57
4.5.7.2 Datapoint types ... 59
4.5.7.3 Process image, types of transmission, event classes, triggers ... 63
4.5.7.4 Status IDs of the data points ... 67
4.5.7.5 Rules for configuring the data point index: ... 69
4.5.7.6 Read cycle ... 70
4.5.7.7 "Trigger“ tab ... 71
4.5.7.8 Threshold value trigger ... 73
4.5.7.9 Analog value preprocessing ... 74
4.5.8 Message configuration ... 81
4.5.9 Security > CP identification ... 83
4.5.10 Security > DNP3 security options ... 83
4.5.11 Security > E-mail configuration ... 86

4.6 Security configuration(CP 1543SP-1) ... 86
4.6.1 VPN ... 86
4.6.1.1 VPN (Virtual Private Network) ... 86
4.6.1.2 Creating a VPN tunnel for S7 communication between stations ... 88
4.6.1.3 VPN communication with SOFTNET Security Client (engineering station) ... 90
4.6.1.4 Establishment of VPN tunnel communication between the CP and SCALANCE M ... 90
4.6.1.5 CP as passive subscriber of VPN connections ... 90
4.6.2 Firewall ... 91
4.6.2.1 Pre-check of messages by the MAC firewall. ... 91
4.6.2.2 Online diagnostics and downloading to station with the firewall activated ... 91
4.6.2.3 Notation for the source IP address (advanced firewall mode) ... 92
4.6.2.4 Firewall settings for S7 connections via a VPN tunnel ... 92
4.6.3 Filtering of the system events ... 92

4.7 Table "Certificate manager" (CP 1542SP-1 IRC, CP 1543SP-1) ... 92

5 Programming (OUC) ... 95

5.1 Program blocks for OUC ... 95

6 Diagnostics and maintenance ... 99

6.1 Diagnostics options ... 99

6.2 Diagnostics with SNMP ... 100

6.3 Web server of the CPU ... 102

6.4 Processing status of the telecontrol e-mails ... 104

6.5 Downloading firmware ... 106

6.6 Module replacement ... 108

7 Technical specifications ... 109

A Approvals 111
B Dimension drawings 115
C Accessories 117
C.1 BusAdapter 117
C.2 Assignment of the Ethernet interface of the bus adapter 118
D Documentation references 119
Index 121

Application and functions

1

1.1 Components of the product

The following components are supplied with the product:

- CP 154xSP-1
- Plug for the socket of the power supply (24VDC) of the CP
- DVD with documentation and license texts

A BusAdapter for the Ethernet connection of the CP does not ship with the product.

1.2 Application

Application of the CP variants

The CP is used to connect the ET 200SP to Industrial Ethernet via a copper cable or fiber-optic cable. It can be used as an additional Ethernet interface of the CPU for S7 communication.

For the Ethernet connection, the CP requires a bus adapter that does not ship with the product.

The three CP variants are intended for the following communication tasks:

- **CP 1542SP-1**

  The CP 1542SP-1 allows the ET 200SP a further Ethernet connection.

- **CP 1542SP-1 IRC**

  The CP 1542SP-1 IRC supports telecontrol communication for connecting the ET 200SP CPU to a control center. The following telecontrol protocols can be used as alternatives:

  – TeleControl Basic

    For connection of the ET 200SP to a master station with telecontrol server (TCSB V3 SP3)

  – DNP3

    For connection of the ET 200SP to a master station with DNP3 masters

  – IEC 60870-5-104

    For connection of the ET 200SP to a master station with IEC masters

- **CP 1543SP-1**

  The CP 1543SP-1 has Security functions for network security, such as a firewall and VPN. This makes protected access to the ET 200SP possible.

1.3 Communications services

Communications services

The following communications services are supported:

- **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)

  For S7 communication, the CP requires a fixed IP address.
- **S7 routing**
  - Routing of S7 connections via the backplane bus and the CPU to other S7 stations
- **Open User Communication (OUC)**

  OUC via program blocks with the following protocols:
  - TCP/IP
  - ISO-on-TCP
  - UDP

  The CP 1543SP-1 supports Secure OUC.

  You will find the program blocks supported by the three CP types in the section Programming (OUC) (Page 95).
- **E-mail using program blocks**
- **HTTP / HTTPS**

  Via HTTP / HTTPS you can access the Web server of the CPU.

For telecontrol communication of the CP 1542SP-1 IRC, see section Telecontrol communication of the CP 1542SP-1 IRC (Page 13).

For information on the Security functions of the CP 1543SP-1, refer to the section Security functions (CP 1542SP-1 IRC, CP 1543SP-1) (Page 15).

1.4 Telecontrol communication of the CP 1542SP-1 IRC

Telecontrol protocols

In addition to the communications services named above, the CP 1542SP-1 IRC supports the following telecontrol protocols for communication with a master station:

- **TeleControl Basic**

  This is a proprietary protocol of Siemens for telecontrol applications. The IP-based protocol is used to connect the CP to the application TCSB.

  TCSB is installed on a PC in the master station, the telecontrol server. Via the OPC-DA or OPC-UA server of TCSB, an OPC client can access the process data of the CP.

  TCSb is supported as of the following version: V3.0 + SP3

  For the TCSB manual, see /3/ (Page 120).

- **DNP3**

  The CP functions as a DNP3 station (Outstation).

  Communication is based on the DNP3 SPECIFICATION Version 2.11 (2007/2009).

  You will find a detailed overview of the attributes and properties specified in the DNP3 protocol and supported by the CP in the DNP3 device profile, see Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man).

  You will find the supported object groups and variations in the section Datapoint types (Page 59).

  Communications partner (DNP3) can be:

  – SIMATIC PCS7 TeleControl
  – SIMATIC WinCC TeleControl
  – SIMATIC WinCC OA
  – A TIM module with DNP3 capability (TIM 3V IE DNP3 / TIM 4R IE DNP3)

    For the manual of the TIM module see /5/ (Page 120).
  – Third-party systems that support the DNP3 specification named above.

- **IEC 60870-5-104**

  The CP functions as a substation (slave).

  Communication is based on the specification IEC 60870-5 Part 104 (2006).

  You will find a detailed overview of the attributes and properties specified in the IEC specification and supported by the CP in the IEC device profile, see Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man).

  You will find the supported IEC type identifiers as in the section Datapoint types (Page 59).

  Communications partner (IEC master) can be:

  – SIMATIC PCS7 TeleControl
  – SIMATIC WinCC TeleControl

- SIMATIC WinCC OA
- Third-party systems that support the DNP3 specification named above.

Properties of the telecontrol CP

- **Data point configuration**

  The process values are configured as data points for the communication. The data points access PLC tags in the CPU. The data points can be processed one-to-one in the control system.

- **Messages / e-mail**

  With configurable events in the process image of the CPU, the CP 1542SP-1 IRC can send messages as e-mails. The data sent by e-mail is configured using PLC tags.

- **Storage of events**

  The CP 1542SP-1 IRC can store events of different classes and transfer them together to the communications partner.

- **Analog value processing**

  Analog values can be preprocessed on the CP 1542SP-1 IRC according to various methods.

1.5 Other services and properties

Further services and properties of the CP

- **IP configuration**
  - Address types

    The CP supports IP addresses according to IPv4 and IPv6.
  - Addressing

    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 using program blocks.
  - DHCP: As an alternative, the IP address can be obtained from a DHCP server.
  - DCP (Discovery and Configuration Protocol) is supported.
- **Time-of-day synchronization**
  - NTP

    On the Ethernet interface, the CP can synchronize its time of day via NTP.

– Only CP 1542SP-1 IRC

When telecontrol communication is enabled, the CP always obtains its local time of day as UTC time from the communications partner. The time of day of the CP can be read by the CPU using a PLC tag. For information on the format of the time stamp of the data frames, refer to the section Datapoint types (Page 59).

If telecontrol communication is disabled, the CP can synchronize its time of day via NTP.

– Only CP 1543SP-1

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

For more information, refer to the section Time-of-day synchronization (Page 43).

- **SNMP**

  As SNMP agent, the CP supports queries via SNMPv1.

  The CP 1543SP-1 also supports SNMPv3.

  For more detailed information, refer to section SNMP (Page 45).

1.6 Security functions (CP 1542SP-1 IRC, CP 1543SP-1)

The Security functions described below are enabled in the configuration for the relevant CP.

For information on the Securityfunctions of Open User Communication, refer to the section Programming (OUC) (Page 95).

Note

Recommendation for critical security plants

Refer to the information in the section Security recommendations (Page 39).

Security functions of the CP 1542SP-1 IRC

- **E-mail**

  For secure transfer of information with encrypted e-mails you have the alternative of using:

  – SSL/TLS

  – STARTTLS

  For information on the configuration, refer to the section Security > E-mail configuration (Page 86).

- **Certificates**

  For the secure authentication of the communications partners, certificates are used.

- **Secure telecontrol communication**

  The telecontrol protocols provide the following Security functions:

  – TeleControl Basic

    As an integrated security function, the telecontrol protocol encrypts the data for transfer between the CP and telecontrol server. The interval for the key exchange between CP and telecontrol server is set to 1 hour.

    The telecontrol password is used to authenticate the CP with the telecontrol server

  – DNP3

    The CP supports the Security mechanisms listed in the specification.

Security functions of the CP 1543SP-1

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. The data transfer via the CP 1543SP-1 can be protected from the following attacks by a combination of different security measures:

- Data espionage
- Data manipulation
- Unauthorized access

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

As a result of using the CP, as a security module, the following security functions are accessible to the ET 200SP station on the interface to the Ethernet network:

- **Firewall**

  The firewall protects the device with:

  – 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")

- **Certificates**

  For the secure authentication of the communications partners, certificates are used.

- **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.

- **Logging**

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

- **NTP (secure)**

  For secure transfer during time-of-day synchronization

- **SNMPv3**

  For secure transmission of network analysis information safe from eavesdropping

For information on configuring the security functions, refer to the section Security configuration(CP 1543SP-1) (Page 86).

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 120).

1.7 Configuration limits and performance data

Number of CPs per station

In each ET 200SP station, up to three special modules can be plugged in and configured; this allows a maximum of two CP 154xSP-1 modules.

For details of the permitted special modules and the slot rules, refer to section Installing the CP (Page 32).

Connection resources

Number of connections via Industrial Ethernet in total maximum of 32,
of which:

- S7: Max. 16
- TCP/IP: Max. 32
- ISO-on-TCP: Max. 32
- UDP: Max. 32

Also:

- Online connections of the engineering station (STEP 7): Max. 2
- TCP connections for HTTP

  For HTTP access upp to 12 TCP connection resources are available that are used by one or more Web browsers to display data of the CP.
- PG/OP connections (HMI): In total maximum of 16,
  of which:
  - Connection resources for PG connections: Max. 16
  - Connection resources for OP connections: Max. 16

Frame memory (send buffer)

Only CP 1542SP-1 IRC

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

The volume of the send buffer is divided equally among all configured communications partners.

The size of the send buffer can be configured in STEP 7, refer to the section Communication with the CPU (Page 56).

The maximum size of the send buffer depends on the telecontrol protocol being used and is as follows:

- TeleControl Basic

  64000 events

- DNP3

  100000 events

- IEC 60870-5-104

  100000 events

You will find details of how the send buffer works such as storing events as well as the options for transferring the data in the section Process image, types of transmission, event classes, triggers (Page 63).

E-mail (via message editor)

Only CP 1542SP-1 IRC

With telecontrol communication enabled, up to 10 messages can be configured in STEP 7. The messages are sent as e-mails.

Telecontrol connections and data points

Only CP 1542SP-1 IRC

- **Telecontrol connections**
  - TeleControl Basic

    A connection can be established to a single or redundant telecontrol server.
  - DNP3

    Connections to up to four masters can be established.
  - IEC 60870-5-104

    Connections to up to four masters can be established.
- **Data points**

  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 59).

  The maximum number of configurable data points is 500.

  In the allocation of the internal CP memory for data points, the length of the data point name is also included. See also the note in section Configuring the data points (Page 57).

Security functions

Only CP 1543SP-1

- **VPN tunnel**

  A maximum of four VPN tunnels 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")

1.8 Requirements for use

1.8.1 Hardware requirements

Bus adapter

To connect to the Ethernet network, the CP requires a BusAdapter. A BusAdapter does not ship with the CP.

The CP supports the following BusAdapter:

- BA 2xRJ45
- BA 2xFC
- BA 2xSCRJ
- BA SCRJ/RJ45
- BA SCRJ/FC

For more detailed information on the bus adapters, refer to the section BusAdapter (Page 117) and the manual /2/ (Page 119).

CPUs and other components of the ET 200SP

The CP supports operation in stations that contain one of the following CPUs:

- CPU 1510SP-1 PN

  Article number: 6ES7510-1DJ01-0AB0

- CPU 1510SP F-1 PN

  Article number: 6ES7510-1SJ01-0AB0

- CPU 1512SP-1 PN

  Article number: 6ES7512-1DK01-0AB0

- CPU 1512SP F-1 PN

  Article number: 6ES7512-1SK01-0AB0

Further parts and modules that are also required to set up the ET 200SP station, such as rails, I/O modules or cabling are not listed here. See also /2/ (Page 119) for information on this.

Components of the communications partner

Components required by the communications partners of the CP 1542SP-1 IRC are not listed here. You will find references to other products (e.g. TCSB) in the list of references in the appendix of the manual.

1.8.2 Software requirements

Configuration software

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

- STEP 7 Professional as of version 14.

Software for online functions

To use the online functions, the following software is required:

- STEP 7 in the version specified above

CPU firmware

To use the CP, a CPU 151xSP with a firmware version ≥ V2.0 is required.

Telecontrol protocols (CP 1542SP-1 IRC)

You will find telecontrol protocols supported by the CP in the section Telecontrol communication of the CP 1542SP-1 IRC (Page 13).

1.9 Configuration examples

Below you will find configuration examples for the use of the three CP variants.

CP 1542SP-1 - Network separation

The CP is used in the ET 200SP to operate lower-level networks separately or to achieve separation from the higher-level network.

The ET 200SP can be expanded flexibly with further Ethernet interfaces via the CP. The network separation allows the setting up of identical machines with the same IP address. The CP takes over the communication and relieves the CPU.

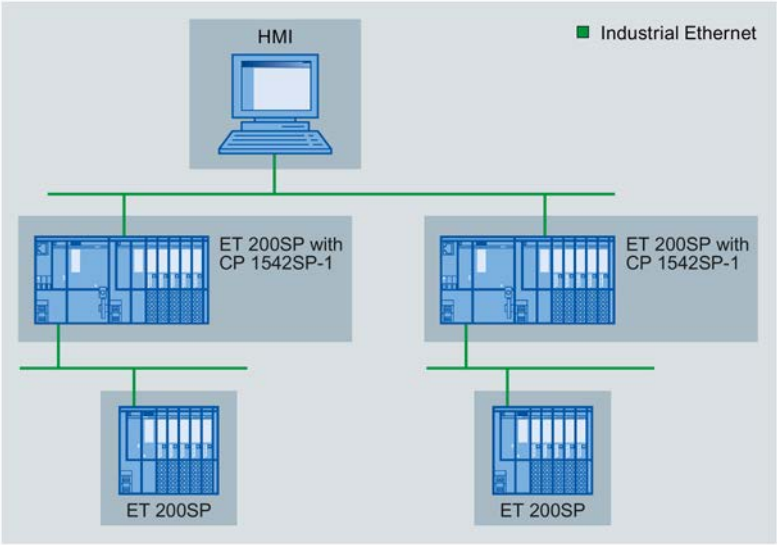


Figure 1-1 Configuration example of an ET 200SP with CP 1542SP-1

CP 1543SP-1 - Cell protection with Security functions

The CP communicates encrypted with communications partners in the connected network. The firewall monitors the access to the ET 200SP and therefore protects lower-level networks. This avoids data loss, disruptions of production and damage to machines.

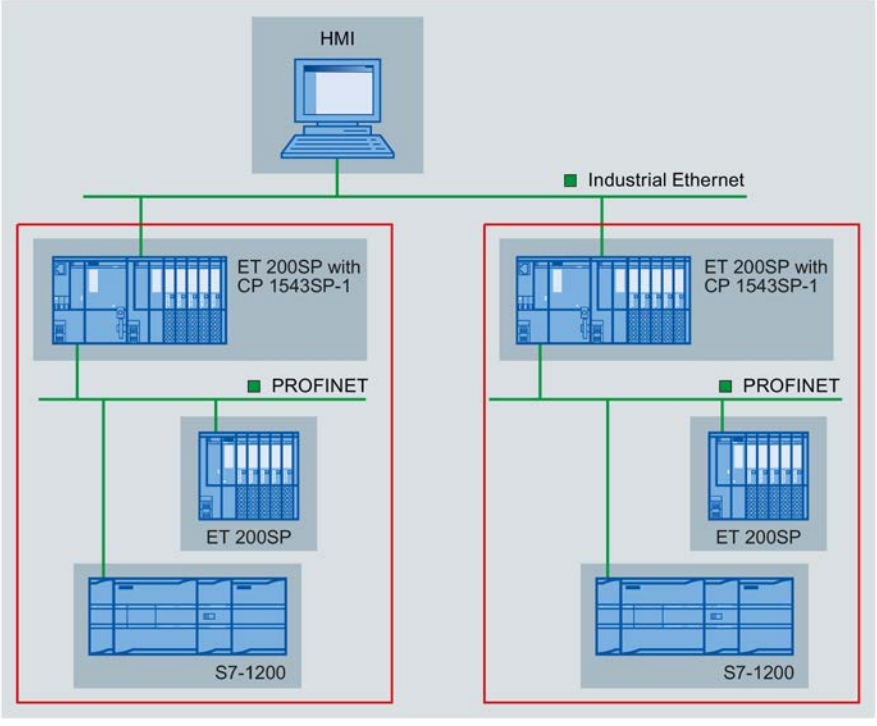


Figure 1-2 Configuration example of an ET 200SP with CP 1543SP-1

CP 1542SP-1 IRC - Connection to control centers

By using the CP the ET 200SP can be used as a remote terminal unit. For the communication, the following telecontrol protocols can be used:

- TeleControl Basic

  The Siemens telecontrol protocol for connection to master stations with TCSB
- IEC 60870-5-104
- DNP3

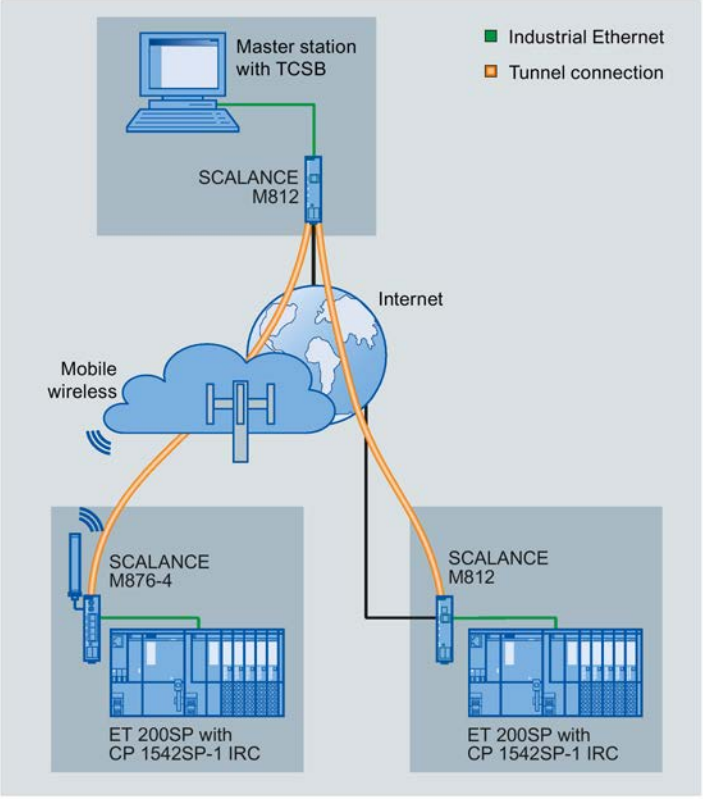


Figure 1-3 Configuration example of an ET 200SP with CP 1542SP-1 IRC; protocol: TeleControl Basic

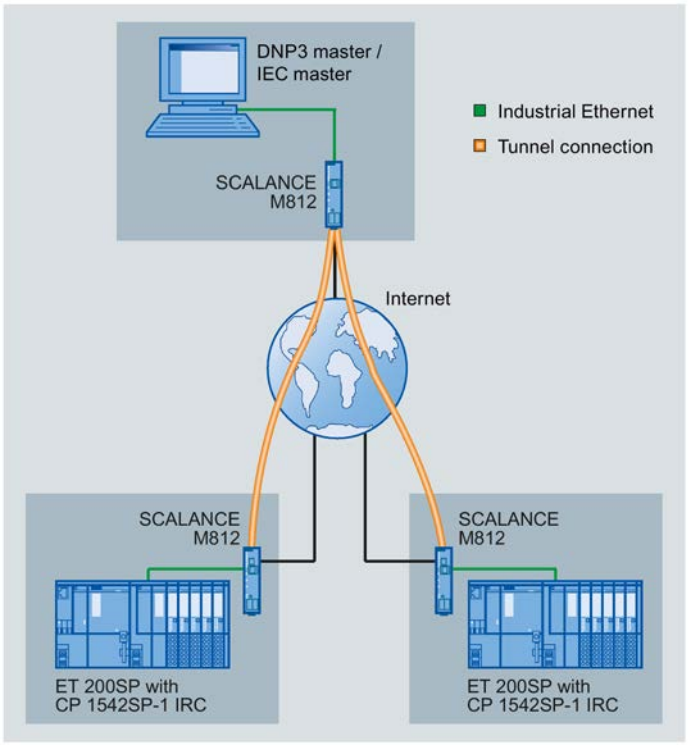


Figure 1-4 Configuration example of an ET 200SP with CP 1542SP-1 IRC; protocol: DNP3 or IEC 60870-5-104

LEDs and connectors

2

2.1 LEDs

Meaning of the LED displays of the CP

The CP has the following light emitting diodes (LEDs) on the front:

LED name	Meaning
PWR	Power supply
RN	Operating mode
ER	Error
MT	Maintenance

Table 2- 1 Legend for the following tables

Symbol				-
Meaning / LED status	ON (LED lit)	OFF	LED flashes	Any

Table 2- 2 Meaning of the LED displays of the CP

PWR (green)	RN (green)	ER (red)	MT (yellow)	Meaning
				No supply voltage on the CP or supply voltage too low
				CP startup
				CP in RUN mode
	-			Error. LED display with the following events: • Duplicate IP address • Bus adapter not plugged in or pulled • No telecontrol connection (CP 1542SP-1 IRC)
				Error: CP defective
				Missing configuration data
				Firmware update running
				There is a maintenance request from the CP. Example: • End of the firmware update

LEDs of the bus adapter

Every port of a bus adapter has an LED "LKx" that informs about the connection status with Ethernet and the frame traffic of the port.

Table 2- 3 Meaning of the LED displays of the bus adapters

LK (green)	Meaning
○	No Ethernet connection. Possible causes: • No physical connection to the network • Port disabled in the configuration
☼	LED flashing test
●	There is an Ethernet connection between the port and communications partner.

2.2 Power supply

External power supply required

The connector for the external 24 VDC power supply is located on the front of the CP.

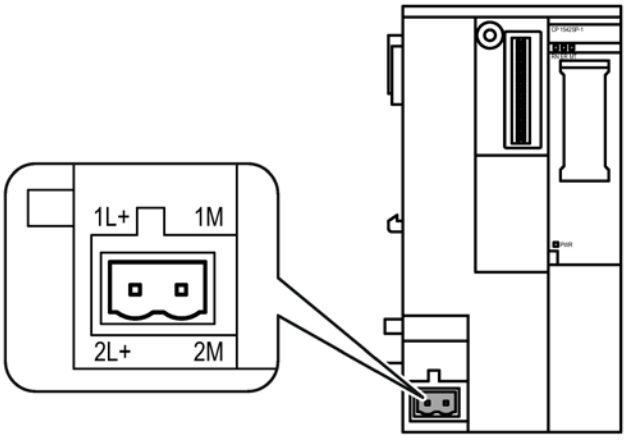


Figure 2-1 Power supply of the CP

Connector X80 is intended for connection to a single or redundant power supply. The power supply is connected to the CP with the supplied plug-in terminal block. The terminal block is plugged in to the socket X80 of the CP.

For information on installing and connecting up, refer to the sections Installing the CP (Page 32) and Connecting the CP (Page 36).

Reverse polarity protection

The plug-in terminal block for connector X80 is designed so that it can only be plugged in in one position. This provides constructional reverse polarity protection.

The connector X80 also has electronic reverse polarity protection.

You will find further data on the power supply in section Technical specifications (Page 109).

2.3 Connector for the BusAdapter

Operation of the device only with BusAdapter

For connecting to Ethernet the CP requires a BusAdapter. A BusAdapter does not ship with the CP.

The slot is on the front of the device:

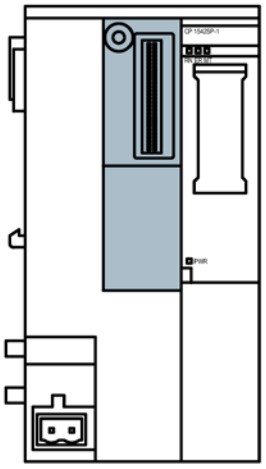


Figure 2-2 Front of the CP, the slot for the bus adapter is marked gray.

You will find the bus adapters supported by the CP in section BusAdapter (Page 117).

For information on installing and connecting up, refer to the sections Installing the CP (Page 32) and Connecting the CP (Page 36).

You will find the pinout of the Ethernet interface in section Assignment of the Ethernet interface of the bus adapter (Page 118). You will find further technical specifications of the bus adapter in the manual /2/ (Page 119).

Installation and connecting up

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 Notes 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 cables to or from the device when a flammable or combustible atmosphere is present.

WARNING

EXPLOSION HAZARD

Replacing components may impair suitability for Class 1, 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.

WARNING

DIN rail

In the ATEX and IECEx area of application only the Siemens DIN rail 6ES5 710-8MA11 may be used to mount the modules.

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

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 Notes on 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 General notices on use in hazardous areas according to FM

⚠ WARNING

EXPLOSION HAZARD

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

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

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

⚠ WARNING

EXPLOSION HAZARD

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

3.2 Installing the CP

NOTICE

Install and remove the CP only when the power is off

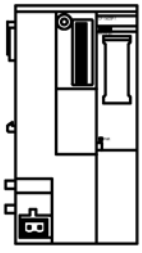
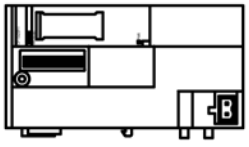
Switch off the power supply of the ET 200SP and the CP before you install or remove modules. Installing and removing modules with the power supply on can lead to damage to the modules and to loss of data.

Note

Note the installation guidelines

When installing and connecting up the CP note the instructions in the manual /2/ (Page 119).

NOTICE
Installation location - Dependency of the temperature range The module must be installed so that its upper and lower ventilation slits are not covered, allowing adequate ventilation. Above and below the modules, there must be a clearance of 25 mm to allow air to circulate and prevent overheating. Note the dependency of the permitted temperature range of the installation location. • Horizontal installation of the rack (DIN rail) means vertical position of the CP. • Vertical installation of the rack (DIN rail) means horizontal position of the CP. You will find the permitted temperature ranges in the section Technical specifications (Page 109).

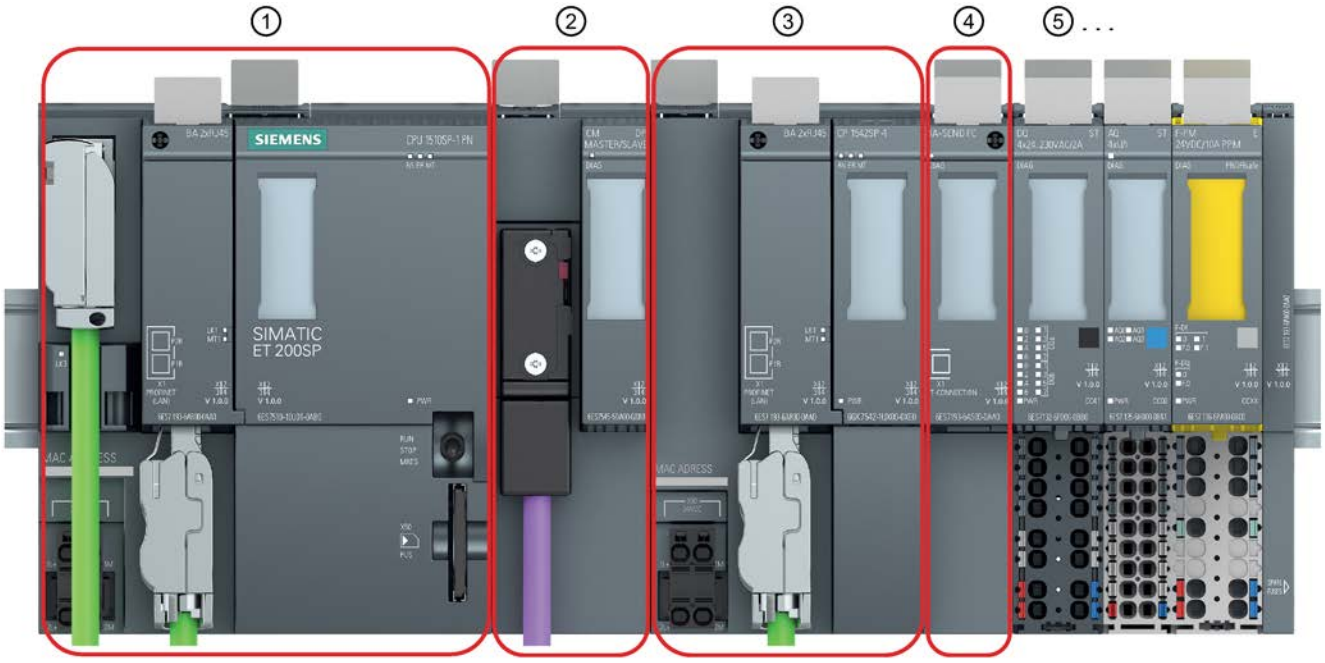
Installation of the rack	Installation position of the CP
Horizontal installation of the rack	
Vertical installation of the rack	

Slot rules

The CPU always occupies slot 1. In an ET 200SP you can plug in up to three of the following modules in slots 1 ... 4 (see figure) to the right of the CPU:

- CMs
- CPs
- BusAdapter Send

Of these three modules, up to two CP 154xSP-1 modules can be plugged in. These two CPs can be of the same type or different.



① Slot 1 - only permitted for the CPU.

② Slot 2 - for CM / CP / BusAdapter Send *
If you use a PROFIBUS CM, you must plug this in directly beside the CPU in slot 1.

③ Slot 3 - for CM / CP / BusAdapter Send *

④ Slot 4 - for CM / CP / BusAdapter Send *

⑤ Slot 5 ff for IO modules

* If you use a BusAdapter Send, this must be plugged in to the slot directly beside the IO modules.

Figure 3-1 Slots of the ET 200SP

Installation on a DIN rail

Note

Protecting the modules from slipping on the DIN rail

If you install the modules in an area with mechanical load, use suitable clamping devices at both ends of the device group to secure the modules on the DIN rail, e.g. Siemens and retainer 8WA1808.

The end retainers prevent the modules separating under mechanical load.

When using the device in the areas of application ATEX or IECEx, note the information on the DIN rai in section Notes on use in hazardous areas (Page 29).

The ET 200SP system is suitable for installation on a mounting rail according to EN 60715 (35 × 7.5 mm or 35 × 15 mm)

1. Hang the CPU / the interface module on the mounting rail.
2. Tilt the CPU / the interface module to the back until the mounting rail release audibly locks in place.
3. Hang the CP to the right next to the CPU.
4. Tilt the CP to the back until the mounting rail release audibly locks in place.
5. Move the CP to the left until it audibly locks in place in the CPU.
6. Mount the other base units and modules accordingly.

   See manual /2/ (Page 119) for information on this.

Plugging in the bus adapter

NOTICE
Touching the plug-in contacts
Do not touch the plug-in contacts when no bus adapter is plugged in.

1. Connect the appropriate cable to the bus adapter if you use a bus adapter with optical or direct electrical or optical connection (without plug).
2. Plug the bus adapter into the slot of the CP.

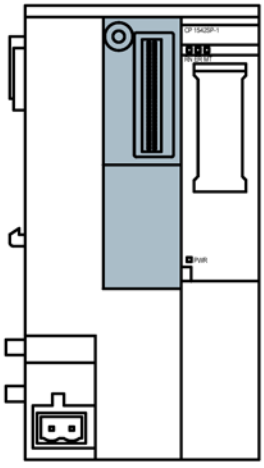


Figure 3-2 Front of the CP, the slot for the bus adapter is marked gray.

3. Screw the bus adapter to the CP.

   The securing screw is located at the top left on the front of the bus adapter.

   To do this use a screwdriver with 3 to 3.5 mm blade width or a suitable Torx screwdriver (T15).

   The maximum tightening torque is 0.25 Nm.

4. Plug the connector of the connecting cable into the socket of the bus adapter if you use a bus adapter with plug.

For information on plugging in the bus adapter and fitting cables see also the manual /2/ (Page 119).

Removal from the DIN rail

Follow the steps below to remove a CP from the DIN rail:

1. Turn off the power supply to the entire station including the CP and CPU.
2. Activate the mounting rail release of the modules to be moved (CPU, CPs) and move them parallel to the left until they are released from the remaining module group (free space approx. 16 mm).

   Press the locking slide marked "PUSH" on the top of a module down to be able to move the module in the DIN rail.
3. Activate the mounting rail release on the CP and move it to the right until it is released from the CPU (free space approx. 8 mm).
4. While holding the mounting rail release on the CP, swing the CP out of the mounting rail.

3.3 Connecting the CP

Order of the work

NOTICE
Connection only with power off Connect the CP only when the power is off. Refer to the information in the system manual, see /2/ (Page 119).

The bus adapter is already connected to the relevant cable, see section Installing the CP (Page 32).

1. Connect the external power supply to the terminal block of connector X80.

   Use the same power supply as the CPU.
2. Turn the power supply on only after the CP has been completely wired and connected.

Power supply at connector X80

You will find the location of the connector X80 four the power supply to the CP in section Power supply (Page 26). There, you will also find notes on reverse polarity protection..

The 2-terminal plug-in terminal block has the following pin assignment for the socket:

Terminal	Assignment
1L+ / 2L+	24 VDC
1M / 2M	Ground

The two terminals 1L+/L2+ and 1M/2m of the terminal block are each bridged internally so that you can connect either a single or a redundant power supply.

Connectable cable cross-section

- Without wire end ferrule 0.2 .. 2.5 mm^2 / AWG 24 .. 13
- With wire end ferrule 0.25 .. 1.5 mm^2 / AWG 24 .. 16
- With TWIN wire end ferrule: 0.5 .. 1.0 mm^2 / AWG 20 .. 17

You will find information about the power consumption and further technical details of the connectors in section Technical specifications (Page 109).

Configuration and operation

4

4.1 Security recommendations

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

Note

Security functions of the CP types

Depending on the supported function - the following notes do not apply to every CP type described in this manual.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- 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.

- Disabling the bus adapter ports

  In the configuration disable a port of the bus adapter being used that is not required.

- 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.
  - Use the Security functions of the telecontrol protocols. e.g. the DNP3 Security options.
  - Use the secure Open User Communication (Secure OUC) via the appropriate program blocks.
  - Leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CP disabled.

- Protection of the passwords for access to program blocks

  Protect the passwords stored in data blocks for the program blocks from being viewed. You will find information on the procedure in the STEP 7 information system in the topic "Know-how protection".

- Logging function

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

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.

- Make sure that all passwords are protected and inaccessible to unauthorized personnel.

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

Protocols

Secure and non-secure protocols

- Only activate protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.

  The NTP protocol provides a secure alternative with NTP (secure).

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 according to 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
DHCP	68 (UDP)	Closed	Open after configuration (while the CP obtains a new address)	No
S7 and online connections	102 (TCP)	Open	Open after configuration	No
Online diagnostics (CP 1543SP-1)	8448 (TCP)	Closed	Open after configuration	No
DNP3 listener port	20000 (TCP/UDP) can be set	Closed	Open after configuration	Yes, when Security is enabled.
IEC listener port	2404 (TCP) can be set	Closed	Open after configuration	No
SMTP	25 (TCP) can be set	Closed	Closed after configuration	No
SSL/TLS	587 (TCP) can be set	Closed	Closed after configuration	No
NTP	123 (TCP)	Closed	Closed after configuration	No
HTTP	80 (TCP)	Closed	Open after configuration	Yes
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)

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 20). You can configure a maximum of two CP 154xSP-1 for an ET 200SP.

You will find comprehensive information on configuration in the Information system of STEP 7 and in the following sections.

Overview of configuration of the CP

Follow the steps below when configuring:

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

7. Optional: Create the program blocks for the Open User Communication.
8. Save and compile the project.

Here you will find information on individual parameter groups in the following sections. You will find information on parameters not described in this manual in the information system of STEP 7.

Details on the parameters of the telecontrol communication of the CP 1542SP-1 IRC can be found in the section Telecontrol communication (CP 1542SP-1 IRC) (Page 45).

Details on the parameters of the security functions can be found in the section Security configuration(CP 1543SP-1) (Page 86).

Loading and saving 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 Ethernet interface

4.3.1 IPv6

Configuring the Ethernet addresses

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

Note

Communication via IPv6

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

4.3.2 Time-of-day synchronization

Procedure for time-of-day synchronization

You will find the parameter group for time-of-day synchronization under the Ethernet interface.

If the Security functions are enabled, the parameter group is displayed below "Security".

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.

Note

No forwarding of the time of day with NTP / NTP (secure)

Both the CPU and CP can have the time of day synchronized using NTP. If you enable time-of-day synchronization for both modules, it is recommended that you use the same NTP server to retain a consistent time-of-day within the station.

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

- **NTP**

  You configure the addresses of the NTP server(s), the synchronization interval and the "Accept time from non-synchronized NTP servers" option

CP 1542SP-1 IRC

With telecontrol communication enabled (parameter group "Communication types" the time of day is normally taken from the partner:

- **Time from partner**

  The CP sets its clock using the time of day that it receives in frames from the communications partner.

The CP 1542SP-1 IRC provides the CPU with the option of it taking its time from the CP using a PLC tag. See section Auto-Hotspot for information on this.

Note

No time-of-day synchronization of the CPU when the time is taken from the CP

When the CPU takes the time from the CP using a PLC tag, disable the CPU's own time-of-day synchronization.

CP 1543SP-1

Note

Ensuring a valid time of day

If you use security functions, a valid time of day is extremely important. It is recommended to use the NTP (secure)NTP (secure) method.

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

- **NTP**
- **NTP (secure)**

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

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

See also

Communication with the CPU (Page 56)

4.4 SNMP

"SNMP" parameter group

- "**Enable SNMP**" parameter group

  Releases the function of the SNMP agent on the CP.

Note

If the security functions are enabled for the CP 1543SP-1 you will find the parameter group "SNMP" in "Security".

Scope of performance of the CPs

The CPs support the following SNMP version:

- **CP 1542SP-1, CP 1542SP-1 IRC**
  - SNMPv1
- **CP 1543SP-1**
  - SNMPv1
  - SNMPv3 (with activated Security functions)

Traps are not supported by the CP.

You will find detailed information about the supported functions in the section Diagnostics with SNMP (Page 100).

4.5 Telecontrol communication (CP 1542SP-1 IRC)

4.5.1 Configuration

Data points for telecontrol communication

No program blocks need to be programmed for the CP 1542SP-1 IRC to transfer user data between the station and communications partner.

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

The individual data points can be transferred to the control system and processed there.

To transfer the process data and for some options of the parameter groups "Partner stations" and "Communication with the CPU" configured data points are required.

For further information, refer to section Data point configuration (Page 57).

4.5.2 Communication types

In this parameter group, you enable the communication types you want to use for the particular 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.

The Open User Communication does not exist in the parameter group because these communications services are not configured but programmed using program blocks.

The parameter group does not exist for the CP 1542SP-1, since the communications services supported by this CP are always enabled.

"Communication types" parameter group

- **Enable telecontrol communication**

  Only with the CP 1542SP-1 IRC

  Enables telecontrol communication on the CP. The following protocols can be used as alternatives:

  – **TeleControl Basic**

    Enables communication with the telecontrol server

  – **DNP3**

    Enables communication with up to four DNP3 masters

  – **IEC 60870-5-104**

    Enables communication with up to four IEC masters

Note

Full telecontrol functionality only when Security functions are enabled

For the following functions, you need to enable the Security functions:

- Send messages (e-mails) using the telecontrol functionality
- Use of the "TeleControl Basic" protocol (general)
- Use of the DNP3 Security functions
- Use of certificates

Note

Loss of configuration data when changing the telecontrol protocol

If you change the protocol on a configured CP, protocol-specific configuration data is lost, for example, the data point configuration, the partner configuration and the messages (e-mails).

- **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 and S7 routing 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.

4.5.3 Address and authentication information

Address and authentication information for telecontrol communication

Depending on the telecontrol protocol the news, the communications partners of the CP require the following address and authentication information of the CP that needs to be configured for the CP:

- **TeleControl Basic**

  The telecontrol server requires:

  – Project number

  – Station number

  – Telecontrol password (for authentication)

  You will find the parameters in the parameter group "CP idenfication" under "Security".

  – IP address (in the "Ethernet interface“ parameter group)

    Since the CP always establishes the connection to the telecontrol server, the IP address of the CP does not need to be configured in TCSB.

- **DNP3**

  The master requires:

  – Station number (in the "CP identification" parameter group)

  – IP address (in the "Ethernet interface“ parameter group)

  – Port number of the CP

- **IEC**

  The master requires:

  – Station number (in the "CP identification" parameter group)

  – IP address (in the "Ethernet interface“ parameter group)

  – Port number of the CP

Address information required by the CP

You will find information about the address information of the communications partner required by the CP in section Partner stations (Page 52).

4.5.4 Ethernet interface (X1) > Advanced options

Configure the generally available parameters just as for every other Ethernet interface:

- General data (name etc.)
- Addresses and possibly routers
- Port settings
- Access to the Web server

Below you will find only the description of the specific parameters for telecontrol communication.

TCP connection monitoring

The setting made here applies globally to all TCP connections of the CP. Note the option of overwriting the value configured here for individual communications partners, see below.

- **TCP connection monitoring time**

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

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

  The monitoring time is configured for the Ethernet interface as the default for all TCP connections. The default value can be adapted individually for each connection in "Partner stations", compare section Partner stations (Page 52). The function can only be disabled by entering 0 (zero) for the partners.

- **TCP keepalive monitoring time**

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

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

  The monitoring time is configured for the Ethernet interface as the default for all TCP connections. The default value can be adapted individually for each connection in "Partner stations". The function can only be disabled by entering 0 (zero) for the partners.

Transmission settings - TeleControl Basic

- **Connection establishment delay**

  Basic value for the wait time until the next connection establishment following an unsuccessful attempt to establish a connection. After every 3 attempts, the basic value is doubled up to a maximum of 900 s.

  Permitted range: 10 ... 300. Default setting: 10

  Example: The basic value 20 results in the following wait times: 3 x 20 s, 3 x 40 s, 3 x 80 s etc. up to max. 3 x 900 s.

- **Send monitoring time**

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

  Permitted range: 1 ... 65535. Default setting: 5

- **Key exchange interval**

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

  Permitted range: 0 ... 65535. Default setting: 8

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

Transmission settings - DNP3

You will find information on the permitted ranges of the functions and defaults in the tooltips of STEP 7.

- **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**
- **Frame repetitions**
- **Connection confirmation**
- **Connection monitoring time**
- **Transfer mode "Unsolicited"**
- **Max. number of unsolicited frames**
- **Monitoring time for unsolicited frames**

- **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 ... 255.

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

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, types of transmission, event classes, triggers (Page 63).

Transmission settings - IEC

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.

You will find information on the permitted ranges of the functions and defaults in the tooltips of STEP 7.

- **Max. time between Select and Operate**
- **Monitoring time for connection establishment (t_0)**
- **Frame monitoring time (t_1)**

  Monitoring time 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.

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

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

  After receiving data from the master, the CP acknowledges the received data alternatively:

  – 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 at the latest when t_2 elapses.

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

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

  Monitoring time 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 longer times without data traffic.

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

  Maximum number of unacknowledged data frames (I-APDUs) as maximum difference between send sequence number N(S) and receive sequence number N(R).

  When k is reached and t_1 has not yet elapsed, the CP does not send any frames until all the frames sent have been acknowledged by the master.

  When k is reached and t_1 has elapsed, the TCP connection is terminated.

- **Max. number of unacknowledged data frames**

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

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

Port [X1 Px]

If you do not want to use both ports of the bus adapter, you can disable one of the two ports.

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

4.5.5 Partner stations

4.5.5.1 Partner configuration

The STEP 7 configuration of the communications partners of the CP (telecontrol server, DNP3 or IEC master) and the connections to the partners is not possible and not necessary.

Address information of the communications partners

For the communications partners of the CP, the following information is required during the configuration of the CP:

- TeleControl Basic
  - Partner IP address

    See section Auto-Hotspot for information on this.
  - Partner port (port number of the listener port of TCSB)
- DNP3 / IEC
  - Master station address

    Station address specified on the master

    With the IEC protocol the Master station address is not evaluated.
  - Partner IP address

    IP address of the master

    For the addressing of redundant partners, see section Addressing of single and redundant communications partners (Page 55).
  - Partner port

"Partner stations" (only with DNP3 / IEC)

- **Listener port**

  CP's own listener port

"Telecontrol server" / "Partner"

- **Activate partner**

  Enable the option to be able to use the partners configured later for the communication.

  In "TeleControl Basic" the telecontrol server is always enabled as a partner.

- **Partner number**

  The partner number is always signed by STEP 7.

- **Station address / Master station address**

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

"Connection to partner"

You will find information on the permitted ranges and defaults in the tooltips of STEP 7.

- **Partner IP address**

  IP address or host name (FQDN) of the telecontrol server. This can, for example, also be the FQDN of a DynDNS service.

- **Connection monitoring**

  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, see also the section Ethernet interface (X1) > Advanced options (Page 48). These settings apply to all TCP connections of the CP.

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

- **TCP connection monitoring time**

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

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

  The function can be disabled by entering 0 (zero) for the individual partners.

- **TCP keepalive monitoring time**

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

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

  The function can be disabled by entering 0 (zero) for the individual partners.

- **Connection mode**

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

- **Connection establishment**

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

- **Partner port**

  Port number of the communications partner

"Connection to redundant partner" (only with DNP3 / IEC)

- **Redundancy mode**

  Enable the option if the communications partner is a redundant master.

For information on the other parameters see above.

"Advanced settings"

- **Partner monitoring time (only with DNP3 / IEC)**

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

- **Report partner status (connection to partner)**

  If the function is enabled, the CP signals the status of the connection to the communications partner to the CPU.

  – 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.

DNP3-specific settings

- **DNP3 level**

  DNP3 conformity level supported by the partner.

- **Event transmission mode**

  Mode with which the frames in the send buffer of the CP (events) are transferred:

  – Chronological transfer of individual frames

    or

  – Block-by-block transfer of the frames of a data point

4.5.5.2 Addressing of single and redundant communications partners

Addressing the telecontrol server

- **Addressing of a single telecontrol server**

  Configure the IP address of the telecontrol server or the DSL router when connecting via the Internet.

  When using a DynDNS service with the host name (FQDN) can be specified.

- **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 a 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 (TCP) 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.

Addressing redundant DNP3 or IEC masters

For each master specify the master station address and the IP address being used.

4.5.5.3 Partner for inter-station communication

Only when using the "TeleControl Basic" protocol

Inter-station communication

In this table, you specify the S7 stations and CPs 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

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

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

Access ID

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

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

4.5.6 Communication with the CPU

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 70).

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 17).

  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, types of transmission, event classes, triggers (Page 63).

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.

4.5.7 Data point configuration

4.5.7.1 Configuring the data points

Creating data points and messages

You configure the data points and messages 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

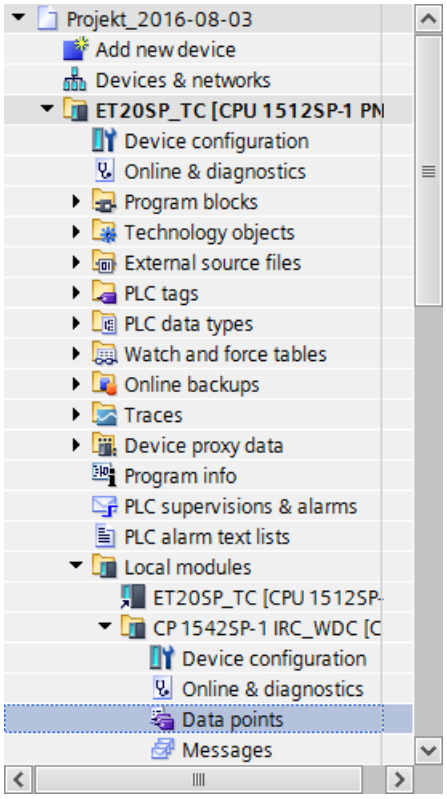


Figure 4-1 Open the data point and message editor

Open the data point and message editor by double-clicking on the entry "Data points" or "Messages".

Requirement for data points: 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.

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 17).

Access to the memory areas of the CPU

The values of the PLC tags or DBs referenced by the data points are read and transferred to the communications partner by the CP. Data received from the communications partner is written by the CP to the CPU via the PLC tags or DBs.

The address ranges, formats and S7 data types of the PLC tags that are compatible with the protocol-specific data point types of the CP can be found in the section Datapoint types (Page 59).

Properties of the data points

All PLC tags intended to be used for data point configuration must have the attribute "Visible in HMI".

Note

Length of the data point names

If you want to use the maximum number of configurable data points, assign data point names, CP names and station names that are as short as possible.

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 may be used with the exceptions listed below.

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

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

4.5.7.2 Datapoint types

Supported data point types of the CP 1542SP-1 IRC

During the configuration of the user data to be transferred by the CP 1542SP-1 IRC, each data point is assigned a protocol-specific data point type. The data point types along with the compatible S7 data types are listed below. They are grouped according to format (memory requirements).

TeleControl Basic: Data point types

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

Format (memory requirements)	Data point type	S7 data types	Address area
Bit	Digital input	Bool	I, Q, M, DB
	Digital output	Bool	Q, M, DB
Byte	Digital input	Byte, USInt	I, Q, M, DB
	Digital output	Byte, USInt	Q, M, DB
Integer with sign (16 bits)	Analog input	Int	I, Q, M, DB
	Analog output	Int	Q, M, DB
Counter (16 bits)	Counter input	Word, UInt	I, Q, M, DB
Integer with sign (32 bits)	Analog input	DInt	Q, M, DB
	Analog output	DInt	Q, M, DB

Format (memory requirements)	Data point type	S7 data types	Address area
Counter (32 bits)	Counter input	UDInt, DWord	I, Q, M, DB
Floating-point number with sign (32 bits)	Analog input	Real	Q, M, DB
	Analog output	Real	Q, M, DB
Floating-point number with sign (64 bits)	Analog input	LReal	Q, M, DB
	Analog output	LReal	Q, M, DB
Block of data (1 .. 64 bytes)	Data	ARRAY [1]	DB
	Data	ARRAY [1]	DB

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

Block of data (ARRAY)

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

- Byte, USInt (total of up to 64 per data block)
- Int, UInt, Word (total of up to 32 per data block)
- DInt, UDInt, DWord (total of up to 16 per data block)

Time stamp in UTC format

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

DNP3: Data point types

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

Format (memory requirements)	Data point type	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		
	Binary Output Event [1]	**11** [1, 2]	out		
	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		
	Counter Event	**22** [2, 6]	in	UInt, Word	I, Q, M, DB
	Frozen Counter Event [3]	**23** [2, 6]	in		
	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		
	Analog Output	**41** [2]	out	Int	Q, M, DB
	Analog Output Event [4]	**42** [2, 4]	out		

Format (memory requirements)	Data point type	DNP3 object group [variations]	Direction	S7 data types	Operand area
Integer (32 bits)	Counter Static	**20** [1]	in	UDInt, DWord	I, Q, M, DB
	Frozen Counter [2]	**21** [1, 5]	in		
	Counter Event	**22** [1, 5]	in	UDInt, DWord	I, Q, M, DB
	Frozen Counter Event [3]	**23** [1, 5]	in		
	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		
	Analog Output	**41** [1]	out	DInt	Q, M, DB
	Analog Output Event [4]	**42** [1]	out		
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		
	Analog Output	**41** [3]	out	Real	Q, M, DB
	Analog Output Event [4]	**42** [5, 7]	out		
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		
Block of data (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.

Explanation of the table footnotes [1], [2], [3], [4]: Configuring data points using substitute object groups

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 back, 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 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.

Time stamp of the DNP3 CP in UTC format

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

IEC: Data point types

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 [1)]	<30>	in	Bool	I, Q, M, DB
	Single command	<45>	out	Bool	Q, M, DB
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag [1)]	<32>	in	Byte, USInt	I, Q, M, DB
Integer (16 bits)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag [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 [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

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
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
Block of data (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
Block of data (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

[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.

Time stamp with the IEC CP

IEC CP 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.

4.5.7.3 Process image, types 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 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):

- **Static value (no event)**

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

  Static values correspond to the following classes:

  – DNP3: Class 0

  – IEC: Class 2

- **Event**

  The values of data points configured as an event are also entered in the image memory of the CP. The value of the event is sent unsolicited to the communications partner if this function is enabled by the master.

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

  Events correspond to the following classes:

  – DNP3: Class 1 / 2 / 3

  – IEC: Class 1

The image memory, 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 being queried by the communications partner. Refer to "Transfer after call" in the section "Types of transmission".

The send buffer

The send buffer of the CP is the memory for the individual values of data points that are configured as an event. The maximum number is divided equally among all configured and enabled communications partners. You configure the size of the send buffer with the parameter "Frame memory size", see the section Communication with the CPU (Page 56).

If the connection to a communications partner is interrupted, the individual values of the events are retained in the buffer. 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 value is 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 depending on the protocol being used:

- TeleControl Basic

  The forced image mode

  If the send buffer reaches a fill level of 80%, the CP changes to the forced image mode. New values from data points configured as an event 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 if the fill level of the send buffer has fallen below 50%.

- DNP3 / IEC

  If a send buffer fill level of 100% is reached, the oldest values are overwritten.

  When using the DNP3 protocol, additional conditions for sending the events can be specified:

  – A maximum number of events in the send buffer, configurable for each event class.

  – A configurable maximum storage period for events in the send buffer.

Types of transmission

The following types of transmission are possible:

- **Transfer after call (class 0)**

  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 (events)**

  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 of the identifiers of the data point changes see also the section Status IDs of the data points (Page 67).

Event classes with the "Triggered" type of transmission

Depending on the protocol used the following event classes are available:

- **TeleControl Basic**

  – **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.

- **DNP3**

  The evaluation of the following classification must be handled by the master.

  – **Event class 1**

    Class according to DNP3 protocol: Class 1

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

  – **Event class 2**

    Class according to DNP3 protocol: Class 2

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

  – **Event class 3**

    Class according to DNP3 protocol: Class 3

    Only the current value at the time the trigger condition is met is entered in the send buffer and overwrites the last value stored there.

- **IEC**

  Both of the following event classes correspond to the user data class 1 of the IEC protocol

  – **Every value triggered**

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

  – **Current value triggered**

    Only the current value at the time the trigger condition is met is entered in the send buffer and overwrites the last value stored there.

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 73).

- **Time trigger**

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

- **Event trigger**

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

  Resetting the trigger 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

Whether the value of a data point is transferred to the communications partner immediately after the trigger or after a delay depends on the protocol used and the settings.

- **TeleControl Basic**

  You specify the time of transmission with the parameter "Transmission mode" in the "Trigger" tab of the data point:

  – **Unsolicited**

    The value is transferred immediately.

  – **Conditional spontaneous**

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

    - The telecontrol server queries the station.

    - The value of another event with the Transmission mode “Unsolicited" is transferred.

    - The fill level of the transmission buffer has reached 80% of its maximum capacity.

- **DNP3 / IEC**

  The spontaneous transmission in these protocols depends on whether spontaneous sending or asymmetric communication is possible in the network.

4.5.7.4 Status IDs of the data points

Status IDs of data points

The status IDs od the data points listed below are transferred for each data point in each frame. They differ slightly in the three protocol types.

For the meaning of the status bits, see below. The "Meaning" (2nd table row) relates to the "bit status" (3rd table row).

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 IDs - TeleControl Basic

The status bits are converted to the OPC quality code as follows by TCSB.

- Quality = BAD, If:

  NON_EXISTENT or OVER_RANGE = 1
- Quality = UNCERTAIN, If:

  RESTART or CARRY or SB = 1
- Quality = GOOD, If:

  Bits 1, 2, 3, 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	SB	LOCAL_ FORCED	CARRY	OVER_ RANGE	RESTART	ONLINE
Meaning	-	Data point does not exist or S7 address unreachable	Substitute value	*(Bit is not set)*	Counted value over-flow before reading the value	Limit value of the ana-log value prepro-cessing overshot / undershot	Value not yet updated after start	Value is valid, CPU in RUN
Bit status	*(always 0)*	1	1	*(irrelevant)*	1	1	1	1

Status IDs - TeleControl Basic

The status IDs can be evaluated by the master. They 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 value prepro-cessing over-shot / undershot	Value not updated after start	Value is invalid
Bit status	*(always 0)*	*(always 0)*	*(always 0)*	1	1	1	1	1

Status IDs - IEC

The status IDs can be evaluated by the master. They 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

4.5.7.5 Rules for configuring the data point index:

Configuration of the data point index

Below you will find the configuration rules for the data point index depending on the protocol being used.

TeleControl Basic

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

- Input

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

- Output
  - A data point of the type output can have the same index as a data point of the type input.
  - Several data points of the type output can have the same index.

Note

Data points for the inter-station communication with a CP in another S7 station

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

DNP3

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.

IEC

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.

4.5.7.6 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.

Duration of the CPU scan cycle

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

4.5.7.7 "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 73).

- **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.

4.5.7.8 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 74).

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.

4.5.7.9 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:

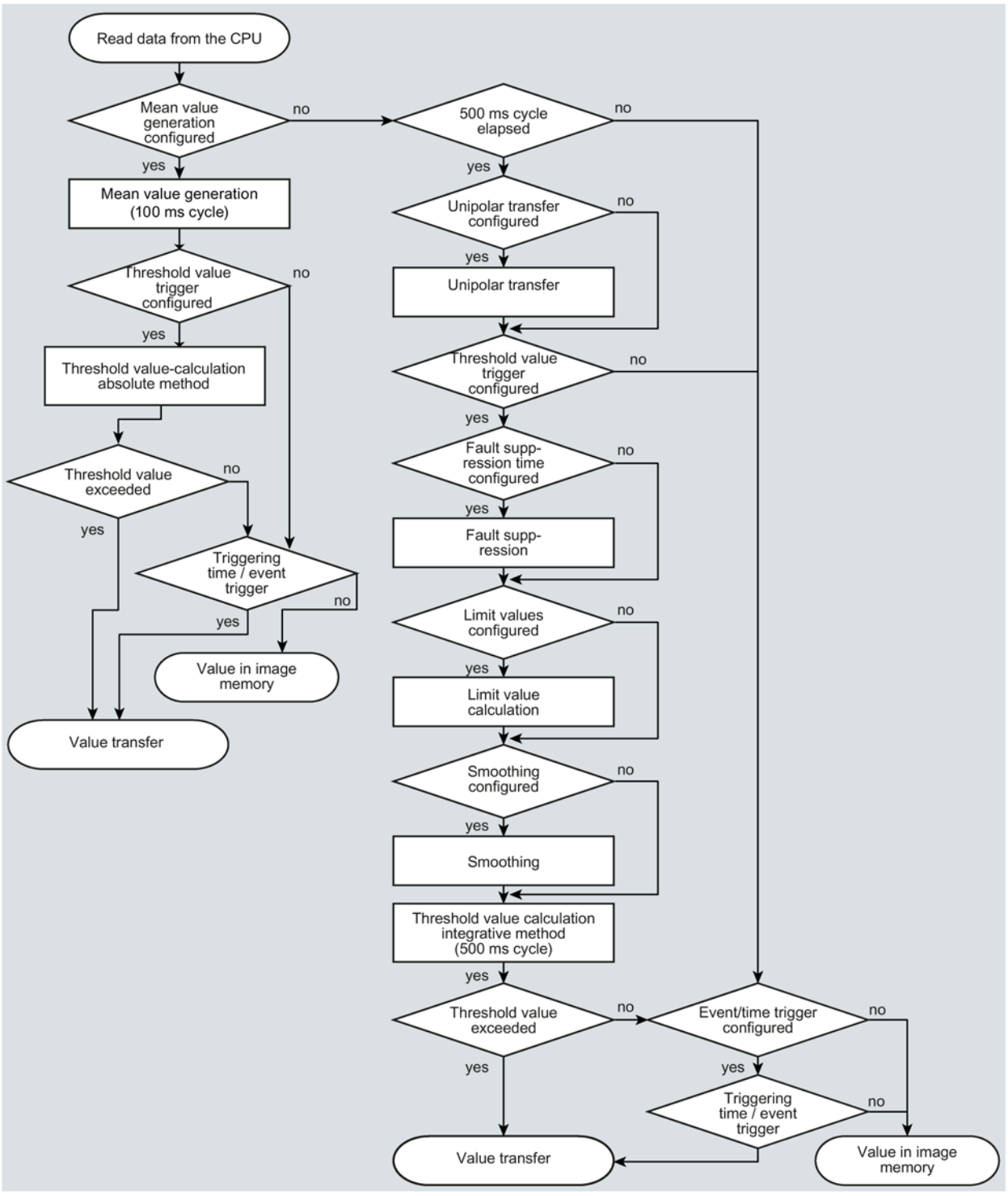


Figure 4-2 Sequence of the analog value preprocessing

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"

If a limit value is overshot or undershot, the status identifier "OVER_RANGE" of the data point is set. This status identifiers are described in the section Status IDs of the data points (Page 67).

The "OVER_RANGE" 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: OVER_RANGE = 1
  - If the value falls below the limit value: OVER_RANGE = 0
- Limit value 'low':
  - If the value falls below the limit value : OVER_RANGE = 1
  - If the value then exceeds the limit value: OVER_RANGE = 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.

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

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)	
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.

4.5.8 Message configuration

Configuring e-mails

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

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 Configuring the data points (Page 57).

Requirements and necessary information

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

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

  To do this, you require the following information:

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

  – Email address of the recipient

Trigger: Triggering e-mail transfer

Using the "Trigger" parameter group in the message table, you configure which of the following events triggers the sending of the e-mail.

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

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

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

With the "TeleControl Basic" protocol, the following events can be configured as the trigger of an e-mail:

- Connection establishment to the partner has failed.
- A TeleService session has started.
- A TeleService session has ended.

Include value Transfer the value of a PLC tag with a message

If you enable the option "Include value" in the "Trigger" parameter group, 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.

Enable identifier for processing status

If this option is enabled in STEP 7, a status is output on the CP that provides information about the processing status of the sent message. The status is written to a PLC tag of the type DWORD. Select this tag via the "PLC tag for processing status" box.

If there are problems delivering messages, you can determine the status for example via the Web server of the CPU by displaying the value of the PLC tag there.

For the significance of the individual statuses, refer to the section Processing status of the telecontrol e-mails (Page 104).

4.5.9 Security > CP identification

CP identification

Only valid when using the "TeleControl Basic" protocol.

- 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 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 the "TCSB" application for this station.

4.5.10 Security > DNP3 security options

Authentication and key exchange with the DNP3 protocol

If the Security functions are enabled, the master and station (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 DNP 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.

- Authentication requests before key exchange
- Key exchange interval

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

DNP3 security options

- **Enable DNP3 security options**

  Method with which the CP authenticates itself to the master.

  – Disabled

    Non-secure authentication. If this option is selected the CP logs on only using its station address.

  – Enabled

    Secure authentication. If this option is selected, the CP and master use the DNP3 Security mechanisms. The parameters are configured as follows.

- **IKE mode**

  Selection of the mode for key exchange (IKE)

  – The Main Mode is the default mode.

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

- **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, authentication requests with date, time and result are saved on the CP and sent to the master for further evaluation.

- **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. Meaning of the options:

  – SHA-1 mode allowed

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

  – SHA-1 mode not allowed

    The CP may not use SHA-1.

    Note: If the master does not support SHA-256, no connection will be established if this option is selected.

- **Secure hash algorithm**

  Selection of the Secure Hash Algorithm (SHA). Possible selections:

  – SHA-1

  – SHA-256

- **Key wrap algorithm**

  Selection of the Advanced Encryption Standard (AES). Possible selections:

  – AES-128

  – AES-256

- **Key length**

  Length of the pre-shared key in bytes

  The following lengths are used depending on the key wrap algorithm.

  – For AES-128: 16 bytes

  – For AES-256: 32 bytes

- Max. number of key exchange requests

  The function is disabled.

- **Authentication requests before key exchange**

  Maximum number of authentication requests of the CP with the master before the session key is renewed.

  If you enter 0 (zero), the function is deactivated and the session key is renewed only depending on the key exchange interval.

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

- **Key exchange interval**

  Period after which the session key is exchanged again between the CP and the master.

  If you enter 0 (zero), the function is deactivated and the key will never be renewed.

  The interval must be matched up on both communications partners.

- **Authentication timeout**

  Maximum waiting (seconds) 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

- **Pre-shared key**

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

  The key must have the key length configured above (2 characters per byte).

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

  – Manual configuration

    Enter the pre-shared key 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 system.

4.5.11 Security > E-mail configuration

E-mail configuration

- **No configuration**

  As default, the sending of e-mails is disabled.

- **Activate SMTP**

  Enable this option if you want to use the sending of unencrypted e-mails via SMTP port 25.

- **Enable SSL/TLS**

  If your e-mail service provider only supports encrypted transfer, enable this option. Select the protocol via the port number:

  – Port no. 587

    When using STARTTLS the CP sends encrypted e-mails.

  – Port no. 465

    When using SSL/TLS (SMTPS) the CP sends encrypted e-mails.

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

  If you want to use an Internet connection with an IPv6 infrastructure, note the information in the section IPv6 (Page 43).

4.6 Security configuration(CP 1543SP-1)

4.6.1 VPN

4.6.1.1 VPN (Virtual Private Network)

VPN tunnel

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

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

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

Properties

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

Areas of application

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

Cell protection concept

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

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

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

- Data espionage
- Data manipulation
- Unwanted access

4.6.1.2 Creating a VPN tunnel for S7 communication between stations

Requirements

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

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

Note

Communication also possible via an IP router

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

Procedure

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

1. Creating a security user

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

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

Creating a security user

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

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

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

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

With all further logons, log on as user.

Select the "Activate security features" check box

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

You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

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

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

Note

Current date and current time on the CP for VPN connections

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

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.

4.6.1.3 VPN communication with SOFTNET Security Client (engineering station)

VPN tunnel communication works only if the internal node is disabled

Under certain circumstances the establishment of VPN tunnel communication between SOFTNET Security ClientSOFTNET 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 to the CP can be established.

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

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

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

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

4.6.1.5 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

4.6.2 Firewall

4.6.2.1 Pre-check of messages by the MAC firewall.

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

4.6.2.2 Online diagnostics and downloading to station with the firewall activated

Setting the firewall - steps involved

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

1. In the global security settings (see project tree), select the entry "Firewall > Services > Define services for IP rules".
2. Select the "ICMP" tab.
3. Insert a new entry of the type "Echo Reply" and another of the type "Echo Request".
4. Now select the CP in the ET 200SP station.
5. Enable the advanced firewall mode in the local security settings of the CP in the "Security > Firewall" parameter group.
6. Open the "IP rules" parameter group.
7. In the table, insert a new IP rule for the previously created global services as follows:
   - Action: Allow; "From external -> To station " with the globally created "Echo request" service
   - Action: Allow; "From station -> to external" with the globally created "Echo reply" service
8. For the IP rule for the Echo Request, enter the IP address of the PG/PC in "Source IP address". This ensures that only PING packets from your PG/PC can pass through the firewall.

4.6.2.3 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.

4.6.2.4 Firewall settings for S7 connections via a VPN tunnel

IP rules in advanced firewall mode

If you set up configured connections (S7, OUC) 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.

4.6.3 Filtering of the system events

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

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

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

4.7 Table "Certificate manager" (CP 1542SP-1 IRC, CP 1543SP-1)

If the Security functions are enabled, in the STEP 7 project the certificates for all Security modules involved are generated for example to allow communication via VPN connections.

Certificates generated by STEP 7 such as SSL certificates or VPN group certificates are automatically assigned to the corresponding modules and do not need to be assigned using the local security settings.

The local certificate manager

Certificates that were imported via the certificate manager in the global security settings are not automatically assigned to the corresponding modules. Imported certificates must be included in the list of trustworthy partner certificates manually via the entry "Certificate manager" in the local Security settings. When assigning a CA certificate the module is also assigned the certificates derived from it.

Parameter group "Security" > table "Certificate manager"

Via the local certificate manager assign certificates to the CP for certain services (e.g. secure sending of e-mails).

1. To do this, click the table cell "Add new".
2. Click on the button on a white background "...".
3. In the certificate list that opens, you can either add a new certificate using the "Add" button or select an existing certificate of the project using the check mark symbol.

   You can recognize the properties of the displayed certificates in the global certificate manager.

Certificates for the CP 1542SP-1 IRC

Requirement in the global security settings

For the secure sending of e-mails, import the certificate of the e-mail service provider into the certificate manager.

Assign the certificate in the CP configuration

Select the following certificate in the CP configuration:

- Table "Trustworthy client certificates":

  The certificate of the e-mail service provider

Certificates for the CP 1543SP-1

Before certificates can be referenced in the program blocks for Secure Communication, these certificates must be assigned to the Security module as device certificates via the local certificate manager.

Requirement in the global security settings

To be able to assign the CP certificate of a communications partner, you need to first import the certificates of the partner in the global certificate manager (Global security settings).

To make the assigned certificate known to the partner module, this certificate must be entered in the list of trustworthy partner certificates after import.

Assign the certificates in the CP configuration

Select the following certificates in the CP configuration:

- Table "Device certificates":

  The device certificate of the CP generated by STEP 7
- Table "Certificates of the partner devices":

  The imported certificate of the partner

Programming (OUC)

5

5.1 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

Connections of Open User Communication are not configured.

For TCP / UDP / ISO-on-TCP communication via Ethernet, the blocks of Open User Communication (OUC) listed below are used. For this, create a suitable program blocks. 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

Program blocks for all three CP types

The following instructions in the specified minimum version are available for programming Open User Communication for all three CP types:

- **TSEND_C V3.0 / TRCV_C V3.1**

  Compact blocks for connection establishment/termination and for sending and receiving data

  or

- **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

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

You create the SDT required for every connection description as a data block. You generate the SDT type in STEP 7 by entering the name (e.g. "TCON_Param") in the "Data type" box manually in the declaration table of block instead of selecting an entry from the "Data type" drop-down list. The corresponding SDT is then created with its parameters.

Depending on the security functions supported, the three CP types support the following SDTs:

SDTs for all three CP types

The following SDTs can be used by all three CP types:

- **TCON_Param**

  For transferring frames via TCP

- **TADDR_Param**

  For transferring frames via UDP

- **TCON_IP_RFC**

  For transferring frames via ISO-on-TCP

- **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 the host name

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

SDT for CP 1542SP-1 IRC and CP 1543SP-1

These two CP types can use the following SDT for e-mail connections with Security function:

- **TMail_V4_SEC**

  For secure transfer of e-mails addressing the e-mail server using an IPv4 address

- **TMail_QDN_SEC**

  For secure transfer of e-mails addressing the e-mail server using the host name

SDT only for CP 1543SP-1

The CP 1543SP-1 can use the following SDT for data transfer with Security function:

- **TCON_IP_V4_SEC**

  For the secure transfer of data via TCP

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.

Diagnostics and maintenance 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 25).

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

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

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

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

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

- General information on the module
- Diagnostics status
- Information on the interfaces of the module

  Information on other functions of the module

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 46).

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

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 Web server of the CPU (Page 102).

SNMP

For information on the functions, refer to the section Diagnostics with SNMP (Page 100).

6.2 Diagnostics with SNMP

Requirement

The requirement for using SNMP is the enabling of the function in the configuration, see section SNMP (Page 45).

SNMP (Simple Network Management Protocol)

SNMP is a protocol for diagnostics and managing 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).

You will find detailed information on SNMP and the Siemens Automation MIB in the manual /6/ (Page 120).

Scope of performance of the CPs

The CPs support the following SNMP version:

- **CP 1542SP-1, CP 1542SP-1 IRC**
  - SNMPv1
- **CP 1543SP-1**
  - SNMPv1
  - SNMPv3 (with activated Security functions)

Traps are not supported by the CP.

Supported MIBs in SNMPv1

The CPs support the following MIBs:

- **MIB II (acc. to RFC1213)**

  The CP supports the following groups of MIB objects:
  - System
  - Interfaces
  - IP
  - ICMP
  - TCP
  - UDP
  - SNMP
- **LLDP MIB**
- **Siemens Automation MIB**

  Note the rights for writing to the MIB objects, see the next section (SNMPv3).

Supported MIB objects in SNMPv3

If SNMPv3 is enabled, the CP returns the contents of the following MIB objects:

- **MIB II (acc. to RFC1213)**

  The CP supports the following groups of MIB objects:

  – System

  – Interfaces

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

  – IP (IPv4/IPv6)

  – ICMP

  – TCP

  – UDP

  – SNMP

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

  – Adress Translation (AT)

  – EGP

  – Transmission

- **LLDP MIB**
- **Siemens Automation MIB**

  Note that 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 and groups, only read access is possible for security reasons.

Access rights using community names (SNMPv1)

TCP uses the following community strings to control the permissions for access to the SNMP agent:

Table 6- 1 Access rights in the SNMP agent

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

*) Note the use of lowercase letters!

6.3 Web server of the CPU

The Web server of the CPU

The CPU has a Web server which you can access from an engineering station using HTTP/HTTPS via the CP.

The Web server of the CPU provides a wide variety of functions for diagnostics and service purposes for example loading firmware files. You will find detailed information in the system manual /2/ (Page 119)and in the information system of STEP 7 in the topic and under the heading "Web server".

Requirements for access to the Web server

Permitted web browsers

You will find the Web browsers supported on the engineering station for access to the Web server of the CPU in the STEP 7 information system under the heading "Web server".

Requirements in the CPU configuration

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

   To load firmware you need to assign this user the right to perform firmware updates in the access level.

   The user name and password are required later for access.
6. Configuration of the option "Allow access only using HTTPS" in the parameter group "General"

   Depending on whether you want to access the Web server using HTTP or HTTPS, the configuration of the parameter differs:

   – "Allow access only using HTTPS" enabled

     Connection establishment is possible only using HTTPS.

   – "Allow access only using HTTPS" disabled

     Connection establishment is possible using HTTP and HTTPS.

Additional requirements in the configuration of the CP 1543SP-1

Activate the firewall in the "Security" parameter group.

Depending on the protocol used you need to make the following further settings in the parameter group of the firewall "From external to station".

- With connection establishment using HTTP
  - Enable the "Allow HTTP" option.
  - Enable the "Allow HTTPS" option
    Reason: There is a switch to HTTPs after authentication on the Web server.
- With connection establishment using HTTPS
  - Disable the "Allow HTTP" option
  - Enable the "Allow HTTPS" option.

Establishing a connection to the Web server

Follow the steps below to connect to the Web server of the CPU from the engineering station.

These two variants are described in the following sections.

Connection establishment with HTTP

1. Connect the PC on which the new firmware file is located to the CP via the Ethernet interface.
2. Enter the address of the CP 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 keyword "Certificates for Web server".

When the connection has changed to the secure mode HTTPS (https://<IP address>/..." in the address box of the Web server), you can work with the Web server for example download a firmware file (see the following section).

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 is located to the CP or CPU via the Ethernet interface.
2. Enter the address of the CP in the address box of your web browser:
   https://<IP address>
3. Press the Enter key.

   The start page of the Web server opens.

You can work with the Web server.

Downloading firmware files via the Web server of the CPU

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

1. Log in on the start page of the Web server.
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.

Refer to the information on the duration of the firmware update in the section Downloading firmware (Page 106).

6.4 Processing status of the telecontrol e-mails

Configuration of the processing status of telecontrol e-mails (CP 1542SP-1 IRC)

The following status identifiers apply to e-mails configured with the message editor of the CP 1542SP-1 IRC, see also section Message configuration (Page 81).

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

Processing status of the telecontrol e-mails

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

Table 6- 2 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.

6.5 Downloading firmware

New firmware versions of the CP

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

Link: (https://support.industry.siemens.com/cs/ww/en/ps/22144/dl)

Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/dl)

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

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

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

- Loading the firmware with the online functions of STEP 7 via Ethernet / Internet

  The description of these methods follows.

- Downloading the firmware via the Web server of the CPU

  You will find the description of these methods in the section Web server of the CPU (Page 102).

Note

Duration of the firmware update

Downloading a new firmware file can take several minutes.

Note that the procedure takes longer the larger the station due to I/O modules.

Always wait until the completion of the firmware update can be recognized from the LEDs (LED pattern "Maintenance demanded" - End of the firmware update).

Loading the firmware with the online functions of STEP 7 via Ethernet / Internet

Requirements:

- The CP or the CPU can be reached via the IP address.
- The engineering station and the CP are located in the same subnet.
- The new firmware file is stored on your engineering station.
- The engineering station is connected to the network.
- The relevant STEP 7 project is open on the engineering station.

Procedure:

1. Select the CP or the CPU of the station whose CP you want to update with new firmware.
2. Enable the online functions using the "Connect online" icon.
3. In the "Connect online" dialog, select the Ethernet interface in the "Type of PG/PC interface" list box.
4. Select the slot of the CP or the CPU.

   Both methods are possible.
5. Click on "Start search" to search for the module in the network and to specify the connection path.

   When the module is found it is displayed in the table.
6. Connect using the "Connect" button.

   The "Connect online" wizard guides you through the remaining steps in installation.
7. In the network view, select the CP and select the "Online & Diagnostics" shortcut menu (right mouse button).
8. In the navigation panel of the Online & Diagnostics view select the entry "Functions > Firmware update".
9. Using the "Browse" button (parameter group "Firmware loader") search for the new firmware file in the file system of the engineering station.
10. Start to download the firmware with the "Start update" button when the correct version of the signed firmware is displayed in the "Status" output box.

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

6.6 Module replacement

CAUTION

Read the system manual "SIMATIC ET 200SP Distributed I/O System"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "SIMATIC ET 200SP Distributed I/O System" refer to the documentation in the Appendix.

When installing and connecting up, keep to the procedures described in the system manual "SIMATIC ET 200SP Distributed I/O System".

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

Module replacement

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 specifications

7

Technical specifications		
Article numbers	CP 1542SP-1	6GK7542-6UX00-0XE0
	CP 1542SP-1 IRC	6GK7542-6VX00-0XE0
	CP 1543SP-1	6GK7543-6WX00-0XE0
Attachment to Industrial Ethernet		
Quantity	1	
Design	Slot for bus adapter	
Properties	100BASE-TX, IEEE 802.3-2005, half duplex/full duplex, autocrossover, autonegotiation, galvanically isolated	
Transmission speed	10/100 Mbps	
Permitted cable lengths Ethernet, copper, at 100 Mbps *		
Cable type - Copper	Max. lengths	
TP Torsion Cable	• Max. 55 m TP Torsion Cable with IE FC RJ45 Plug 180 • Max. 45 m TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet	
TP FC Marine Cable, TP FC Trailing Cable, TP FC Flexible Cable, TP FC FRNC Cable, TP FC Festoon Cable, TP FC Food Cable	• Max. 85 m TP Torsion Cable with IE FC RJ45 Plug 180 • Max. 75 m TP Torsion Cable + 10 m TP Cord via IE FC RJ45 Outlet	
TP FC Standard Cable	• Max. 100 m TP FC Standard Cable with IE FC RJ45 Plug 180 • Max. 90 m TP FC Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet	
Permitted cable lengths Ethernet, fiber-optic cable (FO cable), at 100 Mbps *		
Cable type - Glass FO (multiode).	Max. lengths	
• FO FRNC Cable GP, FO Standard Cable GP, FO Ground Cable, FO Trailing Cable, FO Trailing Cable GP, FO Robust Cable GP	• Max. 2000 m	
• INDOOR FO cable, FO standard cable, flexible FO, trailing cable	• Max. 750 m	
• FO Robust Cable GP	• Max. 2000 m	
Cable type - PCF and plastic FO cable	Max. lengths	
• POF Standard Cable GP 980/1000, POF Trailing Cable 980/1000	• Max. 50 m	

Technical specifications		
• PCF Standard Cable GP, PCF Trailing Cable, PCF Trailing Cable GP	• Max. 100 m	
Electrical data		
External power supply (X80), design	Socket Terminal block for socket	Two terminals with reverse polarity protection 2 x two terminal for single or redundant power supply
Power supply (external)	• Type of voltage • Permitted low limit • Permitted high limit	• 24 VDC • 19.2 V • 28.8 V
Current consumption	• From 24 VDC (external) • From backplane bus (3.3 V)	• 250 mA (typ.) • 4 mA (typ.)
Maximum Inrush current	(Rated value)	12 A
Effective power loss	(typical)	6 W
Overvoltage category according to IEC / EN 60664-1	Category I	
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally	0 .. + 60 °C
	During operation with the rack installed vertically	0 .. + 50 °C
	During storage	-40 .. +70 °C
	During transportation	-40 .. +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Design, dimensions and weight		
Module format	Compact module ET 200SP	
Degree of protection	IP20	
Weight		
• Without bus adapter	• 180 g	
• With bus adapter 2xRJ45	• 230 g	
Dimensions (W x H x D)	60 x 117 x 74 mm	
Installation options	DIN rail (35 mm)	
Mean Time Between Failures (MTBF)		
• At + 40 °C	• 56.87 years	
• At + 60 °C	• 24.78 years	
Product functions **		

***** For details of the cable lengths see ET 200SP system manual, /2/ (Page 119).

****** You will find additional properties and performance data in the section Application and functions (Page 11).

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.

Scope of validity of the approvals

The approvals listed below are valid for the CP.

The tests required for the approvals were performed with a plugged-in bus adapter.

The bus adapters have their own approvals, that are not listed here.

EC declaration of conformity

CE

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

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

  Directive of the European Parliament and the Council of 26 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, official journal of the EC L174, 01/07/2011, page 88-110

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 on the Internet at the following address:

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

> Entry type: "Certificates", certificate type: "EC declaration of conformity"

IECEx

The CP meet the requirements of explosion protection according to IECEx.

IECEx certificate: IECEx DEK 14.0025X

The CP meets the requirements of the following standards:

- IEC 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/)

The conditions must be met for the safe deployment of the CP according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 31).

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 CP meets the requirements of the EC directive 2014/34/EU "Equipment and Protective Devices for Use in Potentially Explosive Atmospheres".

Applied 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'

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

ATEX approval: II 3 G Ex nA IIC T4 Gc

Test number: KEMA 07ATEX0145 X

The conditions must be met for the safe deployment of the CP according to the section Notes on use in hazardous areas according to ATEX / IECEx (Page 31).

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)

EMC

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

Applied standards:

- EN 61000-6-4

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

- EN 61000-6-2

  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments

RoHS

The CP meets the requirements of the EC directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Applied standard:

- EN 50581:2012

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)

Report / UL file: E85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: CULUS Listed E223122 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 T4
- Cl. 1, Zone 2, GP. IIC T4

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

Report / UL file: E223122 (NRAG, NRAG7)

Note the conditions for the safe deployment of the CP according to the section Notes on use in hazardous areas according to UL HazLoc (Page 31).

FM



Factory Mutual Approval Standard Class Number 3600, 3611, 3810

Class I, Division 2, Group A, B, C, D, T4 or Class I, Zone 2, Group IIC, T4

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

The conditions must be met for the safe deployment of the CP according to section General notices on use in hazardous areas according to FM (Page 32).

Australia - RCM



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

Marking for the customs union



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)

MSIP 요구사항 - For Korea only

Registration Number: MSIP-REI-S7M-ET200SP

A급 기기(업무용 방송통신기자재)

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

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

Dimension drawings

B

All dimensions in the dimension drawings are in millimeters.

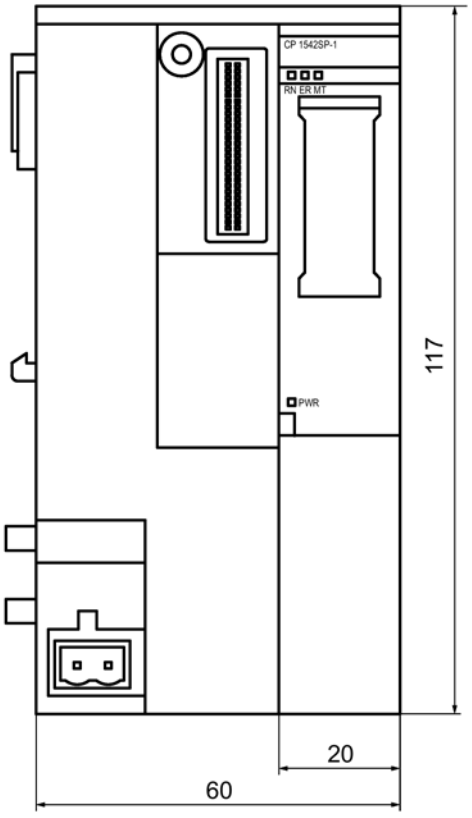


Figure B-1 Front view of the CP

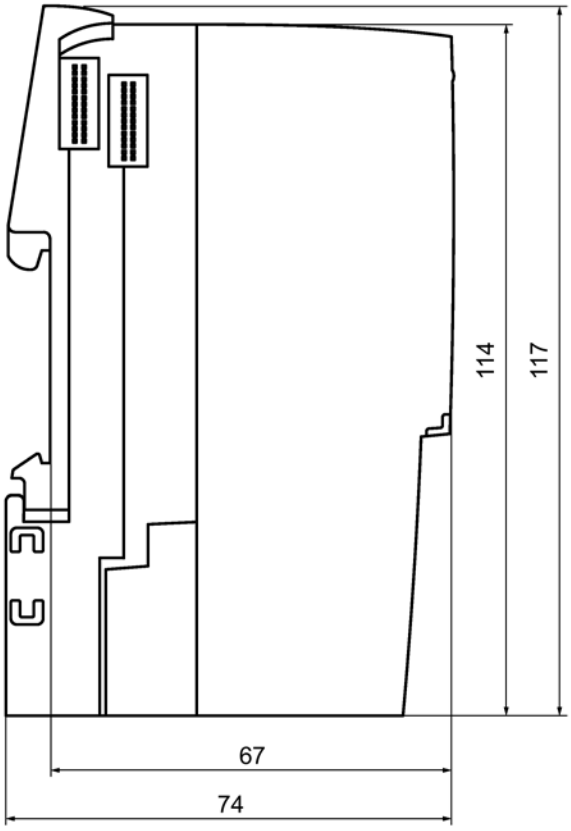


Figure B-2 Side view (left) of the CP

Accessories

C

C.1 BusAdapter

BusAdapter

To connect to the Ethernet network, the CP requires a BusAdapter. A BusAdapter does not ship with the CP.



Figure C-1 Example of a bus adapter, here BA SCRJ/RJ45

The CP supports the following bus adapters:

- BA 2×RJ45

  PROFINET bus adapter with the following connectors:

  – 2 x Ethernet jack RJ-45

  Article number: 6ES7193-6AR00-0AA0

- BA 2xFC

  PROFINET bus adapter with the following connectors:

  – 2 x direct connection of the bus cable (FastConnect)

  Article number: 6ES7193-6AF00-0AA0

- BA 2xSCRJ

  PROFINET bus adapter with the following connectors:

  – 2 x fiber-optic cable POF/PCF

  Article number: 6ES7193-6AP00-0AA0

- BA SCRJ/RJ45

  PROFINET bus adapter, media converter FO - copper with the following connectors:

  – 1 x fiber-optic cable POF/PCF

  – 1 x Ethernet jack RJ-45

  Article number: 6ES7193-6AP20-0AA0

- BA SCRJ/FC

  PROFINET bus adapter, media converter FO - copper with the following connectors:

  – 1 x fiber-optic cable POF/PCF

  – 1 x direct connection of the bus cable (FastConnect)

  Article number: 6ES7193-6AP40-0AA0

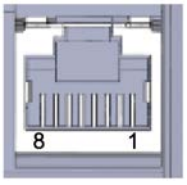
You will find further details in the manual /2/ (Page 119) and in the Siemens Industry Mall in Link: (https://mall.industry.siemens.com).

C.2 Assignment of the Ethernet interface of the bus adapter

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 C- 1 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

Documentation references

D

Where to find Siemens documentation

- Article numbers

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

  – SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI

  – SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70

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

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

- Manuals on the Internet

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

  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15247/man)

  Go to the required product in the product tree and make the following settings:

  Entry type “Manuals”

- Manuals on the data medium

  You will find manuals of SIMATIC NET products on the data medium that ships with many of the SIMATIC NET products.

/1/

SIMATIC
CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1
Operating instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/22144/man)
Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man)

/2/

SIMATIC
ET 200SP - Distributed I/O System
system manual
Siemens AG
Link: (http://support.automation.siemens.com/WW/view/en/58649293)

/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
Basics and Application
Configuration Manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15326/man)

/5/

SIMATIC NET
TIM DNP3
System manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15940/man)

/6/

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

/7/

SIMATIC NET
Industrial Ethernet / PROFINET
System manual
Siemens AG

- Industrial Ethernet
  Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465)
- Passive network components
  Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

Index

A

Abbreviations/acronyms, 4
Article number, 3

B

BusAdapter, 27

C

Conditional spontaneous, 72
Connection resources, 17
CPU firmware, 20
Cross references (PDF), 5

D

Data buffering, 17
DNP3
    Device profile, 13
    Protocol, 13

E

E-mail
    Configuration, 81
    Quantity, 18
Ethernet interface
    Assignment, 118
Events, 64

F

Firewall, 16
Firmware version, 3
Frame memory, 17

G

Gateway, 90
Glossary, 6

H

Hardware product version, 3

I

IEC 60870-5-104
    Device profile, 13
    Protocol, 13
Image memory, 64
IPv4, 14
IPv6, 14

M

MAC address, 3
MIB, 100
Mirroring back, 62

N

NTP, 44
NTP (secure), 44
IPsec tunnel,

O

Online diagnostics, 47, 99
Online functions, 99
OUC (Open User Communication), 95

P

Passive VPN connection establishment, 90
Power supply, 26
Pre-shared key (DNP3), 84
Process image, 64
Product name, 4

R

Replacing a module, 108
Reset trigger bit, 66

S

S7 connections - enable, 46
Safety notices, 29
Security, 15
Send buffer, 17, 64
Service & Support, 6
SIMATIC NET glossary, 6
Slot rules, 33
SMTPS, 86
SNMP, 15, 100
SNMPv3, 17
STARTTLS, 86
Static values, 64
STEP 7 version, 20

T

TCSB, 4
TeleControl Basic, 13
Telecontrol server, 4
Time stamp, 60
TLS, 86
Training, 6
Transmission mode, 67, 72
Trigger tag - resetting, 71
TSCB
    Version, 13

U

Unsolicited, 72

V

Virtual IP address, 55
VPN, 19, 86