SIEMENS

SIMATIC NET

ET 200SP - Industrial Ethernet SIMATIC CP 154xSP-1

Operating Instructions

CP 1542SP-1
CP 1542SP-1 IRC
CP 1543SP-1

02/2023

C79000-G8976-C426-06

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
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C426-06
Ⓟ 02/2023 Subject to change

Preface

Validity of this manual

This document contains information on the following modules:

- **CP 1542SP-1**
  Article number **6GK7542-6UX00-0XE0**
  Hardware product version 2
  Firmware version V2.2
  Communications processor for connecting a SIMATIC ET 200SP CPU to Industrial Ethernet
- **CP 1542SP-1 IRC**
  Article number **6GK7542-6VX00-0XE0**
  Hardware product version 2
  Firmware version V2.2
  Communications processor for connecting a SIMATIC ET 200SP CPU via Industrial Ethernet to a control center (TCSB, ST7, DNP3, IEC 60870-5-104)
- **CP 1543SP-1**
  Article number **6GK7543-6WX00-0XE0**
  Hardware product version 2
  Firmware version V2.2
  Communications processor for connecting a SIMATIC ET 200SP CPU to Industrial Ethernet, Security

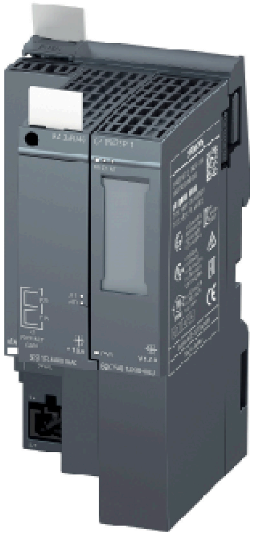


Figure 1 CP 1542SP-1 with plugged in BusAdapter (here BA 2xRJ45)

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 MAC address of the interface is printed on the front at the bottom left, above the connectors for the power supply:

- 00:1B:1B:xx:xx:01 (interface)

You can learn the MAC addresses of the ports via the online functions of STEP 7 (assessible devices):

- 00:1B:1B:xx:xx:02 (port X1P1)
- 00:1B:1B:xx:xx:03 (port X1P2)

New in this edition

- New hardware version with support of additional BusAdapters, see appendix BusAdapter (Page 111).
- New firmware version V2.2 with the following new functions (CP 1542SP-1 IRC):
  - TLS extension for the protocol DNP3
  - TLS extension for the protocol IEC 60870-5-104
  - Secure authentication for the protocol IEC 60870-5-104

  The three new functions require an ET 200SP CPU as of firmware version V2.9.

  For a description of the functions, refer to the respective configuration manual; see "Structure of the documentation" below.
- New approvals (CCC / UKEX)
- Editorial revision

Restriction:

In telecontrol operation with the protocol IEC 60870-5, observe the following:

If the values are sent by two setpoint data points at almost the same time, the second setpoint transmission may be ignored. Observe an interval of at least 70 milliseconds between sending of setpoints.

Replaced edition

Edition 12/2019

New contents in the edition 12/2019:

- New firmware version V2.1, with the following functions among others:
  - Support of additional SDTs for OUC blocks
  - Greater number of configurable data points (telecontrol), see Configuration limits and performance data (Page 24).
  - Direct communication of the CP 1542SP-1 IRC between (DNP3 / IEC 60870-5)

- Description of the functions of firmware version V2.0:
  - Connection to SINEMA Remote Connect (CP 1542SP-1 IRC / CP 1543SP-1)
  - Configured e-mail independent of telecontrol communication (CP 1542SP-1 IRC / CP 1543SP-1)
  - Support of the telecontrol protocol SINAUT ST7 (CP 1542SP-1 IRC)
  - Time-of-day synchronization via time of day of the communication partner (CP 1542SP-1 IRC)

  Released CPUs for CP firmware V2.0: CPUs as of firmware V2.0

  Functions configurable in: STEP 7 Professional as of V15
- New ATEX/IECEx approval
- New structure of the documentation

  The documentation for the CP consists of these operating instructions and additional configuration manuals for the CP 1542SP-1 IRC, see below.

Current manual edition on the Internet

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

- 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)

Structure of the documentation

The documentation for the three CP types consists of the following manuals and contents:

- **Operating instructions**

  Valid for all three CP types
  - Application and functions
  - Requirements (CPUs, configuration software, etc.)
  - Hardware description
  - Installation, wiring, commissioning, operation
  - Configuration of the CP 1542SP-1 and CP 1543SP-1

    For information on configuring the CP 1542SP-1 IRC, refer to the configuration manuals.
  - Diagnostics, maintenance
  - Technical specifications, approvals, accessories

- **Configuration manuals (CP 1542SP-1 IRC)**

  Configuration of the CP 1542SP-1 IRC is described in the following additional documents:

  - **SINAUT ST7 system manual**

    Volume 3 - Configuration under STEP 7 Professional (TIA Portal)
  - **Configuration manual Telecontrol Basic**

    Configuration and diagnostics in STEP 7 Professional (TIA Portal)
  - **Configuration Manual DNP3**

    Configuration and diagnostics in STEP 7 Professional (TIA Portal)
  - **Configuration Manual IEC**

    Configuration and diagnostics in STEP 7 Professional (TIA Portal)

You can find the Internet links for the manuals in the appendix Documentation references (Page 121).

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

Notes on this document

Product name

- **CP / module / device**

  When properties listed in this manual are valid for all three types of CP, these names are used in place of the complete product names of all three types of CP.

  If information is only valid for specific types of CP, the respective CP names are listed in the text or in the section header.

Cross-references

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

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

Search

To display all instances of a search term in a list, some PDF readers support the command <Ctrl>+<Shift>+<F>.

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_99.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 constitute one element of such a concept.

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

For additional information on industrial security measures that may be implemented, please visit
Link: (http://www.siemens.com/industrialsecurity)

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

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

See also:
Security functions (CP 1542SP-1 IRC, CP 1543SP-1) (Page 19)
Security recommendations (Page 51)

Firmware

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

Note on firmware/software support

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

Device defective

If a fault develops, please send the device to your Siemens representative for repair. Repairs on-site are not possible.

Decommissioning

Shut down the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, restore the factory settings on the device.

You achieve this by resetting the CPU using the online functions of STEP 7.

Recycling and disposal

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

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

Keep to the local regulations.

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

SIMATIC NET glossary

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

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:

- On the accompanying DVD
- In the Siemens Industry Online Support at the following address:

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

Training, Service & Support

You will find information on training, service 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

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 BusAdapter. The BusAdapter is not supplied with the CP. For information on the compatible BusAdapters, refer to the section BusAdapter (Page 111).

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

- **CP 1542SP-1**

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

- **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.

- **CP 1542SP-1 IRC**

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

  – TeleControl Basic

    For connection of the ET 200SP CPU to a control center with telecontrol server (TCSB)

  – ST7

    For connection of the ET 200SP CPU to a control center with SINAUT ST7

  – DNP3

    For connection of the ET 200SP CPU to DNP3 master

  – IEC 60870-5-104

    For connection of the ET 200SP CPU to IEC master

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
  - USEND/URCV for uncoordinated data exchange with a remote partner
  - BSEND/BRCV for exchanging large volumes of data with a partner
  - PG functions
  - Operator control and monitoring functions (HMI)

  For fully specified S7 connections, the CP requires a fixed IP address.
- **S7 routing**
  - Routing of S7 connections via the backplane bus and the CPU to other S7 stations
- **SINEMA Remote Connect (SINEMA RC)**

  As of firmware version V2.0, the following CP types support communication via SINEMA RC as of software version V1.3:
  - CP 1542SP-1 IRC
  - CP 1543SP-1

  See section Communication via SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1) (Page 17).

  For the manual, see /8/ (Page 123).
- **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 Program blocks (Page 81).
- **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 (CP 1542SP-1 IRC) (Page 15).

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 19).

1.4 Telecontrol communication (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 and other telecontrol stations:

- **TeleControl Basic ***

  Proprietary protocol 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 /4/ (Page 122).

- **ST7**

  Proprietary protocol for telecontrol applications in the SINAUT ST7 system. The protocol is used to connect the CP to ST7 control centers.

  The SINAUT ST7 supports the following functions, among others:

  – Communication with the master station

  – Communication with other stations

  – MSC transmission protocol

    Under SINAUT S7, the CP uses the following variants of the MSC transmission protocol on OSI layer 3:

    - MSC (default setting)

    - MSCsec when security requirements are higher ("Security" activated)

  – Communication using mobile wireless

    Communication via a mobile wireless network combined with the Internet is made possible by a SCALANCE M router. The SCALANCE M product series provides various VPN routers with IPsec, encryption software and their own firewall.

    You will find a list of routers in the appendix IP-based routers (Page 114).

- **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 of the DNP3 protocol that are supported by the CP in the DNP3 device profile; see
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man)

  Communications partners of the CP can be:

  DNP3 master:

  – SIMATIC PCS 7 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 122).

  – Third-party systems that support the DNP3 specification named above.

  DNP3 stations (outstation):

  – CPUs in stations

    For direct communication, the "Master function" is enabled for the sending data point.

- **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 of the IEC specification that are supported by the CP in the IEC device profile; see
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man)

  Communications partners of the CP can be:

  IEC master:

  – SIMATIC PCS 7 TeleControl

  – SIMATIC WinCC TeleControl

  – SIMATIC WinCC OA

  – Third-party systems that support the IEC specification named above.

  Stations:

  – CPUs in stations

    For direct communication, the "Master function" is enabled for the sending data point.

* Optional telecontrol communication with the master station via SINEMA Remote Connect, see section Communication via SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1) (Page 17).

Further properties of the CP 1542SP-1 IRC

- **Data point configuration**

  The process values are configured as data points for the 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 for the specific data points in the CP. Each data point addresses a PLC tag or element in a data block of the CPU.

  The data points can be processed individually in the control system.

- **Messages / e-mail**

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

- **Send buffer**

  The CP saves the values of data points configured as an event in the send buffer. It transmits the data from the send buffer spontaneously or bundled to the communications partner.

  The data is not saved retentively. It is lost in the event of a power failure.

- **Analog value processing**

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

You can find additional information in the telecontrol configuration manuals, refer to /10/ (Page 123).

1.5 Communication via SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1)

Validity

The following types of communication via SINEMA Remote Connect are supported by the CPs:

- CP 1543SP-1
  - Remote maintenance via SINEMA Remote Connect
- CP 1542SP-1 IRC
  - Remote maintenance via SINEMA Remote Connect
  - Telecontrol communication via SINEMA Remote Connect

Consider this in the applications described below.

Communication via SINEMA Remote Connect (SINEMA RC)

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

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

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

For the CP firmware version required for communication via SINEMA RC see section Communications services (Page 14).

Parameter groups

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

- Communication via SINEMA RC:

  > "Security > VPN"

- Telecontrol communication via SINEMA RC:

  > "Communication types"

  For information on the configuration, refer to the telecontrol configuration manuals /10/ (Page 123).

Applications

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

Application example:

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

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

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

Table 1- 1 Use cases and parameters to be activated

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

***** Explanation of the parameter abbreviations:

SRC - Security > VPN (activated) > "VPN connection type":
"Automatic OpenVPN configuration via SINEMA Remote Connect Server"

TC - Communication types > Telecontrol communication enabled

TC-SRC - Communication types >
"Activate telecontrol communication via SINEMA Remote Connect"

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

Security functions are available for the following CP types:

- CP 1543SP-1

  The security functions are enabled in the configuration of the CP.

- CP 1542SP-1 IRC

  You will find a description of the security functions in the telecontrol configuration manuals, see /10/ (Page 123).

For information on the security functions of the Open User Communication program blocks, see section Program blocks (Page 81).

For information on the encryption methods used, see appendix Encryption methods (Ciphers) (Page 115).

Note

Recommendation for critical security plants

Refer to the information in the section Security recommendations (Page 51).

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 to restrict flooding and DoS attacks ("Define IP packet filter rules")

- **Certificates**

  Certificates are used for the secure authentication of the communications partners.

- **VPN**

  The following alternatives can be used:

  - Secured communication via IPsec tunnels

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

  - Remote maintenance via SINEMA Remote Connect

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

    For information on the configuration, see section SINEMA Remote Connect (Page 68).

- **Logging**

  Sending of events can be enabled for monitoring. The events can be read out using STEP 7 or sent to a Syslog server.

- **Encrypted e-mails**

  For secure transfer of information with encrypted e-mails, you can use the following as an alternative:

  – SSL/TLS

  – STARTTLS

  For information on the configuration, see section E-mail configuration (Page 66).

- **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 (CP 1543SP-1) (Page 63).

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

CP 1542SP-1 IRC

The CP supports the following security functions:

- **Encrypted e-mails**

  For secure transfer of information with encrypted e-mails, you can use the following as an alternative:

  – SSL/TLS

  – STARTTLS

  For information on the configuration, see section E-mail configuration (Page 66).

- **Certificates**

  Certificates are used for the secure authentication of the communications partners.

- **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 the CP and telecontrol server can be set.

  The telecontrol password is used to authenticate the CP on the telecontrol server.

  If the security functions are enabled, the CP can process telecontrol communication via SINEMA Remote Connect.

- **ST7**

  The transmission protocols that can be used by the CP for telecontrol communication via the ST7 protocol support the following security functions:

  – MSC

    The MSC protocol supports authentication of the communications partners and simple encryption of data. A user name and a password are included in the encryption. A tunnel is established between the MSC station and MSC master station.

  – MSCsec

    In addition to MSC, with MSCsec, the shared automatically generated key is renewed between the communications partners at configurable intervals.

- **DNP3**

  The CP supports the use of TLS connections as well as secure authentication according to IEEE 1815.

  If the security functions are enabled, the CP can process telecontrol communication via SINEMA Remote Connect.

- **IEC 60870-5-104**

  The CP supports the use of TLS connections as well as secure authentication according to IEC 60870-5-7.

  If the security functions are enabled, the CP can process telecontrol communication via SINEMA Remote Connect.

For information on communication via SINEMA Remote Connect, see section Communication via SINEMA RC (CP 1542SP-1 IRC, CP 1543SP-1) (Page 17).

1.7 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

    The CP can synchronize its time of day via NTP.

    CP 1543SP-1: If the Security functions are enabled, the secure method NTP (secure) can be used.
  - CP 1542SP-1 IRC: Time from partner

    If telecontrol communication is enabled, the CP can also obtain its time of day via from the communications partner.

    UTC time is used for TeleControl Basic and DNP3.

    The local time of the partner PC is used for ST7 and IEC.
  - The CP can make the time-of-day available to the CPU via a PLC tag.

  For more detailed information, refer to section Time-of-day synchronization (Page 58).
- **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 63).
- **E-mail**

  The CP 1542SP-1 IRC and CP 1543SP-1 support sending e-mails.

1.8 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 43).

Connection resources

Connection resources - valid for all CP variants

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

- S7: Max. 16 (including connections for S7 routing)
- 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

CP 1543SP-1

Security functions of the CP 1543SP-1

- **VPN tunnel (IPsec)**

  A maximum of four **IPsec** 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")

- **E-mail (via message editor)**

  Up to 10 e-mails to be sent can be configured.

  Maximum number of characters that can be transferred per e-mail: 256 ASCII characters including any value sent at the same time

CP 1542SP-1 IRC

Telecontrol functions of the CP 1542SP-1 IRC

- **Telecontrol connections**

  – TeleControl Basic

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

  – SINAUT ST7

    The CP can establish up to eight ST7 connections, of which maximum:

    - 8 individual connections with partners

    - 4 redundant connections with partners

    - 8 connections for inter-station communication between ST7 stations

    - A combination of the three options

  – DNP3 / IEC 60870-5-104

    Connections to up to four single or redundant masters can be established.

- **E-mail (via message editor)**

  Up to 10 e-mails to be sent can be configured.

  Maximum number of characters that can be transferred per e-mail: 256 ASCII characters including any value sent at the same time

- **Frame memory (send buffer)**

  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 ("Communication with the CPU" parameter group).

  The maximum size of the send buffer with the respective remote control protocol is:

  – TeleControl Basic

    64000 frames

  – SINAUT ST7

    32000 frames

  – DNP3

    100000 events

  – IEC 60870-5-104

    100000 events

  For details of how the send buffer works such as storing events as well as the options for transferring the data, see /10/ (Page 123).

- **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. For details, see /10/ (Page 123).

  – Telecontrol Basic: 500

  – ST7: 1500

  – DNP3: 1500

  – IEC: 1500

1.9 Requirements for use

1.9.1 Hardware requirements

Bus adapter

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

You can find the BusAdapters supported by the CP in the appendix BusAdapter (Page 111).

CPUs 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

  Article number: 6ES7510-1DK03-0AB0
- CPU 1510SP F-1 PN

  Article number: 6ES7510-1SJ01-0AB0

  Article number: 6ES7510-1SK03-0AB0
- CPU 1512SP-1 PN

  Article number: 6ES7512-1DK01-0AB0

  Article number: 6ES7512-1DM03-0AB0
- CPU 1512SP F-1 PN

  Article number: 6ES7512-1SK01-0AB0

  Article number: 6ES7512-1SM03-0AB0
- CPU 1514SP-2 PN

  Article number: 6ES7514-2DN03-0AB0
- CPU 1514SP F-2 PN

  Article number: 6ES7514-2SN03-0AB0
- CPU 1514SP T-2 PN

  Article number: 6ES7514-2VN03-0AB0
- CPU 1514SP TF-2 PN

  Article number: 6ES7514-2WN03-0AB0

The respective SIPLUS CPUs are also supported.

Note

Keep the firmware version of the CPUs and communications modules up to date

To avoid possible problems when using newer CPUs together with older communications modules, you should keep the firmware of both your communications modules and your CPUs up to date.

Other components of the ET 200SP

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 /3/ (Page 122) 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.

1.9.2 Software requirements

Configuration software

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

- STEP 7 Professional V16 or higher

To configure the new functions of the firmware V2.2, the CP 1542SP-1 IRC requires the following STEP 7 versions:

- STEP 7 Professional V18

Software for online functions

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

- STEP 7 Professional V16 or higher

CPU firmware

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

Check regularly for new firmware versions or security updates and apply them.

1.10 Configuration examples

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

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.

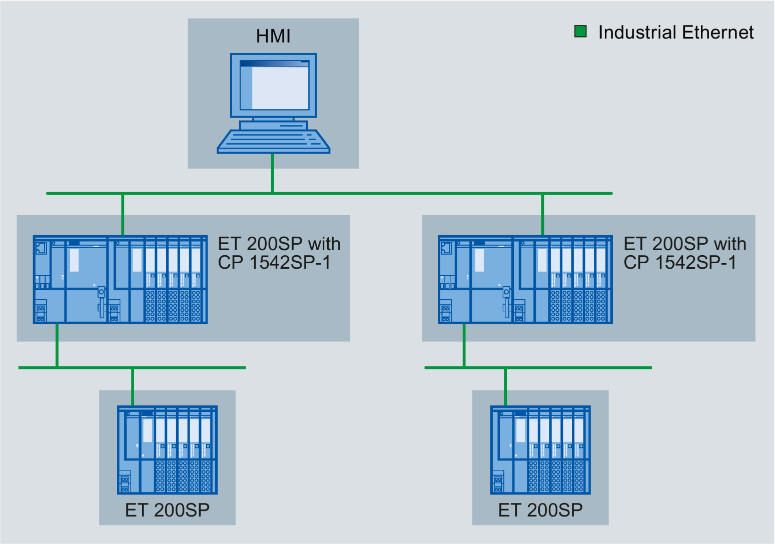


Figure 1-1 Configuration example of an ET 200SP with CP 1542SP-1

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.

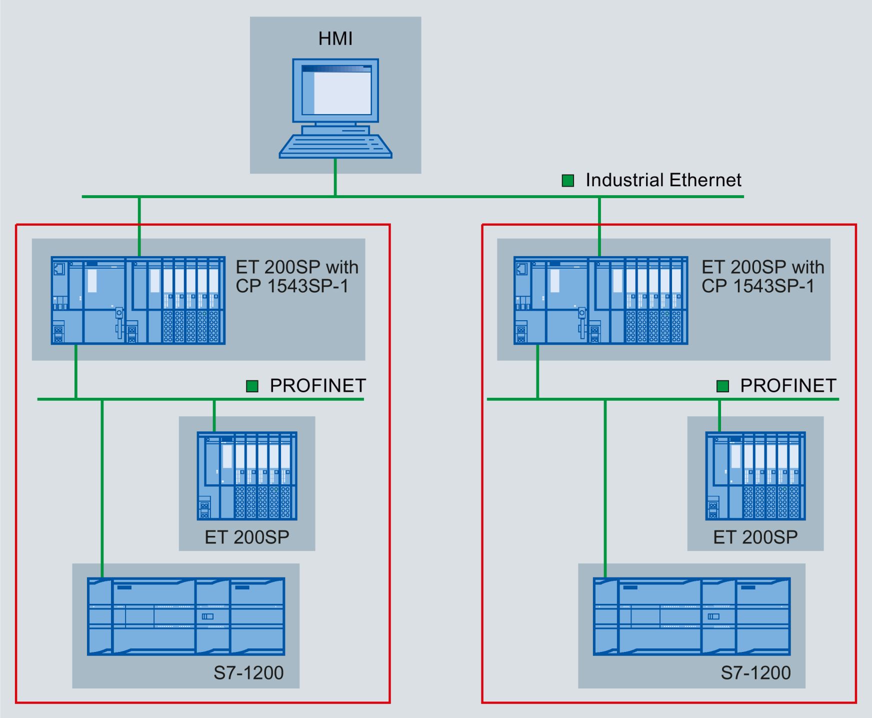


Figure 1-2 Configuration example of an ET 200SP with CP 1543SP-1

CP 1542SP-1 IRC - Connection to control centers

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

- TeleControl Basic
- SINAUT ST7
- IEC 60870-5-104
- DNP3

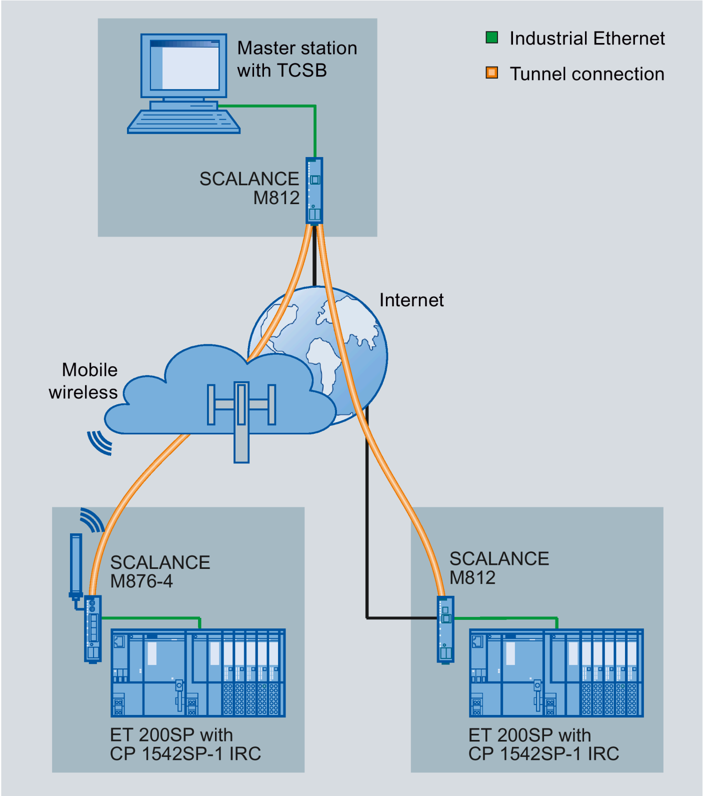


Figure 1-3 Configuration example of an ET 200SP with CP 1542SP-1 IRC; protocol: TeleControl Basic

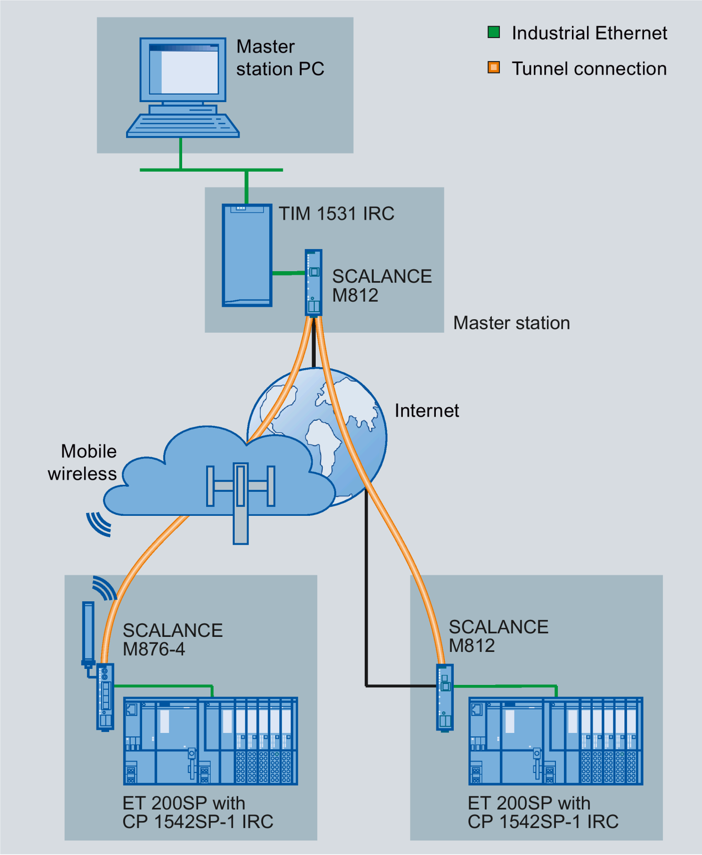


Figure 1-4 Configuration example of an ET 200SP with CP 1542SP-1 IRC; protocol: ST7

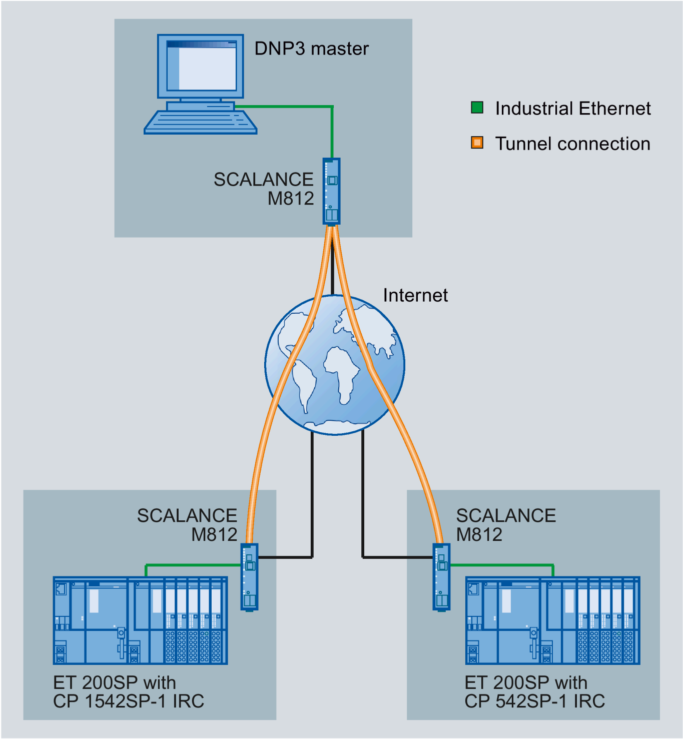


Figure 1-5 Configuration example of an ET 200SP with CP 1542SP-1 IRC; protocol: DNP3

A configuration with which the protocol IEC 60870-5-104 is used could look similar.

Telecontrol via SINEMA Remote Connect

The following figure shows a configuration in which the CP 1542SP-1 IRC communicates with the master station via a SINEMA Remote Connect Server. In this example, the CP uses the protocol IEC 60870-5-104.

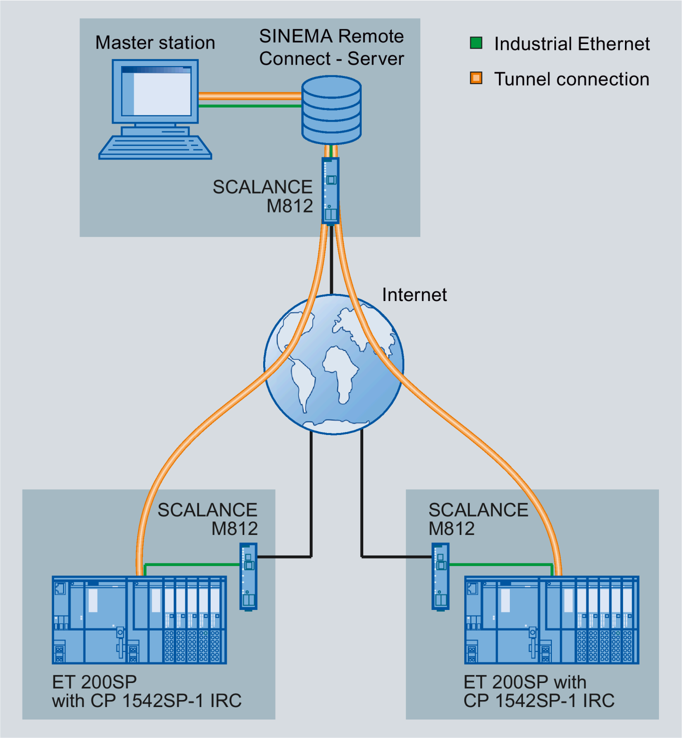


Figure 1-6 Configuration example of an ET 200SP with CP 1542SP-1 IRC for telecontrol communication via SINEMA RC

Remote maintenance with SINEMA RC

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

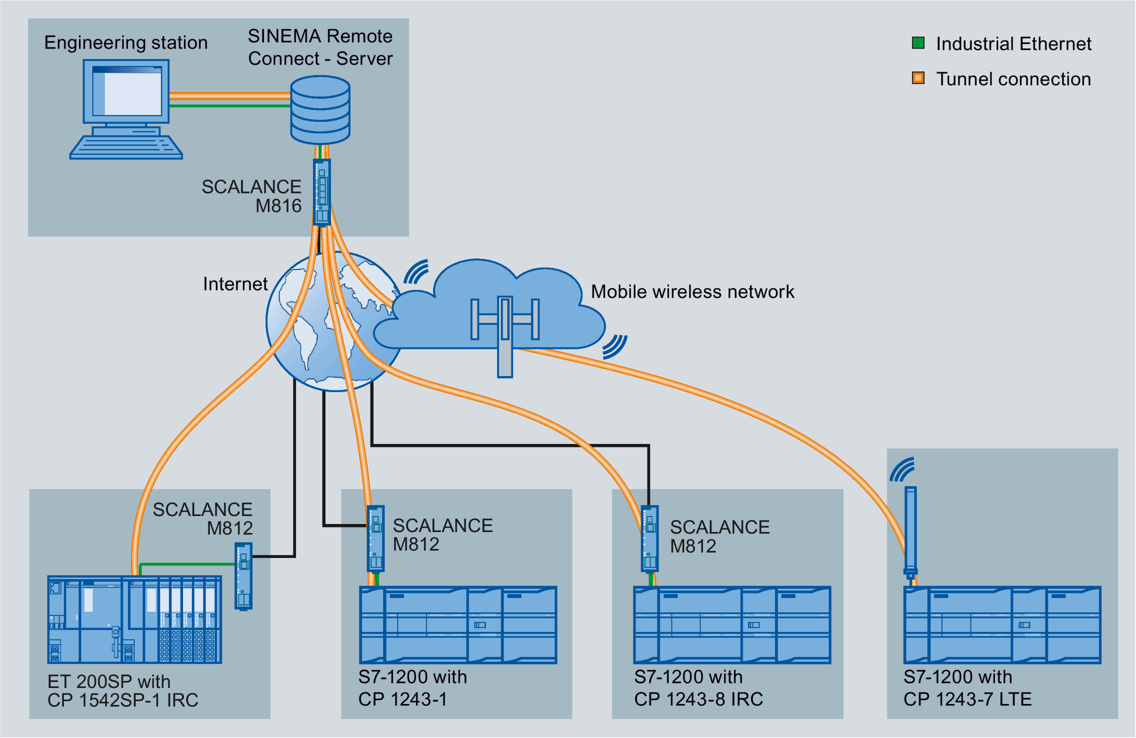


Figure 1-7 Connection of stations to engineering station via SINEMA RC

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
🟢	✺🟢	○	○	• Startup • 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.

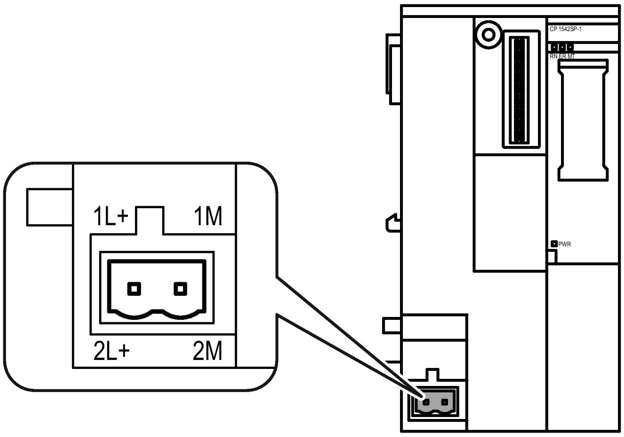


Figure 2-1 Power supply of the CP

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 43) and Connecting the CP (Page 47).

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 of the CP 154xSP-1 (Page 99).

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:

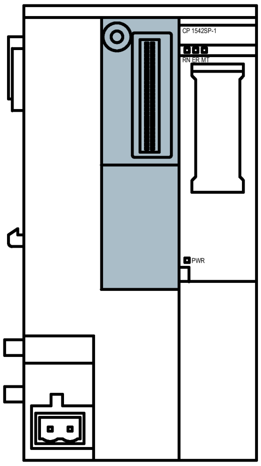


Figure 2-2 Front of the CP, the slot for the bus adapter is marked gray.

You will find the bus adapters supported by the CP in section BusAdapter (Page 111).

For information on installing and connecting up, refer to the sections Installing the CP (Page 43) and Connecting the CP (Page 47).

You will find the pinout of the Ethernet interface in section BusAdapter (Page 111). You will find further technical specifications of the bus adapter in the manual /3/ (Page 122).

Installation, wiring, commissioning 3

3.1 Important notes on using the device

Safety notices on the use of the device

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

Overvoltage protection

NOTICE

Protection of the external power supply

If power is supplied to the module or station over longer power cables or networks, the coupling in of strong electromagnetic pulses onto the power supply cables is possible. This can be caused, for example by lightning strikes or switching of higher loads.

The connector of the external power supply is not protected from strong electromagnetic pulses. To protect it, an external overvoltage protection module is necessary. The requirements of EN61000-4-5, surge immunity tests on power supply lines, are met only when a suitable protective element is used. A suitable device is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element.

Manufacturer:
DEHN+SOEHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt, Germany

3.1.1 Notes on use in hazardous areas

⚠**WARNING**

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

⚠**WARNING**

EXPLOSION HAZARD

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

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

⚠ **WARNING**

Requirements for the cabinet

To comply with EU Directive 2014/34 EU (ATEX 114), UK Regulation SI 2016/1107 or the conditions of IECEx or CCC-Ex, the housing or cabinet must meet the requirements of at least IP54 (according to EN/IEC 60529, GB/T 4208) in compliance with EN IEC/IEC 60079-7, GB 3836.3.

⚠ **WARNING**

Suitable cables at high ambient temperatures in hazardous area

Use heat-resistant cables with an ambient temperature ≥ 60 °C; these cables must be rated for an ambient temperature that is at least 20 °C higher. The cable entries used on the housing must comply with the IP degree of protection required by EN IEC 60079-0 / GB 3836.1.

⚠ **WARNING**

Transient overvoltages

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

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

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

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

⚠ **WARNING**

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**

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

⚠ **WARNING**

EXPLOSION HAZARD

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

3.2 Installation, removal and repairs in hazardous areas

⚠ **WARNING**

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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

⚠ **WARNING**

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

⚠ **WARNING**

Improper installation of shielded cables

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

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

⚠ **WARNING**

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

⚠ **WARNING**

Unprotected cable ends

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

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

⚠ **WARNING**

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

⚠ **WARNING**

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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

3.3 Installing, connecting and commissioning

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

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

⚠ **WARNING**

Open equipment

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

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

3.3.1 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

Observe installation guidelines

When installing and connecting up the CP note the instructions in the manual /3/ (Page 122).

NOTICE

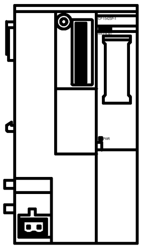
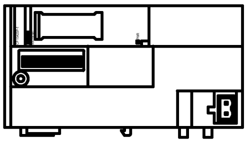
Installation location - Dependency of the temperature range

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 on 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 of the CP 154xSP-1 (Page 99).

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

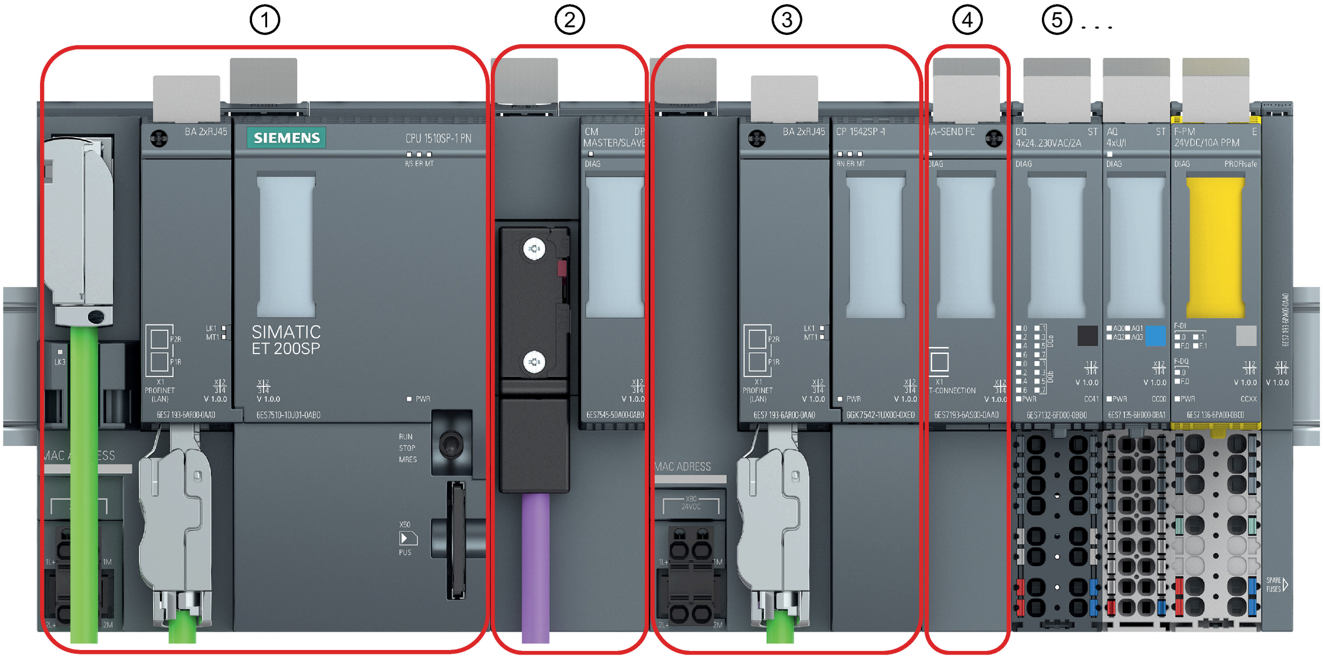
Slot rules

The CPU always occupies slot 1. In an ET 200SP you can plug in up to three of the following modules in slots 2 ... 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.

The CM DP can only be plugged in directly next to the CPU.



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 according to ATEX / UKEX / IECEx / CCC-Ex (Page 40).

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 /3/ (Page 122) 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.

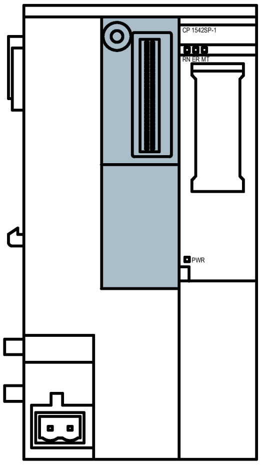


Figure 3-2 Front of the CP, the slot for the bus adapter is marked gray.

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 /3/ (Page 122).

WARNING

Power supply

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

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

- Only safety extra low voltage (SELV) with limited power source (LPS) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.

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

3.3.2 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 122).

The bus adapter is already connected to the relevant cable, see section Installing the CP (Page 43).

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 36). 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 99).

3.3.3 Commissioning the CP

Requirement: Configuration prior to commissioning

A prerequisite for full commissioning of the module is the completeness of the STEP 7 project data.

Commissioning the module

Further commissioning involves the following steps:

1. Compiling the project data
2. Downloading the STEP 7 project data to the device

   The STEP 7 project data of the CP is transferred when you load to the station.

   To load the station, connect the engineering station on which the project data is located to the CPU.

You will find more details in the STEP 7 information system in the section "Compiling and downloading project data".

Note

Time-of-day synchronization when using SINEMA RC

When the CP obtains the time from the CPU, set the CPU time manually during commissioning when using SINEMA Remote Connect; see note in section Commissioning the CP (Page 48).

Manual setting the time of day during commissioning

Note

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

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

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

Recommendation:

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

3.4 Disassembly

⚠ **WARNING**

Improper disassembly

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

For proper disassembly, observe the following:

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

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.

Configuration 4

4.1 Security recommendations

Observe 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.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Check regularly for new features on the Siemens Internet pages.
  - You can find information on Industrial Security here:
    Link: (http://www.siemens.com/industrialsecurity)
  - You can find a selection of documentation on the topic of network security here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.

  Information regarding product news and new firmware versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/22144/dl)
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/dl)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

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

  Configure access to the CPU under "Protection and Security".

  Use the other security functions of the CPU to prevent unauthorized access to the station.

  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 limiting the "transmission speed" via IP packet filter rules in the firewall, you make use of the possibility of restricting flooding and DoS attacks.

  – Use the secure protocol variants NTP (secure) and SNMPv3.

  – 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 deactivated.

- Protection of the passwords for access to program blocks

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

- Logging function

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

Passwords

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

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

Protocols

Secure and non-secure protocols

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

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

Table: Meaning of the column titles and entries

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

- **Protocol / function**

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

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

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

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

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

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

    As default the port is open. After this port is configured, the communications partner needs to log in.
  - 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.

Table 4- 1 Server ports (all three CP types)

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
S7 and online connections	102 (TCP)	Open	Open	No
HTTP	80 (TCP)	Closed	Open after configuration	Yes

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Open	Open after configuration	No

Table 4- 2 Additional server ports with CP 1542SP-1 IRC and CP 1543SP-1

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
Online security diagnostics	8448 (TCP)	Closed	Open after configuration *	Yes
SNMP	161 (UDP)	Open	Open after configuration	Yes (SNMPv3)
Communication via SINEMA RC	443 (TCP), 5243 (UDP)	Closed	Open after configuration	Yes
IPsec	500 (UDP)	Closed	Open after configuration	Yes

* Some service providers consider the opening of port 102 a security vulnerability.
To avoid opening the port during online diagnostics, see section Online security diagnostics via port 8448 (CP 1542SP-1 IRC, CP 1543SP-1) (Page 90).

Table 4- 3 Additional server ports with CP 1542SP-1 IRC

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
DNP3	20000 (TCP/UDP) Can be set	Closed	Open after configuration	Yes, when Secure Authentication is enabled.
DNP3 with TLS	19999 (TCP) Can be set	Closed	Open after configuration	Yes, when Secure Communication is enabled.
IEC 60870-5-104	2404 (TCP) Can be set	Closed	Open after configuration	No
IEC 60870-5-104 with TLS	19998 (TCP) Can be set	Closed	Open after configuration	Yes, when Secure Communication is enabled.

Ports of communication partners and routers

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

These can be:

- TeleControl Basic / 55097 (TCP) - Can be set
- ST7 with MSC protocol / 26382 (TCP) - can be set
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)

- SSL/TLS / 465 (TCP)
- NTP / NTP (secure) / 123 (UDP)
- SINEMA RC Autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)
- OpenVPN / 1194 (UDP)
- Syslog / 514 (UDP)

4.2 Configuration in STEP 7

Configuration in STEP 7

You configure the modules and networks in SIMATIC STEP 7. You will find the required version in the section Software requirements (Page 28).

Note

Configuration of the CP 1542SP-1 IRC

You will find a description of the basic configuration of the CP 1542SP-1 IRC in the following sections.

You will find a description of the configuration of telecontrol communication of the CP 1542SP-1 IRC in the relevant configuration manual, see /10/ (Page 123).

Overview of configuration of the CP

Follow the steps below when configuring:

1. Create a STEP 7 project.
2. Insert the required SIMATIC stations from the following catalog directory:

   Controller > SIMATIC ET200 CPU > ET 200SP CPU
3. Insert the CPs and the input and output modules from the following catalog directory into the stations:

   Distributed I/O > ET 200SP

   You can configure a maximum of two CP 154xSP-1 for an ET 200SP.
4. Create an Ethernet network.
5. Connect the stations to the Ethernet subnet.

6. Configure the inserted CPs.

   When the device view of the CP is open, you can find the BusAdapters in a separate catalog directory.

   You will find detailed information about the security functions in the section Security (CP 1543SP-1) (Page 63).
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.

Downloading the configuration data

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

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

4.3 Communication types (CP 1543SP-1)

Validity: CP 1543SP-1

You will find the description of the CP 1542SP-1 IRC in the relevant configuration manual.

"Communication types" parameter group

To minimize the risk of unauthorized access to the station via Ethernet, you need to enable the following communications services for the CP.

- **Activate online functions**

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

  If the option is disabled, you have no access to the CPU via the CP with the online functions. Online diagnostics of the CPU with a direct connection to the interface of the CPU however remains possible.
- **Enabling S7 communication**

  Enables the functions of S7 communication between the engineering station and the station CPU, as well as S7 routing.

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

  Please note:
  Disabling this function means no security measure. To protect the station, use suitable security functions such as firewall, VPN or password protection of the CPU.

Open User Commmunication does not need to be enabled since you then need to create the relevant program blocks. Unintended access to the CP is therefore not possible.

4.4 Ethernet interface

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

- General data (name etc.)
- Addresses and possibly routers

  Note:
  When using SINEMA Remote Connect, the CP requires fixed IP addresses (IPv4/IPv6).
- Port settings
- Access to the Web server

4.4.1 IPv6

Manual configuration of IPv6 addresses

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

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

Communication partner and IPv6

Note

Internet communication via IPv6

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

OUC communication via IPv6

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

4.4.2 Advanced options

Telecontrol-specific transmission settings of the CP 1542SP-1 IRC

You can find a description of telecontrol-specific transmission settings of the CP 1542SP-1 IRC in the relevant configuration manual, see Documentation references (Page 121).

BA ... (BusAdapter)

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

You will find the supported BusAdapters in appendix BusAdapter (Page 111).

Inserting a BusAdapter

As default setting, the CP uses a "BA 2xRJ45" BusAdapter.

If you are using a different BusAdapter, first go to the device view of the CP.

Open the "BusAdapter" directory on the right in the catalog and drag the BusAdapter to be used onto the interface of the CP. Insert the new BusAdapter via the "Change device" dialog.

Configuring the BusAdapter

In the "Ethernet interface > Advanced options > BA ..." parameter group of the CP, you configure the settings of the network connection via the BusAdapter.

If you do not use both ports of the BusAdapter, you can disable one of the two ports in the "Activate" parameter group.

4.4.3 Access to the Web server

Access to the Web server of the CPU

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

From a PC you can access the Web server of the station if the PC is connected to the system network via LAN.

You will find information on the Web server of the ET 200SP in the manual /2/ (Page 122).

4.5 Time-of-day synchronization

Note

Recommendation for setting the time

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

Note

Consistent time-of-day synchronization via NTP / NTP (secure)

Up to firmware version V2.0 of the CP, both the CPU and CP can have the time of day synchronized using NTP. In this case, only have the time of day of the station from an external time source synchronized by a single module of the station so that a consistent time of day is maintained within the station.

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

- Forwarding of the CP time to the CPU using a PLC tag
- Forwarding of the CP time to the CPU via the backplane bus

Observe the section "Forwarding the time to the CPU" below.

Time-of-day synchronization of the CPs

The CPs support the following methods of time-of-day synchronization:

- CP 1542SP-1
  - NTP

  Configurable at the Ethernet interface
- CP 1543SP-1
  - NTP / NTP (secure)

    NTP servers can be configured manually in the table.

    NTP servers of the type NTP (secure) can be configured in the global security settings and can be selected for the CP in the "Security" parameter group in the table.
- CP 1542SP-1 IRC
  - NTP
  - From WAN
  - From local station (only under ST7)

  For details, refer to the configuration manuals Documentation references (Page 121).

Forwarding the time to the CPU

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

- **CP firmware ≤ V2.0**

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

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

  See section Communication with the CPU (Page 61) for more on this.

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

- **CP firmware ≥ V2.1**

  As of this firmware version of the CP, only one module in the station can be time master. This module distributes the time of day within the station.

If you want to have the time of the station synchronized via the CPU, disable the time-of-day synchronization for the CP.

Time-of-day synchronization with NTP

Configure the following parameters:

- The addresses of the NTP server(s)
- The "Accept time from non-synchronized NTP servers" option
- Synchronization cycle / Update interval

Time-of-day synchronization with enabled security functions

Note

Ensuring a valid time of day

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

Note

Manually setting the time of day during commissioning

If you use security functions or SINEMA RC, set the time manually during commissioning; see section Commissioning the CP (Page 48).

- **NTP / NTP (secure)**

  The secure method NTP (secure) uses authentication with symmetrical keys. Various configurable hash algorithms are available for the integrity check.

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

4.6 DNS configuration

DNS server

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

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

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

4.7 Communication with the CPU

Validity: CP 1542SP-1 / CP 1543SP-1

You will find the description of the CP 1542SP-1 IRC in the relevant configuration manual.

Watchdog bit

- **CP monitoring**

  The CP checks the connection with the CPU via the watchdog bit.

  The CP transfers the bit to the CPU every 5 seconds and resets it in the next CPU sampling cycle. The bit is not transferred in the event of connection faults. This signals the connection fault to the CPU.

  The PLC tag of the watchdog bit must be evaluated by the user program.

CP time

- **CP time to CPU**

  The function allows the CPU to read the time of day of the CP. Using this approach, the CP can synchronize the CPU time.

  Procedure:

  – The CPU sets the input "Time trigger variable" (BOOL) to 1 with the user program.

  – The CP then writes its time to the "CP time variable" (DTL) and resets the "Time trigger variable" value to 0.

  – The user program reads the "CP time variable" to set the CPU time.

  Recommendation:
  Set the "Time trigger variable" no more frequently than once per second to avoid placing an unnecessary communication load on the backplane bus.

Note

Refer to the information in the section Time-of-day synchronization (Page 58).

CP diagnostics

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

- **Enable advanced CP diagnostics**

  Enable the option to use advanced CP diagnostics.

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

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

- **Diagnostics trigger tag**

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

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

  Note

  Fast setting of the diagnostics trigger tag

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

Variable for CP 1542SP-1 and CP 1543SP-1:

- **Current IP address**

  PLC tag (data type String) for the current IP address of the interface of the CP.

Variables only for CP 1543SP-1:

- **VPN IPsec status**

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

  - 0 = No tunnel established
  - 1 = Tunnel established

- **Connection to SINEMA Remote Connect**

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

  - 0 = No tunnel established
  - 1 = Tunnel established

4.8 SNMP

"SNMP" parameter group

- "**Enable SNMP**" parameter group

  Releases the function of the SNMP agent on the CP.

Scope of performance of the CPs

The CPs support the following SNMP version:

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

  If the security functions are enabled, you will find the parameter group "SNMP" under "Security".

Traps are not supported by the CP.

You will find detailed information about the supported functions in the section Diagnostics with SNMP (Page 91).

4.9 Security (CP 1543SP-1)

Security functions of the CP 1542SP-1 IRC

You can find a description of the security functions of the CP 1542SP-1 IRC in the configuration manual of the respective telecontrol protocol, see Documentation references (Page 121).

Security functions of the CP 1543SP-1

The following description of the security functions only applies to the CP 1543SP-1.

For an overview of the functions, refer to the section Application and functions (Page 13).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 64).

4.9.1 Security user

Creating a security user

You need the relevant configuration rights to be able to configure security functions. For this purpose, you need to create at least one security user with the corresponding rights.

Navigate to the global security settings > "User and roles" > "Users" tab.

1. Create a user and configure the parameters.
2. Assign this user the role "NET Standard" or "NET Administrator" in the area below "Assigned roles".

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

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

4.9.2 Firewall

4.9.2.1 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.

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

Setting the firewall for online functions

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

Global security functions:

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

Local security functions of the CP:

Now select the CP in the S7 station.

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

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

Note

Additional services for online security diagnostics and download

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

4.9.2.3 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.

4.9.2.4 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.

4.9.3 Log settings - Filtering of the system events

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

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

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

4.9.4 E-mail configuration

Requirements and necessary information

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

- The security functions are enabled.
- The time of the CP is synchronized.

For the configuration, you require the data of the SMTP server and the user account:

- Server address, port number, user name, password, e-mail address of the sender (CP)
- With encrypted transfer: Server certificate

E-mail configuration

- **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 57).

See also

Character set for e-mail server and messages (CP 1543SP-1) (Page 80)

4.9.5 VPN

4.9.5.1 VPN (Virtual Private Network)

VPN - IPsec

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

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

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

Properties

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

Areas of application

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

Cell protection concept

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

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

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

- Data espionage
- Data manipulation
- Unwanted access

4.9.5.2 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect Server

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

- Exporting the CA certificate (optional)

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

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

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

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

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- CA Certificate

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

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

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

Authentication

- Device ID

  Enter the device ID generated for the module in SINEMA RC.
- Device password

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

  Max. number of characters: 127

Optional settings

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

- **Update interval**

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

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

- **"Connection type"**

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

  – Auto

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

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

  – PLC trigger

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

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

  Note

  Connection abort

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

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

- **PLC tag for connection establishment**

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

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

4.9.5.3 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 must be networked.

Note

Communication also possible via an IP router

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

Procedure

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

1. Creating a security user

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

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

Enable security functions

After logon, enable the "Activate security features" option on both CPs under "Security".

You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

1. In the global security settings, navigate to "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. Double-click on the "VPN groups" > "Assign module to a VPN group" entry.
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

To establish a VPN connection and for 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 by default when you create a VPN group. You cannot disable the option.

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

4.9.5.4 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.

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

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

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

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

4.9.5.6 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

4.9.6 SNMP

SNMP

You will find the range of functions of the device for SNMP in the section Diagnostics with SNMP (Page 91).

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

SNMP

- **"Enable SNMP"**

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

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

- **"Use SNMPv1"**

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

- **"Use SNMPv3"**

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

SNMPv1

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

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

- **"Reading community string"**

  The string is required for read access.

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

- **"Allow write access"**

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

- **"Writing community string"**

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

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

Note

Security of the access

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

SNMPv3

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

- **"Authentication algorithm"**

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

- **"Encryption algorithm"**

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

User management

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

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

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

4.9.7 Certificate manager

If the security functions are enabled, the certificates for all security modules involved are generated in the STEP 7 project, 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 "Certificate manager" entry in the local security settings. When assigning a CA certificate the module is also assigned the certificates derived from it.

Adding certificates

Via the local certificate manager, assign certificates of the partners 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 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

4.10 Messages: E-mails (CP 1542SP-1 IRC / CP 1543SP-1)

Validity

Validity: CP 1543SP-1

You will find the description of the CP 1542SP-1 IRC in the relevant configuration manual.

Note

E-mails via the message editor

The following information applies to e-mails configured with the message editor.

Sending e-mails via OUC program blocks is not affected.

Requirements

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

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

- The security functions are enabled.
- The time of the CP is synchronized.
- Configuring the "E-mail configuration" parameter group

You require the recipient addresses to configure the messages.

Open the message editor

You configure the individual messages (e-mails) in the message editor in STEP 7. Alternatively, you can open the editor:

- By selecting the CP

  Shortcut menu "Open the data point and messages editor"
- Via the project navigation:

  Station > "Local modules" > CP > Messages

  Double-clicking on the "Messages" entry opens the editor.

Creating messages

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

You can change the default name of an e-mail, "Alarm", but it must be unique within the module.

Message parameters

Here you configure the recipient, the subject and the text of the message.

Trigger: Triggering e-mail transfer

In the "Trigger" tab, you configure when sending of an e-mail is triggered and whether additional information is sent with it.

- **E-mail trigger**

  Specifies the event on which the sending of the e-mail is triggered:

  – Use PLC tag

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

    Resetting the trigger bit:
    If the memory area of the trigger bit is in the memory area or in a data block, the trigger bit is reset to zero when the message is sent.
    In all other cases, you need to reset the trigger bit with the user program.

    Note

    Fast setting of the diagnostics trigger tag

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

  – CPU changes to STOP

  – CPU changes to RUN

The following entries can be selected depending on the VPN configuration:

– VPN connection established

– VPN connection terminated

or

– SINEMA RC connection established

– SINEMA RC connection terminated

- **PLC tag for trigger**

  Variable (Bool) for the e-mail trigger "Use PLC tag"

- **Enable identifier for processing status**

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

  The status is written to the "PLC tag for processing status" (DWORD). If there are problems delivering messages, you can determine the status via the Web server of the CPU by displaying the value of the PLC tag there.

  For information on the significance of the individual statuses, see section Processing status of e-mails (CP 1543SP-1) (Page 94).

- **Include value**

  If you enable the option, the CP sends a value for the placeholder $$ from the memory area of the CPU in the message.

  Select a PLC tag whose value is integrated in the message. $$ can be the placeholder for a variable with a simple data type up to a size of 32 bits.

  The respective current value is entered in the message text instead of the placeholder $$. To do this enter "$$" as a placeholder for the value to be sent in the message text.

Editor view: Arranging columns and rows

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

- Arranging columns

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

- Sorting objects

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

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

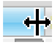
- Adapting the column width

  You can reach this function with the following actions:

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

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

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

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

- Showing/hiding columns

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

Copy messages

If you right-click in the row of an object in the table, you can access the following copy functions from the shortcut menu:

- Cut
- Copy
- Paste

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

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

- Delete

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

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

4.11 Character set for e-mail server and messages (CP 1543SP-1)

Character set for message texts

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

- 0x0A

  LF (line feed)
- 0x0D

  CR (carriage return)
- 0x20

  Space
- 0x21 ... 0x5A

  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0x5F

  £
- 0x61 ... 0x7A

  a b c d e f g h i j k l m n o p q r s t u v w x y z

Program blocks 5

5.1 Program blocks for OUC

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

Program block versions

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

Note

Personal data unencrypted in TMAIL_C

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

Program blocks

Together with the three CP types, the following OUC blocks with the specified minimum version are available to the CPU:

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

  Compact blocks for:

  – Connection establishment/termination and sending data

  – Connection establishment/termination and receiving data

As an alternative, use:

- **TCON V4.0 / TDISCON V2.1**

  Connection establishment / connection termination

- **TUSEND V4.0 / TURCV V4.0**

  Sending and receiving data via UDP

- **TSEND V4.0 / TRCV V4.0**

  Sending and receiving data via TCP or ISOonTCP

- **TMAIL_C V4.0**

  Sending e-mails

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

For changing configuration data of the CP during runtime:

- **T_CONFIG V1.0**

  Program-controlled configuration of the IP parameters

  See section Changing the IP parameters during runtime (Page 84) for more on this.

The program block can be found in STEP 7 in the "Instructions > Communication > Open User Communication" window.

Connection descriptions in system data types (SDTs)

For the connection description, the blocks listed above use the parameter CONNECT (or MAIL_ADDR_PARAM with TMAIL_C). The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

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

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

SDTs

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

- **SDTs for all three CP types**
  - **TCON_IP_V4**

    For transferring data via TCP or UDP
  - **TCON_QDN**

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

    For transferring data via ISO-on-TCP (direct communication between two S7 stations)
  - **TADDR_Param**

    For transferring data via UDP
  - **TMail_V4**

    For transferring e-mails addressing the e-mail server using an IPv4 address
  - **TMail_V6**

    For transferring e-mails addressing the e-mail server using an IPv6 address
  - **TMail_FQDN**

    For transferring e-mails addressing the e-mail server using its name (FQDN)

- **Additionally for CP 1542SP-1 IRC and CP 1543SP-1**
  - **TMail_V4_SEC**

    For secure transfer of e-mails addressing the e-mail server using an IPv4 address
  - **TMail_V6_SEC**

    For secure transfer of e-mails addressing the e-mail server using an IPv6 address
  - **TMail_QDN_SEC**

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

  Note on TMail_Vx_SEC / TMail_QDN_SEC:
  With these SDTs, the mail server certificate is checked, but not the ID of the "TLSServerCertRef" (STEP 7 internal reference) certificate.
- **Additionally for CP 1543SP-1**
  - **TCON_IP_V4_SEC**

    For the secure transfer of data via TCP
  - **TCON_QDN_SEC**

    For the secure transfer of data via the host name

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

Connection establishment and termination

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

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

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

Note

Connection abort

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

5.2 Changing the IP parameters during runtime

Changing the IP address during runtime

Note

Changing the IP parameters with a dynamic IP address

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

As of STEP 7 V14, you can change the following address parameters of the CP program-controlled during runtime with temporary validity using T_CONFIG:

- IP address
- Subnet mask
- Router address

Requirement in the CP configuration

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

Program blocks

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

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

The following program blocks and system data types can be used:

- **T_CONFIG**

  Together with the following SDTs:

  – IF_CONF_V4

  – IF_CONF_V6

  – IF_CONF_NTP

  – IF_CONF_DNS

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

You can find detailed information on the blocks and SDTs in the STEP 7 information system.

5.3 MODBUS blocks

MODBUS (TCP)

All three CP types support the program blocks for MODBUS (TCP):

- MB_CLIENT
- MB_SERVER

You can find detailed information in the STEP 7 information system.

Diagnostics and maintenance 6

CAUTION

Hot surfaces

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

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

WARNING

Cleaning the housing

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

Do not use any liquids or solvents.

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 35).

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

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

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

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

CP 1542SP-1 IRC / CP 1543SP-1: If you want to operate online diagnostics with the station via the CP, you need to activate the "Enable online functions" option under "Communication types" as a prerequisite.

"Diagnostics" group

The diagnostics pages are divided into the following groups:

- **General**

  This group displays general information on the module.

- **Diagnostics status**

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

  - Device-specific events

    Information on internal module events are displayed for modules with security or telecontrol functions.

- **Ethernet interface**

  Address and statistical information

- **Industrial Remote Communication**

  For the CP 1542SP-1 IRC, you receive telecontrol-specific information here. The group has the following diagnostics pages:

  - Partner

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

  - Data point list

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

  - Protocol diagnostics

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

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

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

- **Time of day**

  Information on the time on the device

- **Security**

  This group is available for modules with security functions.

  – Status

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

  – System log

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

  – Audit log

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

  – Communication status

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

  – SINEMA RC - automatic VPN configuration

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

"Functions" group

- **Firmware update**

  For a description, see section Downloading firmware (Page 96).

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

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

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

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 92).

SNMP

For information on the functions, refer to the section Diagnostics with SNMP (Page 91).

Diagnostics e-mail

Validity: CP 1542SP-1 IRC / CP 1543SP-1

The two CPs can send a diagnostics e-mail if configurable events occur, for example a partner cannot be reached or CPU STOP.

The configuration is described in section Messages: E-mails (CP 1542SP-1 IRC / CP 1543SP-1) (Page 76).

Telecontrol diagnostics

Validity: CP 1542SP-1 IRC

- Partner status

  The CP can signal the status of the connection to the communications partner to the CPU via a PLC tag.

  For information on the configuration, refer to the telecontrol configuration manuals /10/ (Page 123).

- CP diagnostics

  The CP can store extended diagnostic data in PLC tags.

  For information on the configuration, see section Communication with the CPU (Page 61).

You can display the states of the PLC tags via the Web server of the CPU or via a watch table, for example.

6.2 Online security diagnostics via port 8448 (CP 1542SP-1 IRC, CP 1543SP-1)

Security diagnostics via port 8448

Requirements:

- With an activated firewall, access must be enabled.

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

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

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

For more information, refer to section Settings for online security diagnostics and downloading to station with the firewall activated (Page 64).

6.3 Diagnostics with SNMP

Requirement

The requirement for using SNMP is the enabling of the function in the configuration, see section SNMP (Page 63).

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 stored in MIB files (MIB = Management Information Base).

You will find detailed information on SNMP and the Siemens Automation MIB in the manual /6/ (Page 122).

Scope of performance of the CPs

The CPs support the following SNMP version:

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

  For information on configuring SNMPv3, see section SNMP (Page 74).

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**

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**

Access rights using community names (SNMPv1)

As default setting, the CP 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!

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

6.4 Web server of the CPU

The Web server of the CPU

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

The Web server of the CPU provides a wide variety of functions for diagnostics and service purposes. You will find detailed information in the system manual /2/ (Page 122) 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 PC 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 PC.

These two variants are described in the following sections.

Connection establishment with HTTP

1. Connect the PC 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 operate the Web server.

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

Connection establishment with HTTPS

1. Connect the PC to the CP or the 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.

6.5 Processing status of e-mails (CP 1543SP-1)

Processing status of e-mails

The following status identifiers apply to e-mails configured with the message editor of the CP, see also section Messages: E-mails (CP 1542SP-1 IRC / CP 1543SP-1) (Page 76).

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

Processing status of e-mails of the message editor

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").
8502	Syntax error. Check the following configuration data: Alarm configuration > E-mail data (Content): • Email address (sender)

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

6.6 Downloading firmware

New firmware versions of the CP

If a new firmware version is available for the 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

  You will find the description below.

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

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 the firmware download 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.

6.7 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.

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

Technical specifications

7

7.1 Technical specifications of the CP 154xSP-1

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	For information on the properties of the BusAdapters and the permissible cable lengths, see /3/ (Page 122).	
Electrical data		
External power supply (X80), design	Socket	Two terminals with reverse polarity protection
	Terminal block for socket	2 x two terminal for single or redundant power supply
Power supply (external)	• Type of voltage	• 24 VDC
	• Permitted low limit	• 19.2 V
	• Permitted high limit	• 28.8 V
Current consumption	From backplane bus (3.3 V)	4 mA (typ.)
	From 24 V DC (external)	Plugged in BusAdapter:
	• With BusAdapter BA 2xRJ45	• BA 2xRJ45
	– typ.	– 115 mA
	– max.	– 140 mA
	• With BusAdapter BA 2xLC	• BA 2xLC
	– typ.	– 185 mA
	– max.	– 225 mA
	• With BusAdapter BA SCRJ	• BA SCRJ
	– typ.	– 150 mA
	– max.	– 240 mA
	• With BusAdapter BA 2xVD	• BA 2xVD
	– typ.	– 150 mA
	– max.	– 180 mA
Maximum Inrush current	(Rated value)	12 A
Effective power loss	(typical)	6 W
Overvoltage category according to IEC / EN 60664-1	Category I	

Technical specifications		
Permitted ambient conditions		
Ambient temperature *	During operation with the rack installed horizontally	-30 .. + 60 °C
	During operation with the rack installed vertically	-30 .. + 50 °C
	During storage	-40 .. +70 °C
	During transportation	-40 .. +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3	
Design, dimensions and weight		
Module format	Compact module ET 200SP	
Degree of protection	IP20	
Weight • Without bus adapter • With bus adapter 2xRJ45	 • 180 g • 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 • At + 60 °C	• 56.87 years • 24.78 years	
Product functions	You will find additional properties and performance data in the section Application and functions (Page 13).	

* Also read the information in the Ambient temperature (Page 100) section.

7.2 Ambient temperature

Restrictions of the maximum specified ambient temperature

The maximum permissible temperatures of the module for altitudes up to 2000 m can be found above in the technical specifications.

When using the module at higher altitudes, the decrease in the cooling effect due to convection as a result of the lower air pressure must be taken into account. According to IEC 61010-2-201 CD2 2015, the temperature at altitudes > 2000 m must be reduced.

The following derating factors and maximum ambient temperatures apply.

Table 7- 1 Restrictions of the maximum permissible ambient temperature in relation to the installation altitude

Installation altitude **(Height above mean sea level)**	**Derating factor** [1]	**Maximum ambient temperature when the rack is mounted horizontally**
-1000 m to 2000 m	1.00	60 °C
2000 m to 3000 m	0.93	56 °C
3000 m to 4000 m	0.86	52 °C
4000 m to 5000 m	0.78	47 °C

[1] Basic value for applying the derating factor is the maximum permissible ambient temperature in °C for 2000 m.

Note

- The derating factors compensate for the decreasing cooling effect of air at higher altitudes due to lower density.
- Linear interpolation between altitudes is permissible.

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.

Documents on the Internet

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

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

Address for declarations of conformity

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

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

EC declaration of conformity

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

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

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

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

  EMC directive of the European Parliament and of the Council of 26 February 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, p. 79-106

- **2011/65/EU (RoHS)**

  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, official journal of the EC L174, 01/07/2011, page 88-110

UK Declaration of Conformity

Importer UK:

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

The product meets the requirements of the following directives:

- UKEX Regulations

  SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.

- EMC Regulations

  SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.

- RoHS Regulations

  SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX / IECEx / UKEX / CCC-Ex

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

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

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 40).

The product meets the explosion protection requirements outlined below.

IECEx

Classification: Ex ec IIC T4 Gc, Certificate no.: IECEx DEK 18.0017X

The product meets the requirements of the standards:

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

ATEX

Classification: II 3 G Ex ec IIC T4 Gc, Certificate no.:DEKRA 18ATEX0027 X

The product meets the requirements of the standards:

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

UKEX

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

The product meets the requirements of the standards:

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

Importer UK: Siemens plc (see above)

CCC-Ex

Classification:Ex ec IIC T4 Gc

The product meets the requirements of the following standards:

- GB 3836.1

  Hazardous areas - Part 0: Equipment - General requirements
- GB 3836.3

  Explosive atmospheres - Part 3: Equipment protection by increased safety 'e'

EMC

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

Applied standards:

- EN 61000-6-4

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

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

RoHS

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

Applied standard:

- EN IEC 63000

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)

Observe the conditions for safe usage of the CP according to the section Notes on use in hazardous areas according to UL HazLoc and FM (Page 40).

FM

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

Equipment rating:
Class I, Division 2, Group A, B, C, D, Temperature Class T4, Ta = 60 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

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

Report Number: 3059889

Observe the conditions for safe usage of the CP according to the section Notes on use in hazardous areas according to UL HazLoc and FM (Page 40).

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

Dimension drawings

B

All dimensions in the dimension drawings are in millimeters.

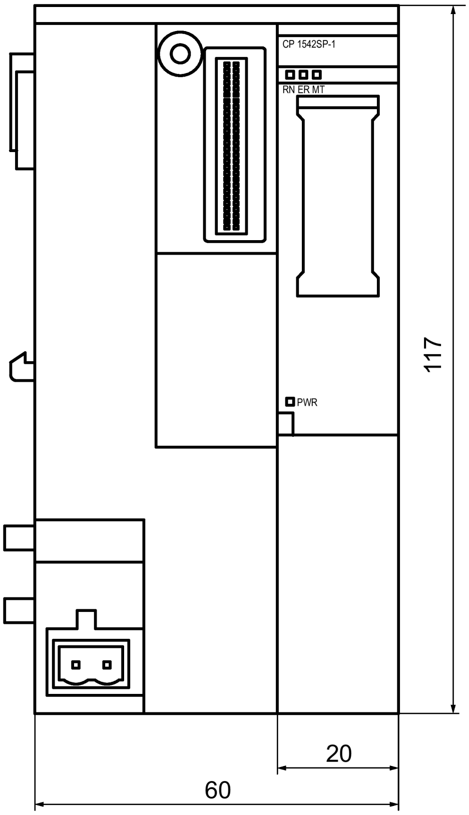


Figure B-1 Front view of the CP

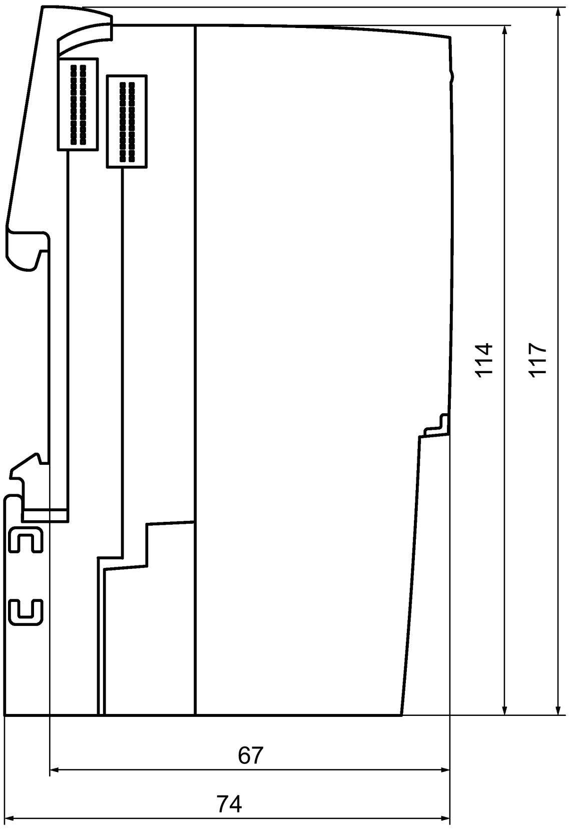


Figure B-2 Side view (left) of the CP

Accessories C

C.1 BusAdapter

Compatible BusAdapter

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

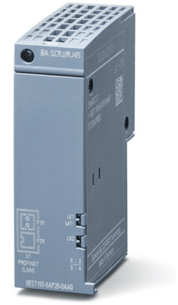


Figure C-1 Example of a bus adapter, here BA SCRJ/RJ45

The CP supports the following bus adapters:

SIMATIC ET 200SP

- SIMATIC BA 2×RJ45

  PROFINET BusAdapter with the following connectors:

  – 2 x Ethernet jack RJ45

  Article number: 6ES7193-6AR00-0AA0
- SIMATIC BA 2xFC

  PROFINET BusAdapter with the following connectors:

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

  Article number: 6ES7193-6AF00-0AA0
- SIMATIC BA 2xSCRJ

  PROFINET BusAdapter with the following connectors:

  – 2 x fiber-optic cable POF/PCF

  Article number: 6ES7193-6AP00-0AA0
- SIMATIC 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 RJ45

  Article number: 6ES7193-6AP20-0AA0

- SIMATIC 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

SIMATIC ET 200SP HA

- SIMATIC BA 2xLC

  SIMATIC BusAdapter with the following connectors:

  – 2 x glass fiber-optic cables LC

  Article number: 6ES7193-6AG00-0AA0

- SIMATIC BA LC/RJ45

  SIMATIC BusAdapter with the following connectors:

  – 1 x glass fiber-optic cables LC FO

  – 1 x Ethernet jack RJ45

  Article number: 6ES7193-6AG20-0AA0

- SIMATIC BA LC/FC

  SIMATIC BusAdapter with the following connectors:

  – 1 x glass fiber-optic cables LC FO

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

  Article number: 6ES7193-6AG40-0AA0

- SIMATIC BA 2xRJ45VD HA

  SIMATIC BusAdapter VD (Variable Distance) for Ethernet communication and PROFINET, extended temperature range, conformal coating, with the following connectors:

  – 2 x Ethernet jack RJ45

  Article number: 6GK5991-2VA00-8AA2

You can find additional details in the manual /2/ (Page 122) and on the following Siemens web pages.

Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/14072)

Siemens Industry Mall at:
Link:
https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10147556?tree=CatalogTree
Link:
https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10412114?tree=CatalogTree

SIPLUS BusAdapter

SIMATIC ET 200SP

- SIMATIC BA 2xFC

  PROFINET BusAdapter with the following connectors:

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

  Article number: 6DL1193-6AF00-0AA0

- SIMATIC BA 2xLC

  SIMATIC BusAdapter with the following connectors:

  – 2 x glass fiber-optic cables LC

  Article number: 6DL1193-6AG00-0AA0

- SIMATIC BA 2×RJ45

  PROFINET BusAdapter with the following connectors:

  – 2 x Ethernet jack RJ45

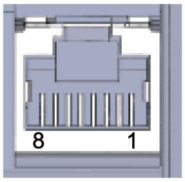
  Article number: 6DL1193-6AR00-0AA0

See also Siemens Industry Mall at:
Link:
https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10290278?tree=CatalogTree

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

C.2 IP-based routers

Routers for IP-based communication

To connect a communications module to IP-based infrastructure networks, various routers are available from Siemens.

Information on the devices can be found on the following Siemens Internet pages.

Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15982)

Siemens Industry Mall at:
Link:
https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10215915?tree=CatalogTree

Encryption methods (Ciphers) D

The following tables list the encryption methods (ciphers) used by the CP.

The tables are valid for all three CP variants in the firmware version specified in the preface.

Meaning of the table columns

- **Category**
  - Cipher: Cipher suite (encryption methods)
  - DSA: Signature algorithm
  - SEA: Signature and encryption algorithm
- **Name**

  Name of the category according to IANA

  You can find an overview of the TLS parameters and Cipher Suites on the following page: Link: (https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4)
- **Value**

  Value (hexadecimal) of the suite according to IANA
- **TLS**

  TLS version with which the respective category is used.
- **FW**

  Configured firmware version of the CP
- **Security**
  - ✓

    Ciphers considered secure
  - Legacy

    Ciphers no longer considered secure
- **Protocol**

  Communication protocols that use the respective category.
  - All

    All communication services and protocols including telecontrol communication (DNP3 / IEC 60870-5) and OUC
  - No TC

    All communication services and protocols except telecontrol communication
  - OUC

    Open User Communication (OUC) only

TLS versions used by the CP

TLS version	Firmware	Security
TLS Version 1.0	≤ V2.1	Legacy
TLS Version 1.1	≤ V2.1	Legacy
TLS Version 1.2	≤ V2.2	✓
TLS Version 1.3	≤ V2.2	✓

Ciphers used by the CP

Category	Name	Value	TLS	FW	Security	Protocol
Cipher	TLS_AES_128_GCM_SHA256	0x13,0x01	TLS 1.3	≤ V2.2	✓	All
Cipher	TLS_AES_256_GCM_SHA384	0x13,0x02	TLS 1.3	≤ V2.2	✓	All
Cipher	TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS 1.3	≤ V2.2	✓	No TC
Cipher	TLS_AES_128_CCM_SHA256	0x13,0x04	TLS 1.3	≤ V2.2	✓	No TC
Cipher	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00,0xA2	≤ TLS 1.2	≤ V2.2	✓	No TC
Cipher	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00,0xA3	≤ TLS 1.2	≤ V2.2	✓	No TC
Cipher	TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x9E	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9E	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_DHE_RSA_WITH_AES_256_CCM	0xC0,0x9F	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9F	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAA	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0,0xAC	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0,0x2B	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0,0xAD	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC0,0x2C	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA9	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC0,0x2F	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x30	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA8	≤ TLS 1.2	≤ V2.2	✓	All
Cipher	TLS_RSA_WITH_AES_128_CCM	0xC0,0x9C	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_128_CCM_8	0xC0,0xA0	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9C	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_128_CBC_SHA	0x00, 0x2F	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_128_CBC_SHA256	0x00, 0x3C	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_256_CCM	0xC0, 0x9D	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_256_CCM_8	0xC0, 0xA1	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9D	≤ TLS 1.2	≤ V2.1	Legacy	All

Category	Name	Value	TLS	FW	Security	Protocol
Cipher	TLS_RSA_WITH_AES_256_CBC_SHA	0x00, 0x35	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_AES_256_CBC_SHA256	0x00, 0x3D	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_ARIA_128_GCM_SHA256	0xC0, 0x50	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x51	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_128_CBC_SHA	0x00,0x90	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	0x00,0xB2	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_128_CCM	0xC0,0xA6	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_DHE_WITH_AES_128_CCM_8	0xC0, 0xAA	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	0x00,0xAA	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_256_CBC_SHA	0x00,0x91	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	0x00,0xB3	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_256_CCM	0xC0,0xA7	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_DHE_WITH_AES_256_CCM_8	0xC0, 0xAB	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	0x00,0xAB	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256	0xC0,0x6C	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384	0xC0,0x6D	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAD	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_AES_128_CCM_8	0xC0,0xA2	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x00,0x33	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x00,0x67	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_AES_256_CCM_8	0xC0,0xA3	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x00,0x39	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x00,0x6B	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256	0xC0,0x52	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384	0xC0,0x53	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	0xC0,0x60	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	0xC0, 0x61	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	0xC0,0xAE	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xC0,0x09	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xC0,0x23	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	0xC0,0xAF	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0xC0,0x0A	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xC0,0x24	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256	0xC0,0x5C	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	0xC0,0x5D	≤ TLS 1.2	≤ V2.1	Legacy	All

Category	Name	Value	TLS	FW	Security	Protocol
Cipher	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA	0xC0,0x35	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	0xC0,0x37	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA	0xC0,0x36	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	0xC0,0x38	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAC	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0xC0,0x13	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0xC0, 0x27	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xC0,0x14	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0xC0, 0x28	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_128_CBC_SHA	0x00,0x8C	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_128_CBC_SHA256	0x00,0xAE	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_128_CCM	0xC0,0xA4	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_128_CCM_8	0xC0,0xA8	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_128_GCM_SHA256	0x00,0xA8	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_256_CBC_SHA	0x00,0x8D	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_256_CBC_SHA384	0x00,0xAF	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_256_CCM	0xC0,0xA5	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_256_CCM_8	0xC0,0xA9	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_AES_256_GCM_SHA384	0x00,0xA9	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_ARIA_128_GCM_SHA256	0xC0,0x6A	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_ARIA_256_GCM_SHA384	0xC0,0x6B	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_PSK_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAB	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_AES_128_CBC_SHA	0x00,0x94	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256	0x00,0xB6	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	0x00,0xAC	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_AES_256_CBC_SHA	0x00,0x95	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384	0x00,0xB7	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	0x00,0xAD	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256	0xC0,0x6E	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384	0xC0,0x6F	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAE	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_SRP_SHA_WITH_AES_128_CBC_SHA	0xC0,0x1D	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_SRP_SHA_WITH_AES_256_CBC_SHA	0xC0,0x20	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA	0xC0,0x1E	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA	0xC0,0x21	≤ TLS 1.2	≤ V2.1	Legacy	All
Cipher	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	0x00,0x32	≤ TLS 1.2	≤ V2.1	Legacy	OUC

Category	Name	Value	TLS	FW	Security	Protocol
Cipher	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x00,0x40	≤ TLS 1.2	≤ V2.1	Legacy	OUC
Cipher	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	0x00,0x38	≤ TLS 1.2	≤ V2.1	Legacy	OUC
Cipher	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x00,0x6A	≤ TLS 1.2	≤ V2.1	Legacy	OUC
Cipher	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256	0xC0,0x56	≤ TLS 1.2	≤ V2.1	Legacy	OUC
Cipher	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384	0xC0,0x57	≤ TLS 1.2	≤ V2.1	Legacy	OUC
Cipher	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA	0xC0,0x1F	≤ TLS 1.2	≤ V2.1	Legacy	OUC
Cipher	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA	0xC0,0x22	≤ TLS 1.2	≤ V2.1	Legacy	OUC
SEA	DSA_SHA256	0x0402		≤ V2.2	✓	No TC
SEA	DSA_SHA384	0x0502		≤ V2.2	✓	No TC
SEA	DSA_SHA512	0x0602		≤ V2.2	✓	No TC
SEA	ecdsa_secp256r1_sha256	0x0403		≤ V2.2	✓	All
SEA	ecdsa_secp384r1_sha384	0x0503		≤ V2.2	✓	All
SEA	ecdsa_secp521r1_sha512	0x0603		≤ V2.2	✓	All
SEA	ed25519	0x0807		≤ V2.2	✓	All
SEA	ed448	0x0808		≤ V2.2	✓	All
SEA	rsa_pss_pss_sha256	0x0804		≤ V2.2	✓	All
SEA	rsa_pss_pss_sha384	0x0805		≤ V2.2	✓	All
SEA	rsa_pss_pss_sha512	0x0806		≤ V2.2	✓	All
SEA	rsa_pss_rsae_sha256	0x0809		≤ V2.2	✓	All
SEA	rsa_pss_rsae_sha384	0x080A		≤ V2.2	✓	All
SEA	rsa_pss_rsae_sha512	0x080B		≤ V2.2	✓	All
SEA	rsa_pkcs1_sha256	0x0401		≤ V2.2	✓	No TC
SEA	rsa_pkcs1_sha384	0x0501		≤ V2.2	✓	No TC
SEA	rsa_pkcs1_sha512	0x0601		≤ V2.2	✓	No TC
DSA	DSA_SHA1	0x0202		≤ V2.1	Legacy	All
DSA	DSA_SHA224	0x0302		≤ V2.1	Legacy	All
SEA	ecdsa_sha1	0x0203		≤ V2.1	Legacy	All
SEA	ecdsa_sha224	0x0303		≤ V2.1	Legacy	All
SEA	rsa_pkcs1_sha1	0x0201		≤ V2.1	Legacy	All
SEA	rsa_pkcs1_sha224	0x0301		≤ V2.1	Legacy	All

Documentation references E

Structure of the documentation

Note the structure of the documentation for the devices, see Preface (Page 3).

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
ET 200SP
Manual Collection
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/84133942)

/4/

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

- Volume 1: Industrial Ethernet

  Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465)
- Volume 2: Passive network components

  Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

/8/

SIMATIC NET
SINEMA Remote Connect - Server
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/21816/man)

/9/

SIMATIC NET
SINAUT ST7
System Manual
- Volume 1: System and hardware
- Volume 2: Configuration in STEP 7 V5
- Volume 3: Configuration in STEP 7 Professional
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/21771/man)

/10/

SIMATIC NET - TeleControl
Siemens AG
Configuration manuals of the protocols:
- TeleControl Basic
- SINAUT ST7
- DNP3
- IEC 60870-5
Link: (https://support.industry.siemens.com/cs/ww/en/ps/22143/man)

/10/

Index