SIEMENS

SIMATIC NET

TeleControl
Configuration - TeleControl Basic

Configuration Manual

Configuration and diagnostics

12/2019

C79000-G8976-C577-01

Legal information

Warning notice system

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C577-01
℗ 01/2020 Subject to change

Preface

Validity of this manual

This configuration manual is valid for SIMATIC NET communications modules that support the "TeleControl Basic" protocol:

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

For information on the device versions and the associated configuration software, refer to the section Validity: Communications modules (Page 11).

Structure of the documentation

The documentation of the SIMATIC NET telecontrol CPs consists of the following manuals in each case:

- Operating instructions
- Configuration manuals

  (1 configuration manual for each telecontrol protocol)

  Only the configuration manual Telecontrol Basic is listed below.

You can find the Internet links for the manuals in the Bibliography (Page 173).

The documents have the following content:

- **Operating instructions**

  Valid for the respective CP

  – Application and functions
  – Requirements (CPUs, configuration software, etc.)
  – Hardware description
  – Installation, wiring, commissioning, operation
  – Configuration

    The section "Configuration" only describes the configuration of the telecontrol-independent functions.

    If you use telecontrol functions, read the respective configuration manual.
  – Diagnostics, maintenance
  – Technical specifications, approvals, accessories

- **Configuration manual TeleControl Basic**

  Configuration and diagnostics in STEP 7 Professional (TIA Portal)

Abbreviations/device names

The following designations and abbreviations are frequently used in this manual. They mean:

- **Module / device / CP**

  When properties listed in this manual are valid for all types of CP, these names are used for 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.

- **Mobile wireless CP**

  CPs with mobile wireless interface:

  – CP 1242-7 GPRS V2
  – CP 1243-7 LTE

- **Ethernet CP**

  CPs with Ethernet interface:

  – CP 1243-1
  – CP 1542SP-1 IRC

- **Security CP**

  CPs with security functions:

  – CP 1243-1

  – CP 1243-7 LTE

  – CP 1542SP-1 IRC

- **TCSB**

  Control center software "TeleControl Server Basic" that is installed on the telecontrol server (PC).

New in this edition

First issue

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:

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

Required experience

Knowledge in the following areas is required for configuration and diagnostics of the devices:

- Data transfer via WAN networks
- SIMATIC STEP 7 Professional
- Setting up industrial networks with security functions

Cross references

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

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

License conditions

Note

Open source software

The products contain open source software. Read the license conditions for open source software carefully before using the products.

The operating instructions of the relevant product provide information on finding the license conditions.

Security information

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

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

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

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

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

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

SIMATIC NET glossary

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

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

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

Table of contents

Functions and requirements

1

1.1 Validity: Communications modules

Communication module for the TeleControl Basic protocol

The following SIMATIC NET communication modules can be used for the telecontrol protocol TeleControl Basic.

Meaning of the symbols in the table:

- X = Supported
- - = Not supported

Table 1- 1 Communication module for the TeleControl Basic protocol

Module Article number	Interface type		STEP 7 product *	Firmware **
	Ethernet	Mobile wireless		
CP 1242-7 GPRS V2 6GK7242-7KX31-0XE0 6AG1242-7KX31-7XE0	-	X	STEP 7 Basic / Professional	V3.2
CP 1243-7 LTE 6GK7243-7KX30-0XE0 6GK7243-7SX30-0XE0	-	X	STEP 7 Basic / Professional	V3.2
CP 1243-1 6GK7243-1BX30-0XE0 6AG1243-1BX30-2AX0	X	-	STEP 7 Basic / Professional	V3.2
CP 1542SP-1 IRC 6GK7 542-6VX00-0XE0	X	-	STEP 7 Professional	V2.1

***** / ****** Note the following information on the STEP 7 product and firmware version.

- **STEP 7 product**

  You will find the required STEP 7 version for configuring the full range of functions described in the manual in the section Software requirements (Page 28).

- **Firmware**

  The firmware version specified in the table enables the use of the full range of functions described in this manual.

  Modules with lower firmware versions can be configured in older STEP 7 versions with a deviating scope of functions.

1.2 Communication services and mechanisms

1.2.1 Communications services

The CPs are intended for use in an industrial environment. The following applications are supported:

Telecontrol communication

The following applications are possible depending on the type of CP.

- Communication with the control center

  S7 stations communicate via Ethernet, via the mobile wireless network and the Internet with the telecontrol server in the master station. The telecontrol server communicates with a higher-level control system using the integrated OPC server function.

- Inter-station communication between S7 stations via the telecontrol server

  In this application, the CP establishes a connection to the telecontrol server. The telecontrol server forwards the messages to the destination station.

For this communications service, the CP and TCSB use their own protocol on OSI layer 7 that among other things supports certain security functions, see section Security functions (Page 17).

Event-driven sending of messages

Event-driven sending of messages

- Ethernet CPs
- The CPs are sending e-mails to PCs with an Internet connection via Ethernet.
- Mobile wireless CPs

  Via the mobile wireless network, the CPs send SMS messages to mobile phones or e-mails to PCs with an Internet connection.

Both types of messages are configured in the message editor in STEP 7. The use of program blocks is not necessary.

Communication via SINEMA Remote Connect

See section SINEMA Remote Connect (Page 167).

Direct communication via Open User Communication (OUC)

The program blocks of Open User Communication provide the CP with the following communication options:

- Direct communication between S7-1200 stations

  For this, the CP must be assigned a fixed IP address, see section Ethernet interface (Page 51).

- E-mail / SMS

  In contrast to the telecontrol communication, program blocks must be used to transfer SMS messages/e-mails via OUC, see section OUC program blocks (Page 157).

S7 communication

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

The CP supports the following functions:

- PUT / GET

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

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

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

1.2.2 Address and authentication data

IP address of the CP

Because the CPs generally establish the connection with TCSB, a dynamic IP address can be assigned to a mobile wireless CP by the Internet service provider.

Exceptions
The CP requires a fixed IP address in the following cases:

- The CP uses S7 communication
- The CP receives data via Open User Communication

Address and authentication data for communication with TCSB

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

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

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

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

  See section CP identification (Page 70) for more on this.

1.2.3 Acknowledgment

Acknowledgment of frames

The receipt of a frame is monitored and acknowledged in different ways. The mechanisms differ depending on the type of communication:

- **Telecontrol communication**

  Frames received from TCSB are acknowledged immediately by the CP.

  Frames sent by the CP are acknowledged by TCSB.
- **Inter-station communication**

  Received frames are acknowledged immediately by the CP. The acknowledgment frame is forwarded by the telecontrol server to the destination CP.

  For sent frames, this applies in the opposite direction.
- **Direct communication (Open User Communication)**

  The successful sending and receipt of frames is indicated by status displays of the program blocks.

  With TCP segments, the protocol-specific acknowledgement mechanisms are used.

1.2.4 Inter-station communication

Inter-station communication

When using the TeleControl Basic protocol, two stations exchange data via inter-station communication. Inter-station communication between two stations is always via the telecontrol server that serves as an intermediary.

Compatible modules

For inter-station communication, three groups of station types are available. Inter-station communication is possible only between station types of the same group. Only group 2 is relevant here.

- Group 1
  - S7-1200 / CP 1242-7
- Group 2
  - S7-1200 / CP 1242-7 GPRS V2
  - S7-1200 / CP 1243-1
  - S7-1200 / CP 1243-7 LTE
  - ET 200SP / CP 1542SP-1 IRC
- Group 3
  - S7-200 / MD720
  - S7-300 / MD720

Inter-station communication between station types in different groups is not possible.

1.3 Other services and properties

Other services and properties

- **Data point configuration**

  Due to the data point configuration in STEP 7, you do not need to create program blocks to transfer the process data. The individual data points are processed one-to-one in the control system.

- **IP configuration**

  The CP is assigned a dynamic or a fixed IP address by the mobile wireless network provider:

  – Dynamic IP address

    When using telecontrol communication, the mobile wireless network provider generally assigns the CP a dynamic IP address. You set this in STEP 7 in the parameter group "Ethernet interface > Ethernet addresses".

  – Fixed IP address

    To use S7 communication or to receive data via Open User Communication, the CPU must be reachable via a fixed IP address. In this case, enter the fixed IP address assigned by the mobile wireless network provider in the same parameter group.

- **Time-of-day synchronization**

  The CP supports various methods of time-of-day synchronization. You will find information in the section Time-of-day synchronization (Page 56).

  For information on the format of the time stamp, refer to the section Datapoint types (Page 94).

- **Access to the Web server of the CPU**

  With the aid of the Web server of the CPU, you can read out module data from the station.

- **Send buffer**

  The CP saves the values of data points configured as an event in the send buffer.

  The data is not saved retentively. It is lost in case of a power outage.

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

  The telecontrol communication with TCSB is triggered in two ways:

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

  – Triggered by various selectable criteria

  Logging status data and its transfer to the telecontrol server

  For example:

  – Data volumes transferred

  – ID of the wireless cell in the area of the station

  – GSM signal strength

  – Communication status

    etc.

- **Analog value processing**

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

- **Diagnostics SMS message**

  At the request of a mobile phone, a mobile wireless CP can send an SMS message with diagnostics data to this mobile phone, see Diagnostics options (Page 119).

1.4 Security functions

Note

Recommendation for critical security plants

Refer to the information in the section Security recommendations (Page 41).

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

Security functions

The following security functions are available:

- Configurable security functions

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

- Security functions of the program blocks

  For information on the security functions of the Open User Communication program blocks, see OUC program blocks (Page 157).

Configurable security functions

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

- Data espionage
- Data manipulation
- Unauthorized access

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

As a result of using the CP as a security module, the following security functions are accessible to the station:

General 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

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

- **NTP (secure)**

  For secure transfer during time-of-day synchronization

- **SINEMA Remote Connect**

  (only CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

  For information on communication via SINEMA Remote Connect, see SINEMA Remote Connect (Page 167).

- **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.

Security functions of the Ethernet CPs

- **Firewall**

  (only CP 1243-1)

  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")

- **VPN**

  The following alternatives can be used:

  – Telecontrol communication via SINEMA Remote Connect

  – 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).

  – Secured communication via IPsec tunnels

    (only CP 1243-1)

    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.

- **Logging**

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

- **SNMPv3**

  For secure transmission of network analysis information safe from eavesdropping

1.5 TeleService (Mobile wireless CPs)

TeleService via the mobile wireless network

A TeleService connection can be established between an engineering station (PC with STEP 7) and the mobile wireless CP of a remote S7-1200 station via the mobile wireless network and the Internet.

You can use the TeleService connection for the following purposes:

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

You will find application examples of the structure in the section Configuration examples (Page 30).

For configuration and execution see TeleService (Mobile wireless CPs) (Page 147).

1.6 Performance data and configuration limits

1.6.1 CP 1242-7 GPRS V2

Number of connections for the telecontrol communication

- 1 reserved connection for user data exchange with the telecontrol server
- Additional Inter-station communication

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

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

  - Receive from partners: Max. 15

  - Send to partner: Max. 3 ("Send buffer" parameter enabled)

Number of simultaneous TeleService connections

- Max. 1 TeleService connection

Number of simultaneous connections for S7 communication and Open User Communication

A maximum total of 22 connection resources for S7 communication and Open User Communication (OUC)

The maximum number can be divided up as follows:

- S7 connections: Maximum 8
- OUC connections: Maximum 8
  - TCP connections
  - ISO-on-TCP connections
  - UDP connections
- Additional free resources for S7 or OUC connections: Maximum 6

Number of connections to NTP servers

- Max. 1 connection to an NTP server
- 4 servers configurable

User data

With the connection types listed below, the user data of a frame represent a consistent data area in terms of the time of transfer.

User data per frame with the various connection types:

- For TCP connections: Max. 8192 bytes
- For ISO-on-TCP connections: Max. 1452 bytes
- For UDP connections: Max. 1472 bytes

With frames of telecontrol communication, the individual values of the data points are time stamped.

Number of data points for the data point configuration

The maximum number of configurable data points is 200.

Frame memory (send buffer)

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

The send buffer has a maximum size of 64 000 event messages divided into equal parts for all configured communications partners. The size of the frame memory can be set in STEP 7 ("Communication with the CPU" parameter group).

Messages: E-mail / SMS

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

Maximum number of characters that can be transferred per SMS message: 160 ASCII characters including any value sent at the same time

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

1.6.2 CP 1243-7 LTE

Number of simultaneous connections for telecontrol communication

- 1 reserved connection for user data exchange with the telecontrol server
- Additional Inter-station communication

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

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

  - Send to partner: Max. 3 ("Send buffer" parameter enabled)

  - Receiving from partners: Max. 15 ("Send buffer" parameter disabled)

Number of simultaneous TeleService connections

- Max. 1 TeleService connection

Number of simultaneous connections for S7 communication and Open User Communication

A maximum total of 22 connection resources for S7 communication and Open User Communication (OUC)Open User Communication (OUC)

The maximum number can be divided up as follows into:

- S7 connections: Maximum 8
- OUC connections Maximum 8
  - TCP connections
  - ISO-on-TCP connections
  - UDP connections
- Additional free resources for S7 or OUC connections: Maximum 6

Number of connections to NTP servers

- Max. 1 connection to an NTP server

User data

With the connection types listed below, the user data of a frame represent a consistent data area in terms of the time of transfer.

User data per frame with the various connection types:

- For TCP connections: Max. 8192 bytes
- For ISO-on-TCP connections: Max. 1452 bytes
- For UDP connections: Max. 1472 bytes

With frames of telecontrol communication, the individual values of the data points are time stamped.

Number of data points for the data point configuration

The maximum number of configurable data points is 200.

Frame memory (send buffer)

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

The send buffer has a maximum size of 64 000 events divided into equal parts for all configured communications partners. The size of the frame memory can be set in STEP 7 ("Communication with the CPU" parameter group).

Messages: E-mail / SMS

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

Maximum number of characters that can be transferred per SMS message: 160 ASCII characters including any value sent at the same time

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

IPsec tunnel (VPN)

An IPsec tunnel can be established for secure communication with another Security module.

Firewall rules

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

The firewall rules are divided up as follows:

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

1.6.3 CP 1243-1

Number of CMs/CPs per station

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

Connection resources

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

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

  – S7: Max. 14 (including connections for S7 routing)

  – TCP/IP: Max. 14

  – ISO-on-TCP: Max. 14

  – UDP: Max. 14

Also:

- **Telecontrol connections**

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

  TeleControl Basic

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

  – Additional Inter-station communication

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

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

    - Send to partner: Max. 3 ("Send buffer" parameter enabled)

    - Receiving from partners: Max. 15 ("Send buffer" parameter disabled)

  DNP3 / IEC 60870-5

  – Communication with up to 4 partners

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

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

- **Online connections**

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

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

  In total maximum of 4, of which:

  – Resources for programming device connections: Max. 1

  – Resources for HMI connections: Max. 3

Number of data points for the data point configuration

Maximum number of configurable data points

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

User data

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

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

Frame memory (send buffer)

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

The send buffer has a maximum size of 64000 events divided into equal parts for all configured communications partners. The size of the frame memory can be set in STEP 7 ("Communication with the CPU" parameter group).

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

Messages (e-mail)

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

IPsec tunnel (VPN)

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

Firewall rules

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

The firewall rules are divided up as follows:

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

1.6.4 CP 1542SP-1 IRC

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 the manual.

Connection resources

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

  Total number of connections on Industrial Ethernet: Maximum 32
  of which:

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

  – TCP/IP: Max. 32

  – ISO-on-TCP: Max. 32

  – UDP: Max. 32

Also:

- **Telecontrol connections**

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

  TeleControl Basic

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

  – Additional Inter-station communication

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

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

    - Send to partner: Max. 3 ("Send buffer" parameter enabled)

    - Receive from partners: Max. 15 ("Send buffer" parameter disabled)

DNP3 / IEC 60870-5

– The CP can establish connections to up to 4 communications partners.

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

  Communication between stations is configured via the telecontrol connections.

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

- **Online connections**

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

- **HTTP**

  TCP connections for HTTP access: Max. 12

  HTTP connections can be used by Web browsers to display data of the CPU Web server.

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

  In total maximum of 16, of which:

  – Resources for programming device connections: Max. 16
  – Resources for HMI connections: Max. 16

Messages (e-mail)

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

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

- Sending e-mails via the TMAIL_C program block

Frame memory (send buffer)

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

The send buffer is divided equally among all configured communications partners. The size of the frame memory can be set in STEP 7 ("Communication with the CPU" parameter group).

The maximum size of the send buffer is:

- TeleControl Basic: 64000 frames
- ST7: 32000 frames
- DNP3 / IEC: 100000 events

Number of data points for the data point configuration

Maximum number of configurable data points per CP:

- ST7 / DNP3 / IEC: 1500
- TeleControl Basic: 500

1.7 Software requirements

Software for configuration and online functions

The following version of STEP 7 is required for configuring the full range of functions described in this manual:

- STEP 7 Basic / Professional V16

For the required STEP 7 product, see section Validity: Communications modules (Page 11).

Requirements for using mobile wireless services

- Local availability of a mobile wireless network in the range of the station.
- A contract with a suitable mobile wireless network provider

  The contract must allow the transfer of data.

  IP address:

  – For communication with the telecontrol server, a private (fixed) or public (dynamic) IP address assigned by the mobile wireless network provider can be used.

  – For direct communication between S7 stations (S7 communication and Open User Communication via T blocks) the mobile wireless network provider must assign a fixed IP address to the CP and forward the frames to the destination nodes.
- The SIM card and PIN belonging to the mobile wireless contract

  The SIM card is inserted in the CP.

  With mobile wireless contracts in which the network provider does not assign a PIN, no PIN is necessary for the configuration of the CP.
- Access point (Access Point)

  For the transition between the mobile wireless network and Internet you require an access point. The name of the access point (APN) and the access data are configured for the CP in STEP 7, see section Mobile wireless communications settings (Page 49).

  Generally the mobile wireless network providers make an access point available.

Requirements for TeleService

TeleService functions are supported by mobile wireless CPs for diagnostics and maintenance functions.

For TeleService a switching station is required between the CP and the engineering station. This is either the telecontrol server or a TeleService gateway:

- **TeleService with telecontrol server**

  In this case, the telecontrol server is the switching station.

  For the documentation of the "TCSB" application, see /2/ (Page 174).

- **TeleService without telecontrol server**

  In this case, a PC with Internet connection is required, the TeleService gateway.

  Install the "TS Gateway" software on the TeleService gateway PC. You will find the software on the DVD supplied with the CP.

In both cases, telecontrol communication needs to be enabled in the CP.

1.8 Usable CPUs

Compatible CPUs

To use the full range of functions of the communications modules described in this manual, you need the following CPUs:

- **CP 1200**

  CPU with firmware version as of V4.3

- **CP 1542SP-1 IRC**

  CPU as of firmware version V2.0:

  – CPU 1510SP-1 PN

  – CPU 1510SP F-1 PN

  – CPU 1512SP-1 PN

  – CPU 1512SP F-1 PN

  You will find more detailed information on the CPUs and the BusAdapters in the manual /9/ (Page 175).

1.9 Configuration examples

Configuration with CP for secure network separation

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

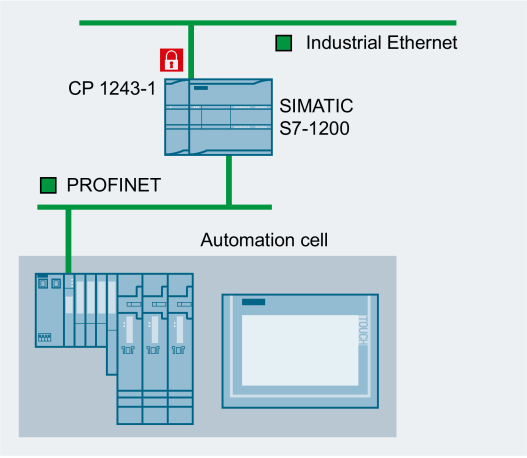


Figure 1-1 Secure communication with CP 1243-1

Configuration with sending of e-mails:

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

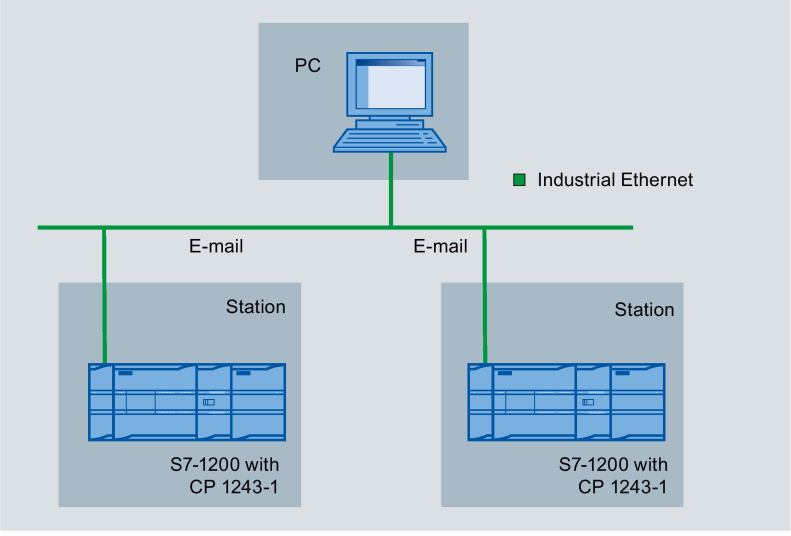


Figure 1-2 Sending e-mails

SMS messages and e-mails from mobile wireless CPs

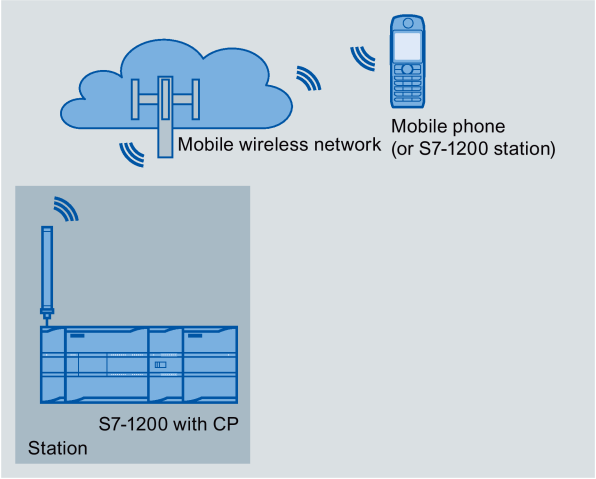


Figure 1-3 Sending messages by SMS from an S7-1200 station

SMS

A mobile wireless CP can send SMS messages to a mobile phone or a configured S7 station or receive them from these stations. The mechanisms for this are as follows:

- SMS messages generated and sent as the result of an event. They are configured in the messages editor.
- SMS messages that are sent or received due to calling the corresponding program blocks of Open User Communication.
- Using a mobile phone, a diagnostics SMS can be requested, see section Diagnostics options (Page 119).

For all mobile phones that send SMS messages to the CP, the authorize phone number must be specified in the STEP 7 configuration of the CP (parameter group "Security > Authorized phone number").

E-mails

The CP can send e-mails to a PC with an Internet connection or a mobile phone. The mechanisms for this are as follows:

- E-mails generated and sent as the result of an event. They are configured in the messages editor.
- E-mails sent as a result of calling the program block TMAIL_C.

For secure transmission of e-mails, the CP must have the current time.

Direct communication between stations

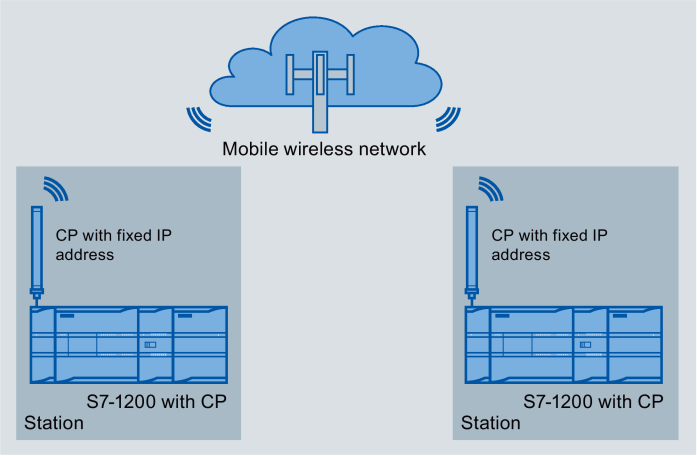


Figure 1-4 Direct communication between two S7 stations - here via mobile wireless CPs

In the configuration shown, two SIMATIC S7 stations communicate directly with each other using the CP via the mobile wireless network.

In this application, the network service provider must provide a fixed IP address for each CP.

Telecontrol with a non-redundant master station (TCSB)

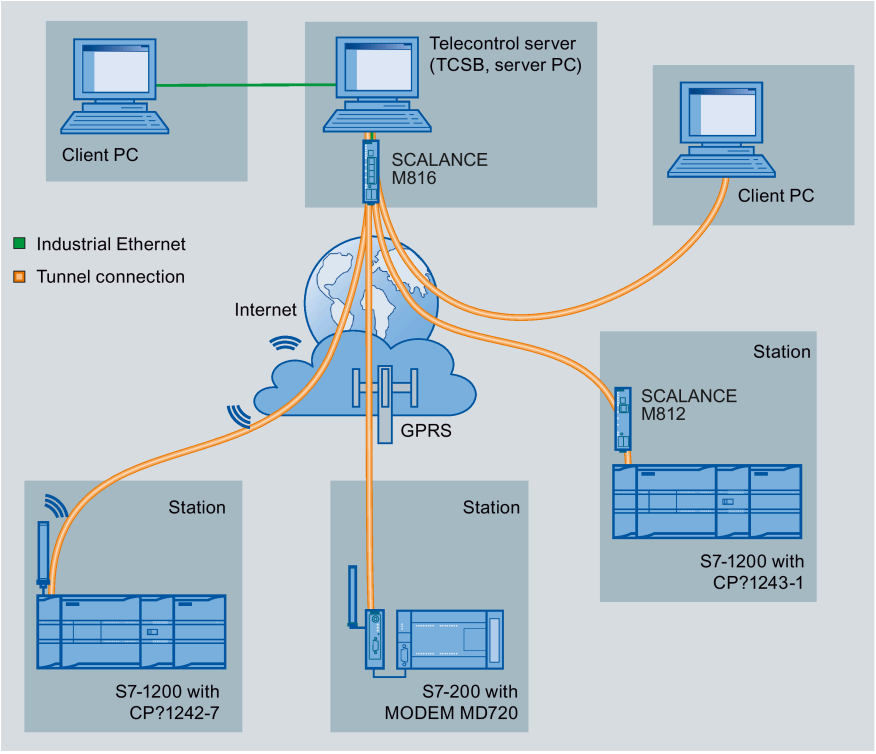


Figure 1-5 Communication between S7 stations and a master station (TCSB)

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

- Telecontrol communication between stations and master station

  The communication in the example shown takes place via the following paths and communication modules:

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

    The connection of a station to CP 1542SP-1 IRC is also possible.

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

    The connection of a station to CP 1243-7 LTE is also possible.

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

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

  The creation of VPN connections security CPs and the telecontrol server is optional.

- Inter-station communication

  Stations with compatible CPs can communicate with each other by sending the frames via the telecontrol server.

  For compatible CPs, refer to the section Inter-station communication (Page 15).

Telecontrol with a redundant master station (TCSB)

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

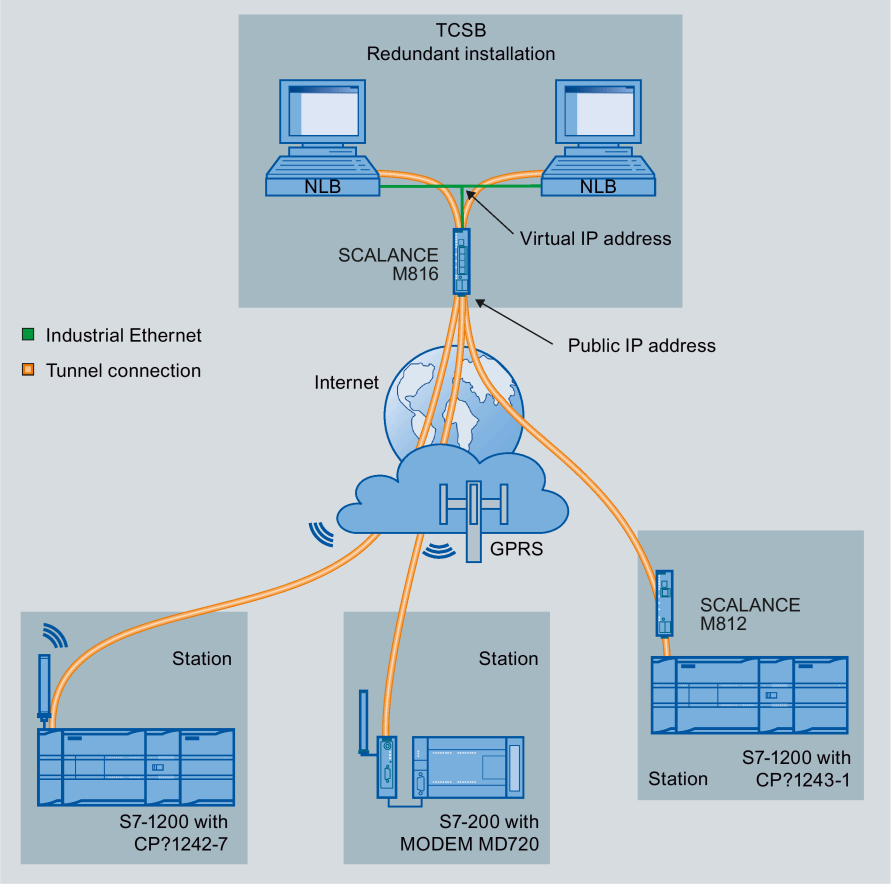


Figure 1-6 S7 station communication with a redundant a master station

TeleService via the mobile wireless network

In TeleService via the mobile wireless network, an engineering station on which STEP 7 is installed communicates via the mobile wireless network and the Internet with the mobile wireless CP in the S7-1200.

Since the firewall of the network provider is normally closed for connection requests from the outside, a switching station between the remote station and the engineering station is required. This switching station can be a telecontrol server or, if there is no telecontrol server in the configuration, a TeleService gateway.

- **TeleService with telecontrol server**

  The connection runs via the telecontrol server.

  – The engineering station and telecontrol server are connected via the Intranet (LAN) or Internet.

  – The telecontrol server and remote station are connected via the Internet and via the mobile wireless network.

  The engineering station and telecontrol server can also be the same computer; in other words, STEP 7 and TCSB are installed on the same computer.

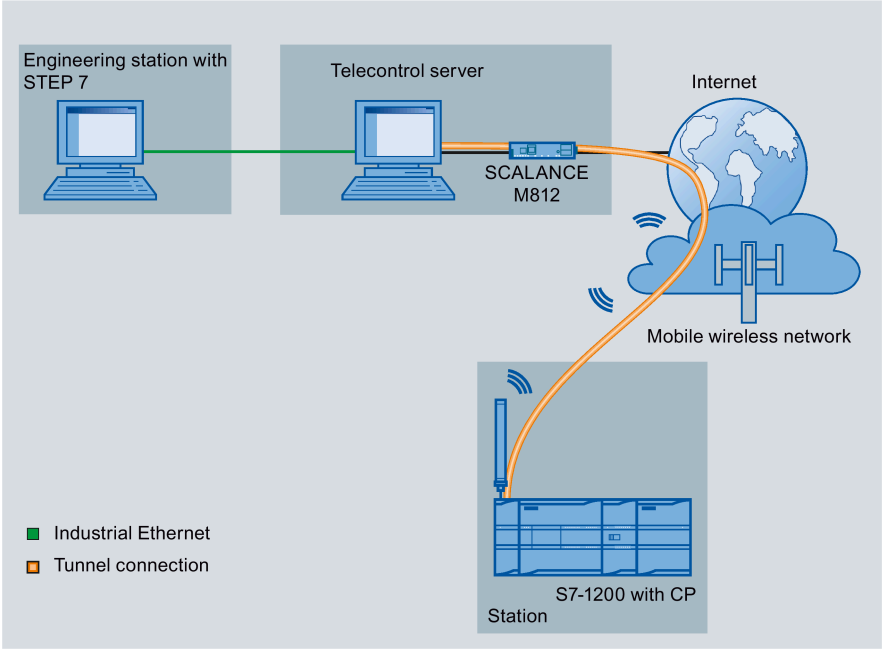


Figure 1-7 TeleService via the mobile wireless network in a configuration with telecontrol server

- **TeleService with TeleService gateway (via LAN)**

  The connection between the engineering station and S7 station is via the TeleService gateway.

  The engineering station is connected to the TeleService gateway via LAN.

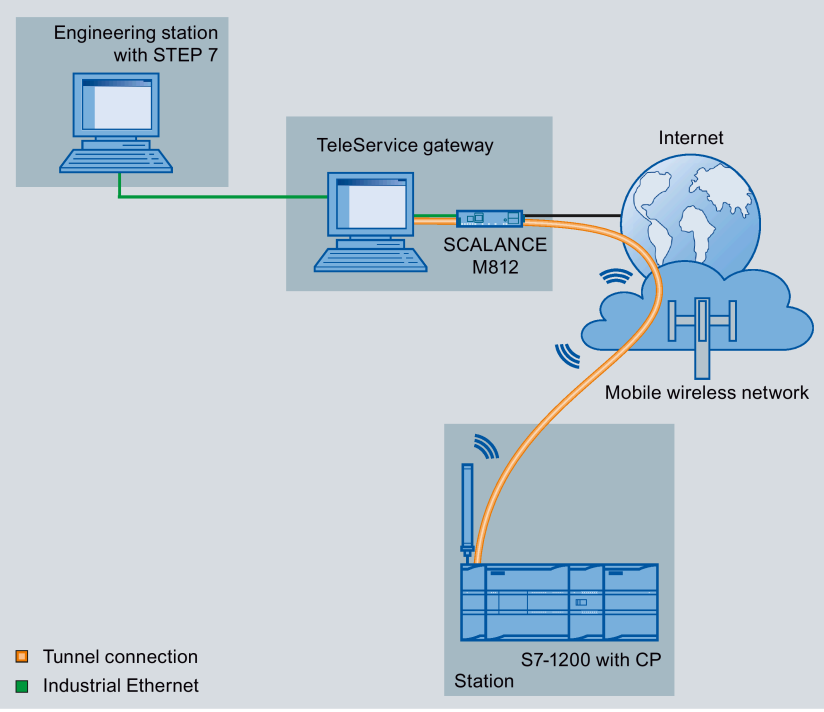


Figure 1-8 TeleService via the mobile wireless network with TeleService gateway connection via LAN

- **TeleService with TeleService gateway (via the Internet)**

  The connection between the engineering station and S7 station is via the TeleService gateway.

  The engineering station is connected to the TeleService gateway via the Internet.

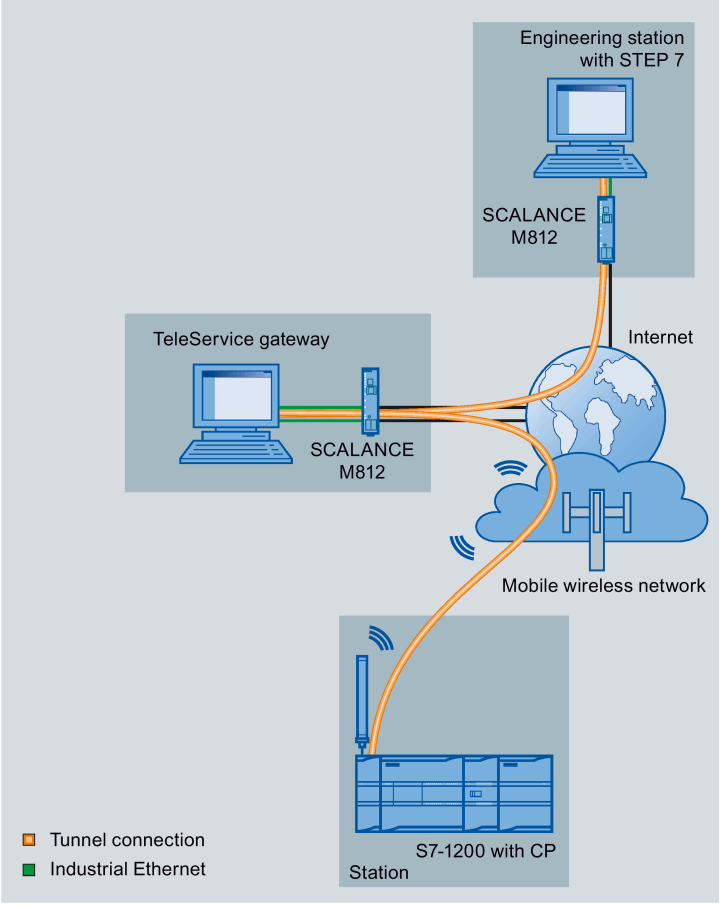


Figure 1-9 TeleService via the mobile wireless network with TeleService gateway connection via the Internet

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.

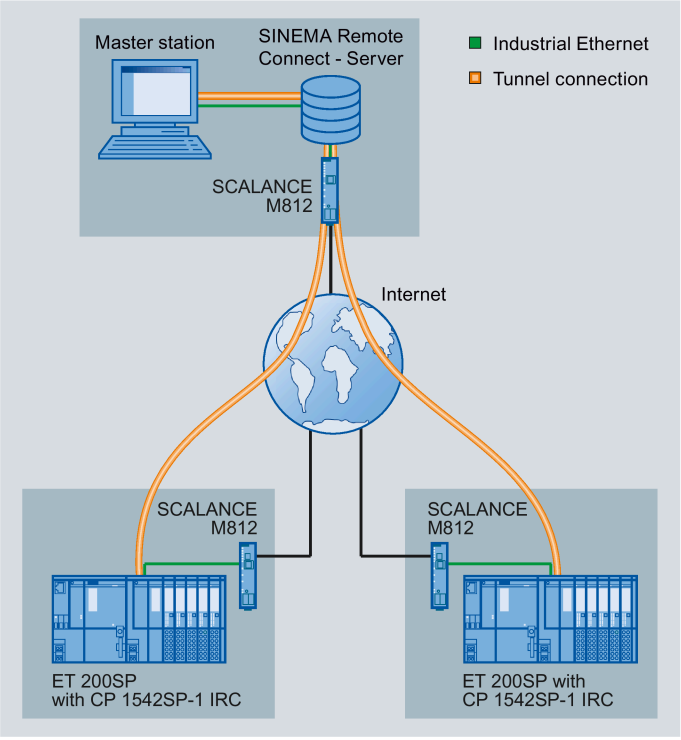


Figure 1-10 Configuration example of an ET 200SP with CP 1542SP-1 IRC for telecontrol communication via SINEMA RC

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.

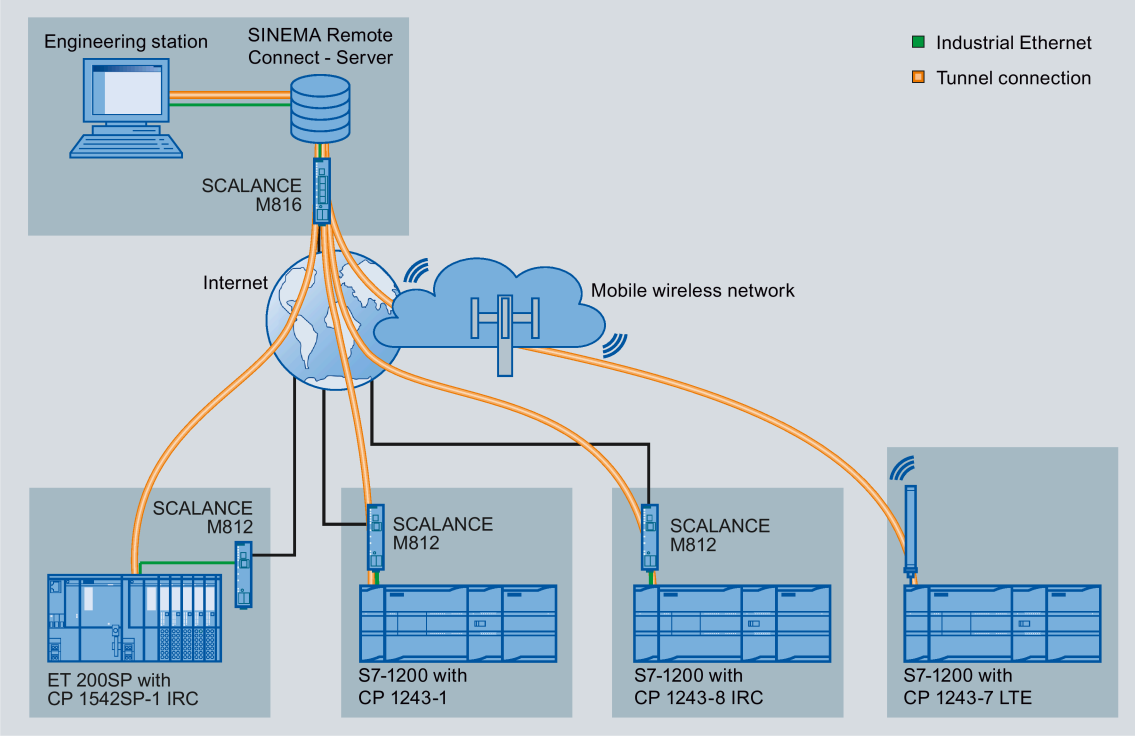


Figure 1-11 Connection of stations to engineering station via SINEMA RC

Configuration 2

2.1 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.
  - Here you can find information on Industrial Security:
    Link: (http://www.siemens.com/industrialsecurity)
  - You can find a selection of documentation on the topic of network security here:
    Link: (https://support.industry.siemens.com/cs/ww/en/view/92651441)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.

  Information regarding new firmware versions is available at the following address:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/21764/dl)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

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

Security functions of the product

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

- Protection levels

  Configure a protection level of the CPU.

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

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

    If you connect to public networks, you should use the firewall. Think about the services you want to allow access to the station via public networks. By limiting the "transmission speed" via IP packet filter rules in the firewall, you make use of the possibility of restricting flooding and DoS attacks.
  - Use the secure protocol variants NTP (secure) and SNMPv3.
  - Using the security functions of the telecontrol protocols.
  - Leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CP disabled.
- Logging function

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

Passwords

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

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

Protocols

Secure and non-secure protocols

- Only activate protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.
  - The NTP protocol provides a secure alternative with NTP (secure) if you do not use telecontrol communication.
  - The HTTP protocol provides a secure alternative with HTTPS when accessing the Web server (configuration of the CPU).
- Deactivate DHCP at interfaces to public networks such as the Internet, for example, to prevent IP spoofing.

Table: Meaning of the column titles and entries

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

- **Protocol / function**

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

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

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

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

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

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

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

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

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

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
S7 and online connections	102 (TCP)	Closed	Open after configuration *	No
Online security diagnostics	102 (TCP)	Open	Open after configuration *	No
Communication via SINEMA RC	443 (TCP)	Closed	Open after configuration	Yes
SysLog	514 (UDP)	Closed	Open after configuration	No
HTTP	80 (TCP)	Closed	Open after configuration	Yes **
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)
Syslog	514 (UDP)	Closed	Open after configuration	No

***** Some service providers consider the opening of port 102 a security vulnerability.
To avoid opening port 102 during online diagnostics, see section Online security diagnostics via port 8448 (Page 139).

****** Authentication using the telecontrol password.

Ports of communications partners and routers

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

These can be, if supported and used:

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

2.2 Information required for configuration

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

Information for telecontrol communication

The following information is required for the STEP 7 configuration of the CP. It is configured in the "Partner stations" parameter group.

- Address of the telecontrol server
  - "Partner IP address"

    Fixed IP address of the DSL router via which the telecontrol server is connected to the Internet.

    or
  - Name of the telecontrol server that can be resolved by DNS
  - "Partner port"

    IPT listener port of the telecontrol server. Default setting: 55097

  If only connections with TCSB are used (no direct communication between stations), a dynamic IP address can be assigned to the CP by the Internet service provider.

  For addressing a redundant TCSB system, refer to the section Partner stations > Telecontrol server (Page 59).
- DNS server address(es)

  You require the DNS server address if you address the telecontrol server using a name that can be resolved by DNS and the DNS server is not operated by the network provider. You configure the DNS server in the parameter group "DNS configuration":
  - If you do not specify an address, the DNS server address is obtained automatically from the network provider (recommended procedure).
  - If you want to use a different DNS server, enter its IP address. In this case, DNS servers of the network provider are not taken into account.

Information for mobile wireless CPs

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

- Own phone number of the CP (required for TeleService)
- Authorized phone numbers

  Call numbers of the nodes that can instigate connection establishment by the CP with an SMS message or call.
- APN

  Name of the access point (APN) from the mobile wireless network to the Internet

  (information from the mobile wireless network provider)

- APN user name

  User name for the access point of the mobile wireless network provider
- APN password

  Password for the access point of the mobile wireless network provider
- Node number of the SMS master station (SMSC) when using SMS
- PIN of the SIM card

Note

Configured PIN and PIN on the SIM card must match.

If you enter the PIN of the SIM card of the CP incorrectly during STEP 7 configuration and download the station, the CP stores the wrong PIN. An incorrectly entered PIN is transferred by the CP only once so that the SIM card is not locked.

If you change the PIN of the SIM card externally to the incorrectly configured PIN (new PIN of the SIM card = incorrectly entered PIN in STEP 7), the CP rejects this PIN again without checking it.

Note

Solution after entering an incorrect PIN:

To avoid the PIN being rejected by the CP again, use a PIN that is different from the incorrectly entered PIN. Procedure:

- If the PIN of the SIM card was not changed:
  - Configure the PIN in STEP 7 with the PIN of the SIM card.
  - Reload the station.
- If the original PIN of the SIM card was changed externally to the PIN that was previously incorrectly entered in STEP 7:
  - Change the PIN of the SIM card externally to a new PIN that has not yet been incorrectly configured in STEP 7.
  - Change the configured PIN in STEP 7 to the newly assigned PIN of the SIM card.
  - Reload the station.

CP parameter for configuring the telecontrol server

The following parameters from the STEP 7 configuration of the CP are required for the configuration of the telecontrol server.

You can find the following parameters in the "CP identification" parameter group:

- Access ID

  The Access ID is formed from the hexadecimal values of the following parameters:

  – Project number

  – Station number

  – Slot of the CP

- Telecontrol password

The following parameters in the "Authorized phone numbers" parameter group are required for TeleService via the mobile wireless network:

- Authorized phone numbers

2.3 Communication types

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

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

"Communication types" parameter group

- **Enable telecontrol communication**

  Enables telecontrol communication on the CP.

  – For the Ethernet CPs, select the desired telecontrol protocol.

  – For mobile wireless CPs, the "TeleControl Basic" protocol is the default for communication with the telecontrol server.

    To use TeleService via the mobile wireless network you need to enable this function.

  To use telecontrol communication, the you also need to enable the security functions.

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

  (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

  Enables communication via SINEMA RC in the CP.

  For telecontrol communication via SINEMA Remote Connect see the section SINEMA Remote Connect (Page 167).

- **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.

  To use TeleService via the mobile wireless network you need to enable this function.

- **Enabling S7 communication to the CPU**

  Enables the functions of S7 communication with the assigned SIMATIC CPU and the S7 routing.

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

  S7 routing is supported by the following modules:

  – CP 1243-1, CP 124x-7, CP 1243-8

    As of CP firmware V2.1 with CPU ≥ V4.2

  – CP 1542SP-1 IRC

    As of CP firmware V1.0 with CPU ≥ V2.0

- **Enabling SMS**

  (only mobile wireless CPs)

  Enables sending and receiving of SMS messages.

  The function can be enabled regardless of whether telecontrol communication is enabled.

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

2.4 Mobile wireless communications settings

"Mobile wireless settings"

Validity: CP 124-7 GPRS V2, CP 1243-7 LTE

In this parameter group you configure the following parameters:

- **CP phone number**

  Telephone number of the CP

- **Activate PIN**

  If your service provider requires a PIN, enable this option.

- **PIN**

  PIN of the SIM card

- **Enable data services**

  Activates the use of the data services in the mobile wireless network for the CP.

  Note
  Subsequent disabling

  If you have already used data services in operation and then disable them later, you need to reload the configuration data and change the CPU to STOP and then RUN.

- **GPRS (2G) / UMTS (3G) / LTE**

  For CP 1243-7 LTE enable the mobile wireless service(s) you want to use. You can enable individual mobile wireless services or all of them.

- **SMSC**

  Phone number of the SMS center (Short Message Service Center)

  The box has the following options:

  – No number

    As default, the CP adopts the SMSC data of the service provider directly from the inserted SIM card. if you want to use the SMSC number of the SIM card, leave the box empty.

  – Configured number

    If you want to use a different SMSC, enter the phone number of this SMSC.

    Note the following:

Note

Permanent storage of the SMSC number

If you configure an SMSC number, the CP no longer accesses the SMSC data of the SIM card. This is also the case if you delete the SMSC number from the configuration again.

Recommendation:
When you configure an SMSC number, first note down the SMSC number of your service provider located on the SIM card. If you want to use it again later, you can then use the SMSC of your provider again by configuring the SMSC number.

"APN settings"

In this parameter group, you configure the data of the access point. You require the APN to send e-mails.

By entering your country in the "Country" box, you can select one of the preset APNs from the drop-down list.

Alternatively configure the APN manually.

The CPs support APNs with IPv4 and IPv6 addresses.

User names and passwords can contain up to 64 characters. You will find the characters permitted in the section Character set for passwords and messages (Page 116).

"List of preferred networks"

In this parameter group, you specify the dial-in behavior of the CP into various mobile wireless networks.

"TeleService settings"

In this parameter group, you specify the connection parameters for the TeleService server.

You will find an overview of configuration for TeleService and more information on this topic in the section TeleService (Mobile wireless CPs) (Page 147).

2.5 Ethernet interface

The Ethernet interface

- **Ethernet CPs**

  The telecontrol communication of the Ethernet CPs takes place over the Ethernet interface. Configure the necessary parameters.

- **Mobile wireless CPs**

  Mobile wireless CPs do not have a physical Ethernet interface.

  In STEP 7, the Ethernet interface is used as a placeholder for the configuration of various address and monitoring parameters.

  When using security functions, you must network the interface.

Ethernet addresses

Here you configure the IP address of the CP and the network connection.

If you enable security functions, for example when using telecontrol communication, for reasons of consistency you need to network the CP. To do this create any Ethernet network.

Options for mobile wireless CPs:

- **Dynamic IP address**

  Enable this option if the CP is assigned the IP address dynamically by the network provider.

- **Fixed IP address from the mobile wireless network provider**

  Enable this option if you have a mobile wireless contract with which the network provider assigns the CP a fixed IP address.

  This is necessary when using S7 communication and receiving data via Open User Communication.

2.5.1 IPv6 (Ethernet CPs)

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.

2.5.2 Advanced options

TCP connection monitoring

The following parameters have an effect on the transport layer (OSI layer 4).

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

Note the option of customizing the global value configured here in the "Partner stations" parameter group for individual communication partners, refer to the section Partner stations > Telecontrol server (Page 59).

- **TCP connection monitoring time**

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

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

  – **The parameter below the Ethernet interface**

    The monitoring time is configured at the Ethernet interface globally for all TCP connections.

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

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

  If you want to change the value for individual partners, you can adapt the value individually in "Partner stations".

- **TCP keepalive timeout**

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

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

  – **The parameter below the Ethernet interface**

    The value is configured at the Ethernet interface as a global setting for all TCP connections.

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

    The value can be adapted for each partner individually in "Partner stations".

    If disruptions or delays occur often when transferring in a mobile wireless network, it may be advisable to increase the value, for example, to 30 or 60 seconds.

Transmission settings – TeleControl Basic

The following parameters have an effect on the application layer (OSI layer 7) of the TeleControl Basic protocol.

- **Connection establishment delay**

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

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

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

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

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

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

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

  Note

  Connection establishment via mobile wireless CPs

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

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

- **Send monitoring time**

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

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

- **Watchdog monitoring time**

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

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

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

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

- **Key exchange interval**

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

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

2.5.3 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.

Notes for mobile wireless CPs:

From a PC you can access the Web server of the station via TCSB if the PC is connected to the telecontrol server via LAN. For the requirements, refer to the manual /2/ (Page 174).

With slow transmission paths between telecontrol server and station, make sure that you set the update time of the Web browser suitably low.

You will find information on the Web server of the S7-1200 in the manual /7/ (Page 175).

You will find information on the Web server of the ET 200SP in the manual /8/ (Page 175).

2.6 Time-of-day synchronization

Note

Time-of-day synchronization when using SINEMA RC

When the CP obtains the time from the CPU, set the CPU time manually during commissioning when using SINEMA Remote Connect; see note in section Set time for operation with Security / SINEMA RC (Page 117).

Note

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

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

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

CP 1542SP-1 IRC

As of firmware version V2.1 of the CP, only 1 module in the station can be time client. This module distributes the time of day within the station.

Note

Time-of-day synchronization with enabled security functions

When you enable the security functions, the CP time must be synchronized. You should also refer to the information in the section Creating a VPN tunnel for S7 communication between stations (Page 76).

Synchronization method

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

There is no forwarding of the time of day from the station to the subnet for the named devices.

Time-of-day synchronization of the CPU

As the synchronization method, with the CPU only NTP can be selected.

For the time-of-day synchronization of the CPU via a CP see below.

Time-of-day synchronization of CPs

The following synchronization methods are available for the CPs:

- **NTP**

  For telecontrol CPs, NTP can also be used when telecontrol communication is disabled. In this case, the CP is used as an extended PROFINET interface of the CPU.

  The address of the NTP server can also be entered as a URL, e.g. <ntp.server.com>.

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

- **Time from partner**

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

  Default with enabled telecontrol communication

- **Time from CPU (S7-1200)**

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

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

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

  If no time synchronization is configured at the CP, the following mechanisms apply.

  – S7-1200

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

  – ET 200SP

    If the time-of-day synchronization of the CP is disabled, CPs with firmware version ≥ V2.1 are automatically synchronized in a cycle of 10 seconds by a CPU with firmware version ≥ V2.0.

    For CPs with firmware-Version ≤ V2.0 the CP reads the CPU time once during start-up, even if the option "No time source" is selected as Time source. The subsequent time synchronization then depends on the configured synchronization method.

Forwarding the time from the CP to the CPU

Depending on the firmware version of the modules involved, the time-of-day of the CP can be forwarded to the CPU using the following methods.

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

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

- **Forwarding of the CP time via PLC tag**

  With the following firmware versions this is the only option for forwarding the clock time from the CP to the CPU:

  – S7-1200: CP firmware ≤ V2.1.6

  – ET 200SP: CP firmware ≤ V2.0

  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.

  Configure the PLC tag in the parameter group "Communication with the CPU" of the CP.

  CPs with higher firmware versions also support the function; in addition, they support the following function.

- **Forwarding of the CP time via backplane bus**

  The CP time is automatically forwarded to the CPU, when a synchronization method is configured at the CP, and CP and CPU have one of the following firmware versions:

  – S7-1200: CP firmware ≥ V3.0 and CPU firmware ≥ V4.2

  – ET 200SP: CP firmware ≥ V2.1 and CPU firmware ≥ V2.0

  Since the CPU automatically adopts the CP time, you no longer require the forwarding option using the PLC tag for these firmware versions, but you can still use it.

2.7 Partner stations

2.7.1 Partner stations > Telecontrol server

Partner stations > "Telecontrol server"

- **Partner number**

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

- **Station address**

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

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

- **Partner IP address**

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

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

- **Connection monitoring**

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

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

  The global values can be adapted individually for the connection to the telecontrol server in the "Partner stations > Telecontrol server" parameter group. The values set in "Partner stations" overwrite the global values that are set in the "Ethernet interface (X1) > Advanced options > TCP connection monitoring" parameter group.

- **TCP connection monitoring time**

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

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

  The monitoring time is specified at a higher level for the Ethernet interface as the default for all TCP connections, see also section Ethernet interface (Page 51).

  You will find information on the acknowledgment of messages in the section "Acknowledgment (Page 14)".

  – **The parameter below the Ethernet interface**

    The monitoring time is configured at the Ethernet interface globally for all TCP connections.

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

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

    If you want to change the value for individual partners, you can adapt the value individually in "Partner stations".

    If you want to check the connection at shorter intervals, reduce the value.

    If disruptions or delays occur often when transferring in a mobile wireless network, it may be advisable to increase the value.

- **TCP keepalive timeout**

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

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

  – **The parameter below the Ethernet interface**

    The value is configured at the Ethernet interface as a global setting for all TCP connections.

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

    The value can be adapted for each partner individually in "Partner stations".

    If disruptions or delays occur often when transferring in a mobile wireless network, it may be advisable to increase the value, for example, to 30 or 60 seconds.

- **Connection mode**

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

  The CPs only support this connection mode.

  For information on connection establishment, refer to the section "Connection establishment (Page 62)".

- **Connection establishment**

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

- **Partner port**

  Number of the listener port of the telecontrol server.

  Default setting: 55097

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

- **Report partner status**

  If the "Report partner status" function is enabled, the CP signals the status of the communication to the remote partner to the CPU via a tag (data type WORD).

  – Bit 0 of the "PLC tag for partner status" is set to 1 when the partner can be reached.

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

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

    - 0: Send buffer OK

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

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

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

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

2.7.2 Connection establishment

Connection establishment

- Connection to the telecontrol server

  The connection to the telecontrol server is always established by the CP.

  If a connection established by the CP is interrupted, the CP automatically attempts to re-establish the connection. Note the settings for re-establishing the connection in STEP 7, refer to the section Ethernet interface (Page 51).

  Note

  Connection interrupted by the mobile wireless network provider

  When using mobile wireless services, remember that existing connections can be interrupted by mobile wireless network providers for maintenance purposes.

- Connections with direct communication (Open User Communication) and S7 communication

  Connections are established as soon as the corresponding program blocks are called on the CPU.

  This also applies to the situation when a different S7 station sends data. In this case, the corresponding receive blocks are called by the receiving station.

2.7.3 Partner for inter-station communication

Inter-station communication

In this table, you specify the partners for inter-station communication of the CP. The partners for inter-station communication are the CPs in S7 stations.

Connections for inter-station communication run via the telecontrol server.

Note the configuration limit of the CP for inter-station communication:

- In total: Max. 15 partners

  of which:

  – Receive: Max. 15 partners

  – Send: Max. 3 partners

    You specify the send function using the "Send buffer" parameter.

The partners for inter-station communication will be configured later in the individual data points, see section "Partner stations" tab (Page 111).

Partner

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

You specify the partner CP for inter-station communication with the parameters "Project", "Station" and "Slot".

Project

Here, enter the project number of the CP in the partner station.

You will find the parameter in the parameter group "Security > CP identification" on the partner CP.

Station number

Here, enter the station number of the CP in the partner station.

You will find the parameter in the parameter group "Security > CP identification" on the partner CP.

Slot

Here, enter the slot number of the CP in the partner station.

You will find the parameter in the parameter group "General" on the partner CP.

Send buffer

Select the option for enabling the CP for active inter-station communication (sending to up to three partners).

Frames for inter-station communication are stored in the send buffer (frame memory) of the CP if the connection is disturbed.

Note that the capacity of the send buffer is shared by all communication partners, including the telecontrol server.

Access ID

The access ID of the partner CP is displayed here.

The Access ID (DWORD) is formed from the hexadecimal values of project number, station number and slot:

Bits 0 to 7: Slot

Bits 8 to 20: Station number

Bits 21 to 31: Project number

2.8 DNS configuration

Configuring DNS servers

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

When addressing a communication partner as FQDN, you need to configure a DNS server. The IP address (IPv4/IPv6) of the communication partner is determined via the configured DNS server. When using IPv6 addresses, make sure to configure the DNS servers accordingly.

When the CP uses mobile wireless service and the mobile wireless provider operates a DNS server in its network, the configuration has the following effects:

- No configuration of a DNS server

  IP addresses are automatically obtained from the DNS server of the network operator (recommended procedure).

- Configuration of a DNS server

  IP addresses are obtained from the configured DNS server. DNS servers of the network provider are not taken into account.

2.9 Communication with the CPU

Communication with the CPU

Using the first three parameters you specify settings for the cyclic access of the CP to the CPU. You will find information on the structure of the sampling cycle in the section Read cycle (Page 99).

- **Cycle idle time**

  Wait time between two sampling cycles of the CPU memory area

- **Max. number of write jobs**

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

- **Max. number of read jobs**

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

- **Frame memory size**

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

  The size of the frame memory is divided equally among all communications partners. You will find the size of the frame memory in the section Performance data and configuration limits (Page 20).

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

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.

  You can display the status of the PLC tag via the Web server of the CPU.

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.

CP diagnostics

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

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

- **Enable advanced CP diagnostics**

  Enable the option to use advanced CP diagnostics.

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

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

- **Diagnostics trigger tag**

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

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

  Note

  Fast setting of the diagnostics trigger tag

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

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

- **Frame memory overflow warning**

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

- **Frame memory occupation**

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

- **Current IP address**

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

- **Mobile wireless signal quality (LED)**

  PLC tag (data type UInt) for the signal quality of the local mobile wireless network as this is displayed by the "SIGNAL QUALITY" LED.

- **Mobile wireless signal quality (dBm)**

  PLC tag (data type INT) for the signal quality of the local mobile wireless network as a dBm value.

- **'NETWORK' LED**

  PLC tag (data type UInt) for the status of the connection for the data service in the mobile wireless network.

  Meaning of the values (decimal)

  – 0 = Booked out of the network
  – 1 = Wrong PIN
  – 2 = Wrong, defective SIM card or not plugged in.
  – 3 = Waiting for PIN / no PIN configured
  – 4 = Booked into the network

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

  PLC tag (data type DTL) for the date on which the CP last logged in to the mobile wireless network.

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

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

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

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

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

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

- **TeleService status**

  Only for mobile wireless CPs in TeleControl Basic

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

  – 0 = No TeleService session active
  – 1 = TeleService session active

- **VPN IPsec status**

  The PLC tag (BOOL) indicates whether a VPN 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

2.10 Security

Note the range and application of the security functions of the CP, refer to the section Security functions (Page 17).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 68).

2.10.1 Security user

Creating a security user

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

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

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

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

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

Note

Special features for TeleService users

Note the restrictions regarding the length of the user name and the password for users who are going to use TeleService, see Configuration of the TeleService access (Page 148).

2.10.2 Security parameters of the CP

Parameter groups

If security functions are enabled, you will find the following parameter groups here:

- **CP identification**

  Here, you configure parameters for authenticating the CP with the telecontrol server.

  You will find details below.

- **Time-of-day synchronization**

  For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 56).

- **Authorized phone numbers**

  You will find details below.

- **E-mail configuration**

  You will find details below.

- **Certificate manager**

  You will find details below.

- **Firewall**

  You will find details below.

- **Log settings**

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

  You will find details below.

- **VPN**

  Here you configure the VPN communication.

  You will find details below.

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

- **VPN groups**

  Here you configure the VPN groups.

- **User management**

  Here you configure the users, roles and rights of the security users.

  This is for example necessary for TeleService access, see section TeleService (Mobile wireless CPs) (Page 147).

2.10.3 CP identification

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

- **Project number**

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

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

- **Station number**

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

- **Telecontrol password**

  Password for the authentication of the CP on the telecontrol server

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

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

- **Access ID**

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

  – Bits 0 - 7: Slot

  – Bits 8 to 20: Station number

  – Bits 21 to 31: Project number

See also

Character set for passwords and messages (Page 116)

2.10.4 Firewall

2.10.4.1 Pre-check of messages by the MAC firewall.

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

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

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

- Separate the two IP addresses only using a hyphen.

  Correct: 192.168.10.0-192.168.10.255

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

  Incorrect: 192.168.10.0 - 192.168.10.255

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

2.10.4.3 Firewall settings for configured connection connections via a VPN tunnel

IP rules in advanced firewall mode

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

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

See section Settings for online security diagnostics and downloading to station with the firewall activated (Page 71) for information on this.

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

Setting the firewall for online functions

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

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.

2.10.5 Authorized phone numbers (mobile wireless CPs)

SMS messages received only from subscribers with an authorized phone number

The CP only accepts an SMS if the sending communication partner is authorized based on its phone number. You configure these phone numbers in the "Authorized phone numbers" list.

"Authorized phone numbers"

A phone number entered here gives the sender who transfers this phone number the right to trigger connection establishment by the CP.

- If only an asterisk (*) is entered in the list, the CP accepts SMS messages from all senders.
- An asterisk (*) after a phone number body authorizes connection establishment for all nodes connected to the body (extension numbers).

  Example: +49123456* authorizes +49123456101, +49123456102, +49123456207 etc.

If the "Authorized phone numbers" list is empty, the CP cannot be induced to a connection establishment by a mobile phone.

2.10.6 E-mail configuration

Configuring e-mails

In the "E-mail configuration" entry, you configure the protocol to be used and the data for access to the e-mail server.

In the message editor ("Messages" entry), you configure the individual e-mails, see section Messages (Page 112).

Requirements for e-mail

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

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

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

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

E-mail configuration

If you want to use the secure transfer of e-mails, the module must have the current date and the current time of day.

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

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

- Port no. 587

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

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

- Port no. 465

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

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

On configuration of the passwords, see AUTOHOTSPOT.

Importing the certificate with encrypted transfer

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

Use the certificate by taking the following steps:

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

For the procedure, refer to the section Certificate manager (Page 83).

2.10.7 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.

2.10.8 VPN (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

2.10.8.1 VPN (Virtual Private Network)

VPN tunnel

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

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

The data traffic between two network components is handled unrestricted through a physical network. This allows networks to be connected together via an intermediate network.

VPN tunnels ensure integrity and confidentiality during data transmission.

Properties

- VPN forms a logical network that is embedded in a physical network. VPN uses the usual addressing mechanisms of the physical network, however it transports only the frames of the VPN subscribers and therefore operates independent of the rest of the physical network.
- VPN allows communication of the subscribers in the VPN network with the physical network.
- VPN is based on tunnel technology and can be configured for individual subscribers.
- 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)
- Protection of computers and their communication within and automation network
- Secure remote access from a PC/PG to automation devices or networks protected by security modules via public networks.

2.10.8.2 Addressing the CP when using VPN

IP addresses and VPN ports

In normal mobile wireless networks it is not possible to reach a dynamic IP address assigned to the CP by the mobile wireless network provider from the Internet. For this reason, for incoming connections make sure that the CP is assigned a fixed public IP address by the mobile wireless network provider.

You must also make sure that apart from this IP address, the ports required for VPN are reachable from the Internet.

2.10.8.3 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 are located in the same subnet.
- All receiving stations require a fixed IP address to be reachable via the public networks. For this, a special mobile wireless contract is normally necessary for the mobile wireless CP.

Note

Communication also possible via an IP router

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

Procedure

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

1. Creating a security user

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

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

Select "Activate security features"

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

You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

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

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

Note

Current date and current time on the CP for VPN connections

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

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

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

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

Configure the properties of the VPN group

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

   Result: The properties of the VPN group are displayed under "Authentication".
2. Enter a name for the VPN group. Configure the settings of the VPN group in the properties.

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

Note

Specifying the VPN properties of the CPs

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

Result

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

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

2.10.8.4 Communications partners in a VPN group

Configuring communications partners

If a node is intended to communicate with several CPs via VPN connections, all communications partners must be assigned to the same VPN group.

The CP itself can only communicate with a single communications partner via VPN.

2.10.8.5 Connection to the telecontrol server

No VPN connection between CP and TCSB

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

Thanks to the encrypted telecontrol protocol, the connection between the CP and telecontrol server is already protected.

2.10.8.6 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".

2.10.8.7 SYSLOG

Use of SYSLOG only with 1 VPN connection

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

2.10.8.8 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect Server

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

- Exporting the CA certificate (optional)

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

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

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

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

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

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

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- CA Certificate

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

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

- Fingerprint

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

Authentication

- Device ID

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

- Device password

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

  Max. number of characters: 127

Optional settings

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

- **Update interval**

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

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

- **"Connection type"**

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

  – Auto

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

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

  – PLC trigger

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

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

Note

Connection abort

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

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

- **PLC tag for connection establishment**

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

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

2.10.9 SNMP (Ethernet CPs)

SNMP

The CP supports the following SNMP versions:

- **SNMPv1**

  Available with enabled and disabled security functions

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

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

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

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

*) Note the use of lowercase letters!

Note

Security of the access

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

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

- **SNMPv3**

  Available only when security functions are enabled

  For information on configuring SNMPv3, refer to the section Diagnostics via SNMP (Ethernet CPs) (Page 139).

Configuration

- **"Enable SNMP"**

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

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

2.10.10 Certificate manager

Assignment of certificates

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

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

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

For a description of the procedure, refer to the section Handling certificates (Page 83).

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

2.10.11 Handling certificates

Certificate for authentication

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

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

Note

No certificate with security functions disabled.

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

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

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

1. Importing third-party certificates from communications partners

   ⇒ Global security settings of the project (certificate manager)

2. Assigning certificates, either:

   – Global security settings > Certificate manager > "Trusted certificates and root certification authorities"

   – Local security settings of the module > Certificate manager > "Certificates of the partner devices"

The steps are described in the following sections.

Importing third-party certificates from communications partners

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

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

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

Assigning certificates in the global security settings

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

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

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

Assigning certificates locally

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

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

   The "Certificate manager" table of the Global security settings is displayed.
4. In the table. select the required third-party certificate and to adopt it click the green check mark below the table.

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

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

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

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

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

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

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

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

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

Certificate for logging server

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

Change certificate: Subject Alternative Name

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

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

2.11 Data points

2.11.1 Data point configuration

Data point-related communication with the CPU

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

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

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

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

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

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

Note

Number of PLC tags

Observe the maximum possible number of PLC tags that can be used for data point configuration.

The formats and S7 data types of the PLC tags that are compatible with the data point types of the modules can be found in the section Datapoint types (Page 94).

Access to the memory areas of the CPU

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

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

Configuring the data points and messages in STEP 7

You configure the data points in STEP 7 in the data point and message editor. You can open both editors alternatively as follows:

- Selecting the communications module

  Shortcut menu "Open the data point and messages editor"

- Via the project navigation:

  Project > directory of the relevant station > Local modules > required communications module

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

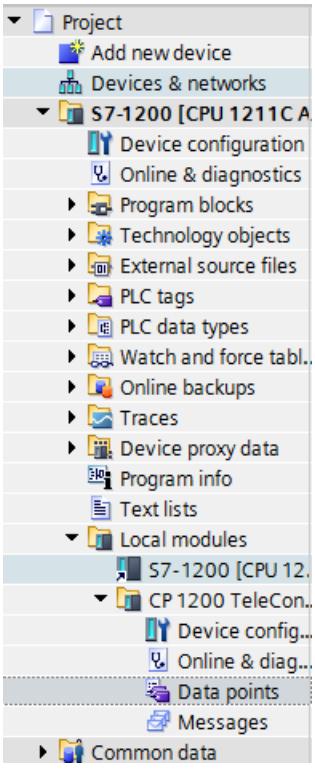


Figure 2-1 Configuring data points and messages

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

Figure 2-2 Switching over between the two editors

Creating objects

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

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

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

Figure 2-3 Data point table

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

Assigning data points to their data source

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

For the assignment you have the following options:

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

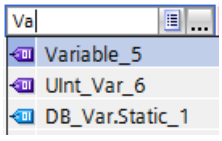
  All configured PLC tags and the tags of the created data blocks are displayed. Select the required data source with the mouse or keyboard.

- Click the symbol ....

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

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

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

  Select the required data source.

Note

Assignment of parameter values to PLC tags

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

Arranging columns and rows, showing/hiding columns

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

- Arrange columns

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

- Sorting objects

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

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

- Adapting the column width

  You can reach this function with the following actions:

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

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

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

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

- Showing / hiding columns

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

Copying data points and messages

As with many other programs, you can copy and paste objects in the data point or message editor.

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

- Cut
- Copy
- Paste

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

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

- Delete

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

With the <Shift> key pressed, you can select the beginning and the end of a contiguous area.

Exporting and importing data points

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

Communications modules with the same telecontrol protocol are compatible with each other. Data points can be imported and exported between compatible modules.

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

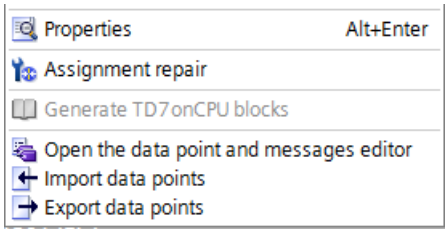


Figure 2-4 Shortcut menu of the module

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

It is not possible to import data points of an older project into a project that was created in STEP 7 V15.1 because the scope of parameters of certain data point types is not identical. However, the import works when missing parameters (see the following parameter descriptions) are added in the CSV file.

Export

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

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

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

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

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

Editing the export files

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

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

The lines of the CSV file have the following content:

- Line 1: ,Name,Type,

  This line must not be changed.

- Line 2: PLC,<CPU name>, <CPU type>,

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

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

  The CPU type must correspond exactly to the name of the CPU in the catalog.

- Line 3: Module,<module name>,<module type>,

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

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

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

  The module type must correspond exactly to the name of the module in the catalog.

- Line 4: Parameter names (English) of the data points

  This line must not be changed.

- Lines 5..n: Values of the parameters according to line 4 of the individual data points

  You can change the parameter values for the particular station.

Importing into a module

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

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

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

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

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

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

Importing into several modules

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

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

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

Restrictions for the import of data points

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

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

  Example: If a data point to be imported uses a time trigger, the import will be aborted if no time-of-day synchronization was configured for the module.

- The telecontrol protocol used by the module differs from that of the original module.

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

Only when importing into several modules:

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

Assignment repair

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

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

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

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

2.11.2 "General" tab

"General" tab

Not all of the following parameters are supported by all protocols.

General parameters

- **Name**

  Unique name of the data point. For the syntax, refer to the section Syntax of the data point names (Page 93).

- **PLC tag**

  For assignment of a tag to a data point, refer to the section Data point configuration (Page 86).

- **Data point type**

  See section Datapoint types (Page 94)

- **Data point index**

  The index is an addressing parameter for a data point. For information on the configuration rules, refer to the section Data point index (Page 96).

- **Type of transmission**

  The type of transmission determines whether the value of the data point is only saved in the image memory or also in the send buffer of the CP. See section Process image, type of transmission, event classes (Page 97) for information on this.

- **Read cycle**

  Only configurable for input data points

  Prioritizes the reading or writing of the data point value in the scan cycle of the CPU; see section Read cycle (Page 99).

  The fast cycle is suitable for data to be acquired quickly (alarms, contact changeover messages). They are read in every cycle.

2.11.3 Syntax of the data point names

Character set for data point names

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

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

Forbidden characters:

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

2.11.4 Datapoint types

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

As of the firmware version named in the preface along with STEP 7Basic V14, the CP supports the following data point types and data types.

The direction relates to the direction of transfer:

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

Data point types

Table 2- 1 Supported data point types and compatible S7 data types

Format (memory requirements)	Data point type	Direction	S7 data types	Operand area
Bit	Digital input	in	Bool	I, Q, M, DB
	Digital output	out	Bool	Q, M, DB
Byte	Digital input	in	Byte, Char, USInt	I, Q, M, DB
	Digital output	out	Byte, Char, USInt	Q, M, DB
Integer with sign (16 bits)	Analog input	in	Int	I, Q, M, DB
	Analog output	out	Int	Q, M, DB
Counter (16 bits)	Counter input [1]	in	Word, UInt	I, Q, M, DB
Integer with sign (32 bits)	Analog input	in	DInt	Q, M, DB
	Analog output	out	DInt	Q, M, DB
Counter (32 bits)	Counter input [1]	in	UDInt, DWord	I, Q, M, DB
Floating-point number with sign (32 bits)	Analog input	in	Real	Q, M, DB
	Analog output	out	Real	Q, M, DB
Floating-point number with sign (64 bits)	Analog input	in	LReal	Q, M, DB
	Analog output	out	LReal	Q, M, DB
Data block (1 .. 64 bytes)	Data	in / out	ARRAY [2]	DB
	Data	in / out	ARRAY [2]	DB

[1] Note the following section "Counter inputs".

[2] For the possible formats see the section "ARRAY" below.

Counter inputs

Counters can only be configured for communication with the telecontrol server as partner.

The S7 data types for the data point types "Counter input" support incremental (counting up) as well as decremental counters (counting down).

The counter inputs of the telecontrol server (TCSB), however, only count incrementally. When a counter input in TCSB is supplied with a decremental counter, TCSB assigns this variable the OPC quality code "UNCERTAIN".

ARRAY

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

- Byte, USInt (total of up to 64 per data block)
- Char (total of up to 64 per data block)

  CP-1200 as of firmware version V2.1.77
- Int, UInt, Word (total of up to 32 per data block)
- DInt, UDInt, DWord (total of up to 16 per data block)

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

Format of the time stamp

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

2.11.5 Status IDs of data points

Status IDs of data points

Along with the value of a data point, status identifiers of the data point are transferred in every frame. They can be evaluated by the communications partner.

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

- Quality = BAD, if:

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

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

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

For the meaning of the status bits, see below. The entries in the table row "Meaning" relate to the entry in the table row "Bit status".

Table 2- 2 Bit assignment of status byte 0

Bit	7	6	5	4	3	2	1	0
Flag name	-	NON_ EXISTENT	SB	LOCAL_ FORCED	CARRY	OVER_ RANGE	RESTART	ONLINE
Meaning	-	Data point does not exist or S7 address unreachable	Substitute value	*(Bit is not set.)*	Counted value overflow before reading the value	Limit value of the analog value preprocessing overshot / undershot	Value not updated after start	Value is valid, CPU in RUN
Bit status	*(always 0)*	1	1	*(irrelevant)*	1	1	1	1

Generation of events if a data point status changes

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

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

2.11.6 Data point index

Configuration of the data point index

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

- Input

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

- Output

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

Note

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

Note that for inter-station communication, the indexes of the two corresponding data points (data point pair) must be identical for the sending and receiving CP, see also section "Partner stations" tab (Page 111).

2.11.7 Process image, type of transmission, event classes

Saving the data point values

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

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

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

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

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

- **Triggered: event**

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

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

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

The image memory, the process image of the CP

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

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

The send buffer (frame memory)

The send buffer of the CP is the memory for the individual values of data points that are configured as an event. The maximum size of the send butter can be found in the section Performance data and configuration limits (Page 20).

The configured number of events is divided equally among all configured and enabled communications partners. For information on the configuration, refer to the parameter "Frame memory size" in the section Communication with the CPU (Page 64).

If the connection to a communications partner is interrupted, the individual values of the events are stored in the RAM of the CP.

When the connection returns, the buffered values are sent. The frame memory operates chronologically; in other words, the oldest frames are sent first (FIFO principle). If a frame was transferred to the communications partner, the transferred values are deleted from the send buffer.

If data cannot be transferred for a longer period of time and the send buffer is threatening to overflow, the TeleControl Basic protocol uses the forced image mode.

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

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

Types of transmission / event classes

The following types of transmission are possible:

- **Transfer after call**

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

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

- **Triggered (event)**

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

  The values of events are saved in the following situations:

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

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

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

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

  – **Every value triggered**

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

  – **Current value triggered**

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

2.11.8 Read cycle

Priority of the data points

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

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

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

- Fast cycle
- Normal cycle

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

Structure of the CPU scan cycle

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

- **High-priority read jobs**

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

- **Low priority read jobs**

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

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

- **Write jobs**

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

- **Cycle pause time**

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

2.11.9 "Trigger“ tab

Trigger

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

Saving the value of a data point configured as an event

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

- **Threshold value trigger**

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

- **Time trigger**

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

- **Event trigger (Trigger tag)**

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

  Resetting trigger tags in the bit memory area / DB:

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

Note

Fast setting of triggers

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

Note

Hardware trigger

You need to reset hardware triggers via the user program.

Transferring the value of a data point configured as an event

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

Transmission mode

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

- Spontaneous (unsolicited - direct transfer)

  The value is transferred immediately.

- Buffered transfer - Conditional spontaneous

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

  – The communications partner queries the station.

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

  – The fill level of the send buffer has reached 80% of its maximum capacity.

2.11.10 Threshold value trigger

Note

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

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

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

Note

Threshold value trigger with configured mean value generation

With enabled mean value generation, the absolute method for the calculation of the threshold value deviation is used for analog values with the threshold value trigger.

For the time sequence of the analog value preprocessing refer to the section "Analog value preprocessing" tab (Page 104).

Threshold value trigger

Function

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

Two methods are used to calculate the threshold value deviation:

- **Absolute method**

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

- **Integrative method**

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

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

Absolute method

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

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

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

Integrative method

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

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

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

Table 2- 3 Example of the integration calculation of a threshold value configured with 2.0

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

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

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

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

2.11.11 "Analog value preprocessing" tab

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

Requirements and restrictions

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

Note

Restrictions due to configured triggers

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

Sequence of the analog value preprocessing options

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

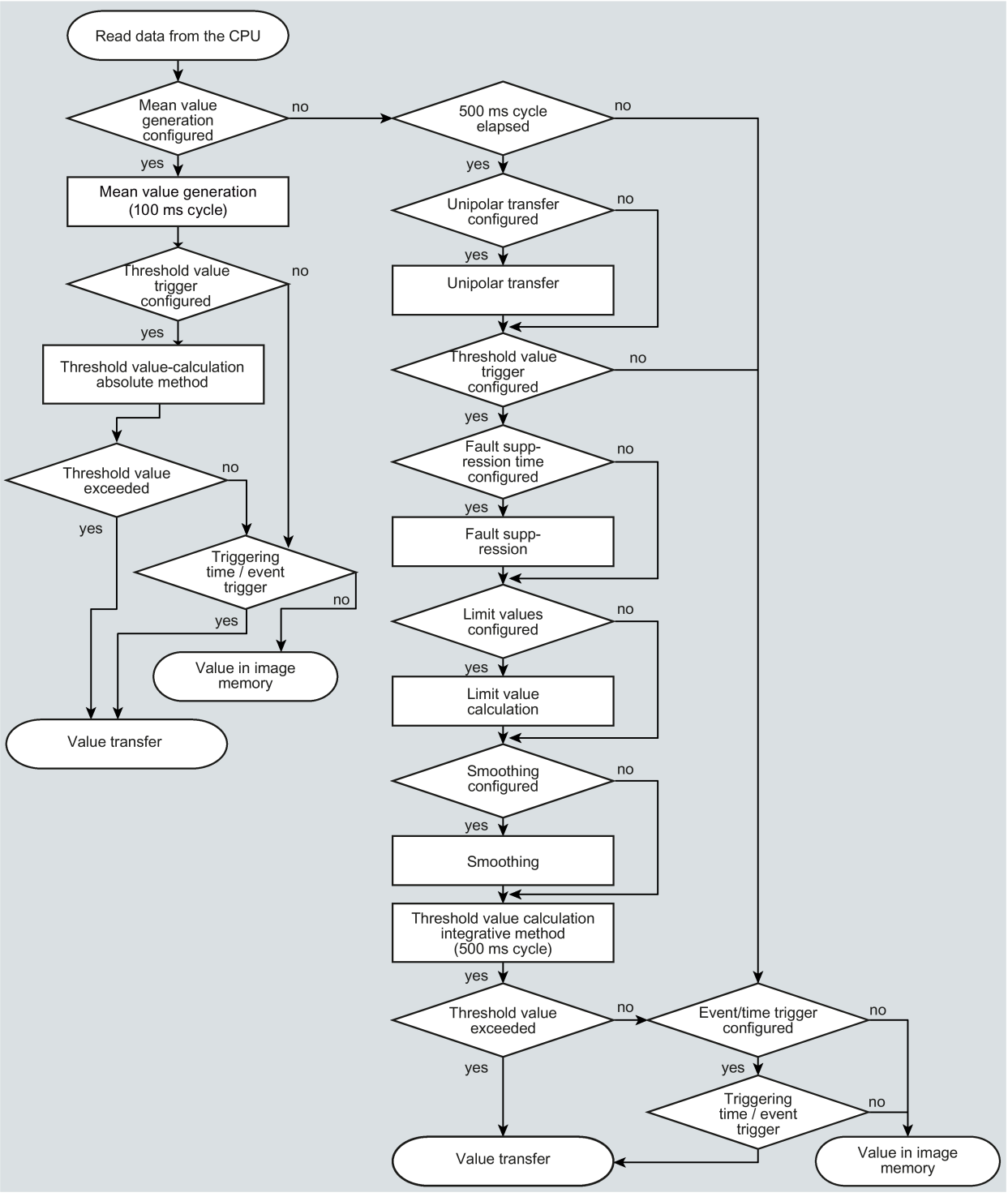


Figure 2-5 Sequence of the analog value preprocessing

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

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

Mean value generation

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

For the following protocols, averaging is only supported for integers of type "Int":

- TeleControl Basic
- DNP3
- IEC 60870-5

Note

Restricted preprocessing options if mean value generation is configured

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

- Unipolar transfer
- Fault suppression time
- Smoothing
- Threshold value calculation only with the absolute method

Function

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

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

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

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

Input modules: Overflow range / underflow range

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

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

Note

Fault suppression time > 0 configured

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

Unipolar transfer

Restrictions

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

Function

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

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

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

Fault suppression time

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

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

Function

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

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

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

Input modules

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

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

Recommendation for finished values that were preprocessed by the CPU:

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

For finished values preprocess in the CPU, the limits for the overflow and underflow can be freely assigned.

Smoothing factor

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

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

Function

Analog values that fluctuate quickly can be evened out using the smoothing function.

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

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

where
y_n = smoothed value in the current cycle n
y_{n-1} = smoothed value in the previous cycle n-1
x_n = acquired value in the current cycle n
k = smoothing factor

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

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

Set limit value 'low' / Set limit value 'high'

Requirements for the function

- Configuration of the threshold trigger for this data point
- Supported variable types of the CPU

  The analog value data point must alternatively be linked to one of the following tags:

  – PLC tag in the bit memory address area

  – DB tag (tag in data block)

  Limit value configuration is not possible for PLC tags that access hardware modules (input/output operand area).

The configuration of limit values is pointless for measured values that have already been preprocessed on the CPU.

Function

In these two input boxes, you can set a limit value in the direction of the start of the measuring range or in the direction of the end of the measuring range. You can also evaluate the limit values, for example as the start or end of the measuring range.

Status identifier "OVER_RANGE" / "overflow"

With protocols that support status identifiers, if the limit value is overshot or undershot, the status identifier of the data point is set for measured range violation known below as the identifier "OV". This status identifiers are described in the section Status IDs of data points (Page 95).

The "OV" bit of the status identifier of the data point is set as follows when the relevant analog value is transferred:

- Limit value 'high':
  – If the limit value is exceeded: OV = 1
  – If the value then falls below the limit value: OV = 0
- Limit value 'low':
  – If the value falls below the limit value: OV = 1
  – If the value then exceeds the limit value: OV = 0

Configuration of the limit value

Depending on the data type, a limit value is configured as an integer decimal number or as a floating-point number.

Table 2- 4 Value ranges of the limit values

Data type	Value range
Int	-32768 ... 32767
DInt	-2147483648 ... 2147483647
Real	1.175495E-38 ... 3.402823E+38
LReal	2.225073E-308 ... 1.797693E+308

The entry of the value 0 (zero) is interpreted as a deactivated limit value.

The following table specifies the ranges of a number with regard to the range of the raw value of an analog input or output module.

Range	Raw value (16 bits) of the PLC tag		Module output [mA]			Measuring range [%]
	Decimal	Hexadecimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
Overflow	32767	7FFF	> 23.515	> 23.515	> 22.810	> 117.593
Overrange	32511 ... 27649	7EFF ... 6C01	23.515 ... 20.001	23.515 ... 20.001	22.810 ... 20.001	117.593 ... 100.004
Nominal range (unipolar / life zero)	27648 ... 0	6C00 ... 0000	20 ... 0		20 ... 4	100 ... 0
Nominal range (bipolar)	27648 ... 0 ... -27648	6C00 ... 0000 ... 9400		20 ... 0 ... -20		100 ... 0 ... -100
Underrange (unipolar / life zero)	-1 ... -4864	FFFF ... ED00	-0.001 ... -3.518		3.999 ... 1.185	-0.004 ... -17.59
Underrange (bipolar)	-27649 ... -32512	93FF ... 8100		-20.001 ... -23.516		-100.004 ... -117.593
Undershoot / wire break	-32768	8000	< -3.518		< 1.185	< -17.593

Recommendation for quickly fluctuating analog values:

If the analog value fluctuates quickly, it may be useful to smooth the analog value first if limit values are configured.

2.11.12 "Partner stations" tab

Telecontrol server enabled / Partners for inter-station communication

Here, you specify the communication partner of the data point.

- Telecontrol server enabled

  If no CP was enabled as the partner for inter-station communication, the "Telecontrol server enabled" option is selected automatically. In this case, the telecontrol server is the communications partner of the data point.

- Partner for inter-station communication

  If instead a CP of an S7 station should be the communication partner of the data point, select this option. The option "Telecontrol server enabled" is disabled in this case.

The telecontrol server and a CP in an S7 station cannot be selected as the partner at the same time. If the data of a data point is to be sent to the telecontrol server and an S7 station, you must create the data point twice and configure each of them with a different partner.

Partner number (inter-station communication)

Specify the partner CP for inter-station communication for the selected data point by selecting the required partner from the drop-down list. The access ID of the relevant partner is shown in brackets.

The partners you specified in the "Partner stations" > "Partner for inter-station communication" can be selected.

Data point index

Index of the corresponding data point on the communications partner.

Note:

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

2.12 Messages

Configuration of the messages

If important events occur, the CP can send messages. The following are configurable:

- E-mails

  The recipient can be a PC with an Internet connection or an S7 station.

- SMS (only mobile wireless CPs)

  The recipient can be a mobile phone or an S7 station.

You configure the messages with the message editor of the CP. Alternatively, you will find it:

- Via the shortcut menu of the CP
- Via the project navigation: Directory of the station > Local modules > CP

For information on the network editor, refer to the section Data point configuration (Page 86).

You will find the characters permitted for message texts and additional parameters in the section Character set for passwords and messages (Page 116).

Requirements and necessary information

To transfer messages, telecontrol communication (parameter group "Communication types") no longer needs to be enabled. With the CP you can send messages without using telecontrol communication.

You obtain the access data for the mobile wireless network and for an APN for transferring e-mails from your network provider. You configure this in the parameter group "Mobile wireless communication settings" see section Mobile wireless communications settings (Page 49).

You will find other required information for SMS messages and e-mails that you receive from your service provider in the following sections.

Configuring e-mails

Required information:

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

You create the configuration in the following parameter groups.

- Enabling security functions

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

- Configuration of the service / protocol:

  "E-mail configuration", see section E-mail configuration (Page 73).

- When using STARTTLS or SSL/TLS:
  - Import of the certificate of the e-mail service provider:

    "Global security settings"
  - Using the imported certificate for the CP:

    Parameter group "Security" > "Certificate manager"

Configuring SMS messages (mobile wireless CPs)

Required information:

- Number of the SMSC

You create the configuration in the following parameter groups.

- Enabling the SMS function

  "Communication types" > "Enable SMS"

- Configuration of the SMSC

  "Mobile wireless communication settings" see above.

- Configuring the SMS

  Message editor, see above.

"Message parameter"

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

"Trigger"

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

- **E-mail trigger / SMS trigger**

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

  – **Use PLC tag**

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

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

    Note

    Fast setting of the diagnostics trigger tag

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

  – **CPU changes to STOP**

  – **CPU changes to RUN**

  – **Connection to a partner interrupted**

    Triggers the sending of the message when the telecontrol connection to a partner is interrupted.

  – **Connection to a partner established**

    Triggers the sending of the message when the connection returns.

  – **Connection establishment to partner failed**

    Triggers the sending of the message when the telecontrol connection to a partner could not be established.

  – **Teleservice session started**

    (Mobile wireless CPs)

    Triggers the sending of the message when telecontrol communication is enabled and a TeleService connection is established.

  – **Teleservice session ended**

    (Mobile wireless CPs)

    Triggers the sending of the message when telecontrol communication is enabled and a TeleService connection has been terminated.

- **Weak mobile wireless network**

  (SMS only)

  If the mobile wireless connection for telecontrol communication is too weak, an SMS message is triggered and sent to the configured recipient.

- **VPN connection established**

  (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

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

- **VPN connection terminated**

  (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

  Triggers the sending of the message when the VPN connection is interrupted.

- **SINEMA RC connection established**

  (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

  Triggers the sending of the message when the VPN or OpenVPN connection is established or returns.

- **SINEMA RC connection terminated**

  (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)

  Triggers the sending of the message when the VPN or OpenVPN connection is interrupted.

- **PLC tag for trigger**

  PLC tag for the trigger "Use PLC tag"

- **Enable identifier for processing status**

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

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

  For the significance of the status output in hexadecimal, refer to the section Processing status of messages (Page 141).

- **PLC tag for processing status**

  PLC tag of the type DWORD for the processing status

- **Include value**

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

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

  $$ as placeholder for the values of data points supports the following data types:
  Bool, Byte, Char, Int, UInt, Word, DWord, UDInt, DInt, Real, String,
  arrays of the specified data types

- **PLC tag for value**

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

2.13 Character set for passwords and messages

Character set for APNs, e-mail servers, message texts and the Telecontrol password

The following permitted characters apply to:

- APN:

  User names and passwords

- SMTP server:

  User names and passwords

- Messages in the message editor:

  Message texts

- CP identification

  Telecontrol password

Entered as ASCII character sets (hexadecimal value and character name):

- 0x20

  Space

- 0x21 ... 0x5F

  ! " # $ % & ' ( ) * + , - . / 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 [\ ] ^ _

- 0x61 ... 0x7E

  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 { | } ~

- 0x7C, 0x7E

  | ~

Commissioning 3

3.1 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".

3.2 Set time for operation with Security / SINEMA RC

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.

Diagnostics and maintenance

4

4.1 Diagnostics options

The following diagnostics options are available:

LEDs of the modules

For information on the LED displays, refer to the section LED displays of the CPs (Page 124).

STEP 7: The "Diagnostics > Device information" tab in the Inspector window

With an online connection to the station, you can obtain information about the online status of the selected station:

- Device information
- Connection information
- Display of messages

STEP 7: "Online > Online and diagnostics" menu

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

If you want to operate online diagnostics via the CP, you need to activate the online functions in the "Communication types" parameter group of the CP.

"Diagnostics" group

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

- **General information on the module**

  General information on the module
- **Diagnostics status**

  Information on the diagnostics status
- **Ethernet interface**

  Address and statistical information

- **Industrial Remote Communication**

  Here, you obtain specific information on the WAN interface and other parameters of the CP. The entry job has the following subentries:

  – Partner

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

  – Mobile wireless interface

    For mobile wireless CPs: Diagnostics information on the network, statistical connection information, information on received/sent messages

  – Data point list

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

  – Protocol diagnostics

    With the function "Enable protocol trace" the frames received and sent by the module are copied for several seconds.

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

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

  – Device-specific events

    Information on CP-internal events

- **Time**

  Information on the time on the device

- **Security**

  Only CPs with security functions

  The group has the following diagnostics pages:

  – Status

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

  – System log

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

  – Audit log

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

  – Communication status

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

  – SINEMA RC - automatic VPN configuration

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

"Functions" group

- Saving service data

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

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

Partner status

The CP can signal the status of the connection to the communication partner to the CPU via a PLC tag. You can display the status of the PLC tag via the Web server of the CPU.

For information on the configuration, refer to the section Communication with the CPU (Page 64).

CP monitoring / CP diagnostics

The telecontrol CP can store the status of the connection to the CPU (watchdog bit) and extended diagnostic data in PLC tags. You can display the states of the PLC tags via the Web server of the CPU.

For information on the configuration, refer to the section Communication with the CPU (Page 64).

Web server of the CPU

You will find details on the diagnostics options of the Web server in the system manual of the respective SIMATIC family, see Bibliography (Page 173).

SNMP

For information on the functions, refer to the section Diagnostics via SNMP (Ethernet CPs) (Page 139).

TeleService

From the engineering station you can connect to the remote station via mobile wireless using TeleService and view the diagnostics data of the mobile wireless CP. For information on establishing a TeleService connection, see below.

For the diagnostics contents see below ("Online > Online and diagnostics").

Diagnostics SMS message from mobile wireless CPs

The CP sends a diagnostics SMS message to a telephone with an authorized call number if it receives an SMS message with the following text from this telephone:

```
CPDIAG
```

The diagnostics SMS message that is then sent contains the following data of the S7 station:

- Firmware version of the CP
- Mode of the CPU (RUN / STOP)
- Status of the mobile wireless network connection

  Range of values and meaning:

  – 0 = Booked out of the network
  – 1 = Wrong PIN
  – 2 = Wrong SIM card
  – 3 = Waiting for PIN / no PIN configured
  – 4 = Booked into the network
- Date and time of the last dial-in to the mobile wireless network

  The data is specified in the ISO 8601 format ("Attach: YYYY-MM-DD hh:mm:ss").

  If the time-of-day of the CP has not been synchronized at the time of the dial-in, the default date of the CP (01.01.2000) is transferred as the trime.

  If the last attempted dial-in to the mobile wireless network was not successful, "Attach: -" is sent.
- Name of the current mobile wireless network
- IP address of the CP

- Signal strength of the mobile wireless network
  - good: Good signal quality (-73 ... -51 dBm)
  - medium: Medium signal quality (-89 ... -74 dBm)
  - weak: Bad signal quality (-109 ... -90 dBm)
  - no signal: Signal too weak to be received (≤ -110 dBm)
- Received Signal Strength Indication (RSSI)- Received field strength at the station [0 ... 31]
- Status of the connection to the telecontrol server

If the data to be sent exceeds the default size of an SMS message, several SMS messages are sent.

Diagnostics options of the telecontrol server

For telecontrol communication, TCSB provides several diagnostics options that you should use if problems occur during productive operation.

If there are connection problems between the station and telecontrol server, you can check the connection step-by-step using the following system tags:

- ConnectionState
- PLCConnected
- PLCCpuState

Failed mobile wireless transmission

If mobile wireless transmission is not working but all other settings and connections are correct, check the external power supply of the CP.

4.2 LED displays of the CPs

4.2.1 CP 1242-7 GPRS V2

LEDs of the module

The CP has the following LEDs for displaying the status:

- "DIAG" LED on the front panel

  The "DIAG" LED that is always visible shows the basic statuses of the module.
- LEDs below the upper cover of the housing

  These LEDs provide further details on the module status.

Table 4- 1 LED on the front panel

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

Table 4- 2 LEDs below the upper cover of the housing

LED / colors	Name	Meaning
red/green	NETWORK	Status of the connection to the mobile wireless network
green	CONNECT	Status of the connection to the master station
yellow / green	SIGNAL QUALITY	Signal quality of the mobile wireless network
green	TELESERVICE	Status of the TeleService connection

Note

LED colors when the module starts up

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

Display of the operating and communication status

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

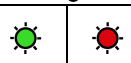
Table 4- 3 Meaning of the LED symbols

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

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

DIAG (red / green)	**NETWORK** (red / green)	**CONNECT** (green)	**SIGNAL QUALITY** (yellow / green)	**TELE-SERVICE** (green)	**Meaning**
Display of the basic statuses of the module					
○	○	○	○	○	Power OFF
● red	●	●	●	●	Startup
☼ flashing red	-	○	-	-	Errors: • Invalid CP configuration or • CP type does not match the configuration data on the CPU.
● green	-	-	-	-	Running (RUN) without error
☼ flashing red	-	☼	-	-	Backplane bus error
☼ flashing red	●	-	-	-	Missing SIM card
☼ flashing red	☼	-	-	-	Missing or incorrect PIN
Connection to the mobile wireless network					
-	●	-	-	-	Connection exists to the GPRS service in the GSM network
-	○	-	-	-	No connection to the GPRS service in the GSM network

DIAG (red / green)	NETWORK (red / green)	CONNECT (green)	SIGNAL QUALITY (yellow / green)	TELE-SERVICE (green)	Meaning
Connection to communications partners					
green	green	green	-	-	Connection established to at least one partner, CPU in RUN
green	green	flashing green	-	-	Connection established to at least one partner, CPU in STOP
flashing green	green	green	-	-	No partner reachable, CPU in RUN
flashing green	green	flashing green	-	-	No partner reachable, CPU in STOP
flashing green	○	green	-	-	Telecontrol configuration exists, partner not reachable, CPU in RUN mode
flashing green	○	flashing green	-	-	Telecontrol configuration exists, partner not reachable, CPU in STOP mode
TeleServiceconnection					
-	green	-	-	green	TeleService connection established
-	-	-	-	○	No TeleService connection established
Quality of the mobile wireless connection					
-	-	-	green	-	Good network (-73 ... ≥ -51 dBm)
-	-	-	yellow	-	Medium strength network (-89 ... -74 dBm)
-	-	-	flashing yellow	-	Weak network (-109 ... -90 dBm)
-	-	-	○	-	No network (≤ -110 dBm)
flashing red	-	-	○	-	Missing external power supply

DIAG (red / green)	NETWORK (red / green)	CONNECT (green)	SIGNAL QUALITY (yellow / green)	TELE-SERVICE (green)	Meaning
Loading firmware					
					Loading firmware. The "DIAG" LED flashes alternating red and green.
 flashing green					Firmware was successfully loaded.
 flashing red					• Error loading firmware or • Internal error of the CP; remedy: Power OFF → ON

4.2.2 CP 1243-7 LTE

LEDs of the module

The CP has the following LEDs for displaying the status:

- "DIAG" LED on the front panel

  The "DIAG" LED that is always visible shows the basic statuses of the module.
- LEDs below the upper cover of the housing

  These LEDs provide further details on the module status.

Table 4- 4 LED on the front panel

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

Table 4- 5 LEDs below the upper cover of the housing

LED / colors	Name	Meaning
 red/green	NETWORK	Status of the connection to the mobile wireless network
 green	CONNECT	Status of the connection to the master station
 yellow / green	SIGNAL QUALITY	Signal quality of the mobile wireless network
 green	VPN	Status of the VPN or SINEMA Remote Connect configuration

Note

LED colors when the module starts up

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

Display of the operating and communication status

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

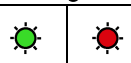
Table 4- 6 Meaning of the LED symbols

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

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

DIAG (red / green)	**NETWORK** (red / green)	**CONNECT** (green)	**SIGNAL QUALITY** (yellow / green)	**VPN** (green)	**Meaning**
Display of the basic statuses of the module					
○	○	○	○	○	Power OFF
● red	●	●	●	●	Startup
☼ flashing red	-	○	-	-	Errors: • Invalid CP configuration or • CP type does not match the configuration data on the CPU.
● green	-	-	-	-	Running (RUN) without error
☼ flashing red	-	☼	-	-	Backplane bus error
☼ flashing red	●	-	-	-	Missing SIM card
☼ flashing red	☼	-	-	-	Missing or incorrect PIN
Connection to the mobile wireless network					
-	●	-	-	-	Existing connection to the service in the mobile wireless network
-	○	-	-	-	No connection to the service in the mobile wireless network

DIAG (red / green)	**NETWORK** (red / green)	**CONNECT** (green)	**SIGNAL QUALITY** (yellow / green)	**VPN** (green)	**Meaning**
Connection to communications partners					
green	green	green	-	-	Connection established to at least one partner, CPU in RUN
green	green	flashing green	-	-	Connection established to at least one partner, CPU in STOP
flashing green	green	green	-	-	No partner reachable, CPU in RUN
flashing green	green	flashing green	-	-	No partner reachable, CPU in STOP
flashing green	○	green	-	-	Telecontrol configuration exists, partner not reachable, CPU in RUN mode
flashing green	○	flashing green	-	-	Telecontrol configuration exists, partner not reachable, CPU in STOP mode
Quality of the mobile wireless connection					
-	-	-	green	-	Good network (-73 ... ≥ -51 dBm)
-	-	-	yellow	-	Medium strength network (-89 ... -74 dBm)
-	-	-	flashing yellow	-	Weak network (-109 ... -90 dBm)
-	-	-	○	-	No network (≤ -110 dBm)
flashing red	-	-	○	-	Missing external power supply
VPN/SINEMA Remote Connect connection					
-	green	-	-	green	VPN/SINEMA Remote Connect connection established
-	green	-	-	flashing green	Attempting to establish a configured VPN/SINEMA Remote Connect connection
-	-	-	-	○	VPN/SINEMA Remote Connect connection not configured or currently not established on the CP

DIAG (red / green)	NETWORK (red / green)	CONNECT (green)	SIGNAL QUALITY (yellow / green)	VPN (green)	Meaning
Loading firmware					
					Loading firmware. The "DIAG" LED flashes alternating red and green.
 flashing green					Firmware was successfully loaded.
 flashing red					• Error loading firmware or • Internal error of the CP; remedy: Power OFF → ON

4.2.3 CP 1243-1

LEDs of the module

The module has various LEDs for displaying the status:

- **LED on the front panel**

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

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

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

Table 4- 7 LED on the front panel

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

Table 4- 8 LEDs below the upper cover of the housing

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

LED colors and illustration of the LED statuses

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

Table 4- 9 Meaning of the LED symbols

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

Note

LED colors when the module starts up

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

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

Table 4- 10 Display of the basic statuses of the CP

DIAG (red / green)	**Meaning** **(if more than one point listed: alternative meaning)**
Basic statuses of the CP	
○	• Power OFF • Incorrect startup
 green	Running (RUN) without serious error
 flashing green	• Partner not connected • Firmware loaded successfully
 flashing red	• Starting up • Module fault • Invalid STEP 7 project data
 flashing red-green	Error loading firmware

Display of the operating and communications statuses

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

Table 4- 11 Display of the operating and communications statuses

DIAG (red / green)	-	LINK (green)	CONNECT (green)	VPN (green)	SERVICE (green)	Meaning (if more than one point listed: alternative meaning)
Module startup (STOP → RUN) or error statuses						
○		○	○	○	○	Power OFF
● red		●	●	●	●	Startup - phase 1
☼ flashing red		-	○	○	○	Startup - phase 2
● green		-	-	-	-	Running (RUN) without serious error
○			●	●	●	Incorrect startup
● red		-	☼	-	-	Invalid STEP 7 project data
☼ flashing red		-	○	-	-	Missing STEP 7 project data
☼ flashing red		●	☼	-	-	Backplane bus error
Connection to Industrial Ethernet						
-		●	-	-	-	Connection to Industrial Ethernet exists
● green		☼	-	-	-	• Connection to Industrial Ethernet being established. • IP address being obtained.
-		○	-	-	-	No connection to Industrial Ethernet

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

4.2.4 CP 1542SP 1 IRC

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 4- 12 Legend for the following tables

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

Table 4- 13 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 4- 14 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.

4.3 Web server S7-1200: Connection establishment

Establishing a connection to the Web server of the CPU

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

Requirements in the CPU configuration

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

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

- **Connection establishment with HTTP**

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

- **Connection establishment with HTTPS**

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

These two variants are described in the following sections.

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

Connection establishment with HTTP

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

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

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

   The certificate is loaded on your PC.

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

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

Connection establishment with HTTPS

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

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

   Use the user data configured in the user administration of the Web server of the CPU.
5. After logging in, select the entry "Module status" in the navigation panel of the Web server.
6. Select the CP in the module list.

   The CP-specific content is displayed.

4.4 Online security diagnostics via port 8448

Security diagnostics via port 8448

Requirements:

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

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

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

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

4.5 Diagnostics via SNMP (Ethernet CPs)

SNMP (Simple Network Management Protocol)

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

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

Range of performance of the CP as an SNMP agent

The CP supports data queries in the following SNMP versions:

- SNMPv1 (standard)
- SNMPv3 (security)

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

- **MIB II**

  The CP supports the following groups of MIB objects:

  – System
  – Interfaces

    The "Interfaces" MIB object provides status information about the CP interfaces.
  – IP
  – ICMP
  – TCP
  – UDP
  – SNMP

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

  – Adress Translation (AT)
  – EGP
  – Transmission

- **LLDP MIB**

Traps are not supported by the CP.

For more detailed information about the MIB files and SNMP, refer to the manual /11/ (Page 175).

Configuration

For information on the configuration, refer to:

- With security functions disabled (SNMPv1): SNMP (Ethernet CPs) (Page 82)
- With security functions enabled (SNMPv1 / SNMPv3): SNMP (Ethernet CPs) (Page 82)

4.6 Processing status of messages

Processing status

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

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

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

The returned statuses of the Messages configured in the message editor have the following meaning:

Table 4- 15 SMS: Meaning of the status ID output in hexadecimal format

Status	Meaning
0000	Transfer completed free of errors
0001	Error in the transfer, possible causes: • SIM card invalid • No network • Wrong destination phone number (number not reachable)

Table 4- 16 E-mails: 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 status 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.

Status	Meaning
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 status 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: Message configuration > Message parameters: • Recipient address ("To" or "Cc").
8502	Syntax error. Check the following configuration data: Message configuration > Message parameters: • Email address (sender)
8535	SMTP authentication incomplete. Check the "User name" and "Password" parameters in the CP configuration.
8550	SMTP server cannot be reached. You have no access rights. Check the following configuration data: • CP configuration > E-mail configuration: – User name – Password – Email address (sender) • Message configuration > Message parameters: – Recipient address ("To" or "Cc").
8554	Transfer failed
85xx	Other error message from the e-mail server Apart from the leading "8", the status corresponds to the three-digit error number of the SMTP protocol.

4.7 Module replacement

4.7.1 Replacement of a CP 1200

Module replacement

CAUTION

Read the system manual "S7-1200 Programmable Controller"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller" (refer to the documentation in the Appendix).

When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".

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

The STEP -7 project data of the CP is stored on the local CPU. If there is a fault on the device, this allows simple replacement of the CP without needing to download the project data to the station again.

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

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

4.7.2 Replacement of a CP 1542SP-1 IRC

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.

4.8 Loading firmware

Note
CPU STOP

Always set the CPU to STOP mode before you download a new firmware file to the CP:

4.8.1 Loading firmware - CP 1200

New firmware versions of the CP

If a new firmware version is available for the module, you will find this on the Internet pages of Siemens Industry Online Support under the following address:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/21764/man)

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

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

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

  You will find a description of the procedure for loading on the memory card of the CPU on the Internet page of the Siemens Industry Online Support.
- Loading the firmware with the online functions of STEP 7 via a WAN

Note
Effects on the retentive memory of the CPU

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

You can recognize that firmware is being loaded by the flashing LEDs of the CP, see LED displays of the CPs (Page 124).

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

Requirements:

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

Procedure:

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

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

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

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

4.8.2 Loading firmware - CP 1542SP-1 IRC

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.

See also

Web server of the ET 200SP (Page 154)

4.9 TeleService (Mobile wireless CPs)

4.9.1 Requirements for TeleService

Note

Terminating a TeleService connection in case of high user data load

User data have a higher priority than the data of an online connection.

If the mobile wireless CP permanently transmits a high volume of data, the data flow is slowed down by a simultaneous TeleService connection and the duration of the TeleService session is increased significantly. When you transfer large amounts of data over the TeleService connection, the connection may be terminated.

If you want to transfer the configuration data over the TeleService connection, it may be useful to set the CPU to STOP before you start the transfer and to restart it after the transfer.

Requirement for the engineering station and the STEP 7 project

- The STEP 7 project with the CP is stored on the engineering station.
- The required configuration steps have been performed, see section Configuration of the TeleService access (Page 148).

Requirement for TeleService via a telecontrol connection: TeleService server

For TeleService via telecontrol, a TeleService server is required as the intermediary between S7 station and engineering station.

Since a firewall is normally closed for connection requests from the outside, a switching station between the remote station and the engineering station is required. The switching station forwards the messages through the firewall. This allows access by the engineering station with Internet access to the S7-1200 via a router and via the APN of the network provider.

This intermediary can be either:

- Telecontrol server

  If you use a telecontrol server, the intermediary can be the telecontrol server.

- TeleService gateway

  If there is no telecontrol server in your system, a TeleService gateway must exist as the intermediary.

  For information on the required "TS Gateway" software, see Software requirements (Page 28).

  For the documentation of the "TS Gateway" software, see /12/ (Page 176).

4.9.2 Configuration of the TeleService access

Configuration for using TeleService

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

"Communication types" parameter group of the CP

Select the following options:

- Enable telecontrol communication
- Activate online functions

TeleService server in "Mobile wireless communication settings" of the CP

You configure the following information in the "Mobile wireless communications settings > TeleService settings" parameter group of the CP:

- TeleService server

  IP address or name of the telecontrol server that can be resolved by DNS or of the TeleService gateway

- Server port

  Port number of the telecontrol server or the TeleService gateway

Security > firewall

When the firewall is enabled, select the "Allow S7 protocol" option in "Predefined IP rules".

Global security settings > Users and roles

1. Open the following page in the project tree:

   Global security settings > Users and roles

   The two "User" tables and below it the table for assignment of the user groups, roles and rights will become visible.

   If necessary, enlarge the second table if it is hidden by the "User" table.

2. If a corresponding user has not be created yet, create a user in the "User" table (above).

   You need the user when establishing a TeleService session.

   Configure the following parameters:

   – User name

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

     Note:
     The user name that TeleService is to use must not exceed 20 characters.

   – Password

     Assign the password.

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

     Note:
     The user password that TeleService is to use must not exceed 30 characters.

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

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

   – Authentication method

     Select the authentication method "Password" for this user.

– Maximum time of the session

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

Leave the entry of the new TeleService user selected.

3. Open the "Assigned roles" tab.

   Assign the TeleService user one of the following roles:

   – NET Administrator

   or

   – NET Remote Access

4. Open the "Assigned rights" tab.

   Expand the "Runtime rights" entry.

   Expand the entry of a mobile wireless CP and check whether the TeleService user has been assigned the "Use TeleService" right.

"Authorized phone numbers" for TeleService in the local security settings of the CP

In some cases, it may be necessary to trigger connection establishment with an SMS message, see also the section Configuration of the TeleService access (Page 148).

If you need to wake the CP to establish a TeleService connection with an SMS, the CP accepts an SMS only when the phone authorizes itself with its phone number. These phone numbers are configured for the CP in STEP 7 in the "Authorized phone numbers" list in the security settings.

- A phone number entered here gives the sender the right to trigger connection establishment.
- If only an asterisk (*) is entered in the list, the CP accepts SMS messages from all senders.
- An asterisk (*) after a phone number body authorizes connection establishment for all nodes connected to the body (extension numbers).

  Example: +49123456* authorizes +49123456101, +49123456102, +49123456207 etc.

Note

No wake-up without an authorized phone number

If the "Authorized phone numbers" list is empty, the CP cannot be woken up for connection establishment.

Requirements in the security configuration of the CP

For the remote station, TeleService can only be used if the engineering station (with CP 1628 or via SCALANCE S) and the CP are configured in a common VPN group.

For TeleService, you need to enable the option "Allow S7 protocol" in the IP rules of the firewall configuration.

Remember the following when establishing TeleService connections via mobile wireless.

Note

TeleService only by a TIA Portal instance

You can operate TeleService with a certain S7 station only from a single engineering station (TIA Portal instance / STEP 7 project). TeleService using several engineering stations at the same time with a station is not possible.

TeleService with several engineering stations with different S7 stations is possible if the suitable STEP 7 project exists on every engineering station.

Note

No TeleService connection establishment using "Online" > "Go online"

If you attempt to establish a TeleService connection by selecting the CPU and then selecting the menu or shortcut menu command "Online" > "Connect online", STEP 7 will automatically attempt to connect via Ethernet. Reason: In STEP 7, the last connection path used to download the project data is stored.

Note

Termination of a TeleService connection when launching online dialogs

An existing TeleService connection is terminated when you attempt to access an additional station or a node.

When there is an existing TeleService connection, do not select any of the menu commands "Go online", "Online & Diagnostics", "Load to device", "Extended download to device" or "Accessible nodes".

Mechanisms of connection establishment

The request for establishment of a TeleService connection is triggered by the engineering station. This request is sent via the intranet or Internet to the TeleService server (telecontrol server or TeleService gateway).

The TeleService server forwards to request to the CP in the S7 station. The TeleService server sends the request by e-mail to the SMS gateway which converts the e-mail and forwards it as an SMS to the CP in the S7 station via the mobile wireless network.

The TeleService connection is actively established by the CP.

User data and TeleService

Connections between a CP and telecontrol server for transferring user data are not interrupted by a TeleService connection.

Establishing a TeleService connection

Follow the steps below to establish a TeleService connection to the remote station via the mobile wireless network from the engineering station:

1. Select the CPU of the remote station in the STEP 7 project.
2. Select the menu "Online" > "Extended go online".

   The "Connect online" dialog box opens.
3. Choose the entry "TeleService via telecontrol" in the "Type of interface" drop-down list.
4. Choose the entry "TeleService board" in the "PG/PC interface" drop-down list.
5. Click on the  icon next to the "PG/PC interface" drop-down list.

   The "Establish remote connection via telecontrol" dialog box opens.
6. Make the necessary entries in this dialog.

Information in the "Establish remote connection via telecontrol" dialog.

In this dialog, enter the data previously configured in STEP 7 under the following headings:

- **Telecontrol server / TeleService gateway...**

  Selection whether the TeleServiceTeleService switching station is located on the PC of the engineering station or in the network or can be reached via the Internet.

  – In the latter case, enter the address of the TeleService server.

    IP address or name and port number of the telecontrol server that can be resolved by DNS or of the TeleService gateway

  – Own server password

    If the option is enabled and the server password is configured in TCSB, enter the password to authenticate the CP with the telecontrol server.

    The server password is not required for TeleService via a TeleService gateway.
- **Authentication ...**

  – User name and password

  – Here, enter the data for the TeleService user that you configured in STEP 7 in the global security settings, see also section Configuration of the TeleService access (Page 148).

You will also find information on the necessary entries in the tooltips of the STEP 7 online help.

Ways to deal with connection establishment problems

If you have triggered the establishment of a TeleService connection with the engineering station and the connection is not established, among other things this may be because there is a connection disruption between the TeleService server and station or that the data of the SMS gateway configured on the TeleService server is incorrect.

In this case you can also use a wake-up SMS to make the station establish a TeleService connection. The phone number of the phone must be configured on the CP as "Authorized phone numbers".

Send an SMS to the phone number of the CP with the following text:

- Text for the wake-up SMS message for establishing a connection via the first configured TeleService server:

  ```
  TELESERVICE
  ```

  or

  ```
  TELESERVICE 1
  ```

- If a second TeleService server is configured:

  Text for the wake-up SMS message for establishing a connection via the second configured TeleService server:

  ```
  TELESERVICE 2
  ```

Sending the SMS does not replace the establishment of the TeleService connection on the engineering station.

Terminate TeleService connection

On completion of the TeleService session, terminate the TeleService connection again using the "Disconnect" button. The connection is terminated after approximately 5 minutes.

4.10 Web server of the ET 200SP

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 /8/ (Page 175) 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 work with the Web server to, for example, download a firmware file (see the following section).

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

Connection establishment with HTTPS

1. Connect the PC 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.

See also

Loading firmware - CP 1542SP-1 IRC (Page 146)

OUC program blocks

A

A.1 Validity

The functions described below are supported by the following modules:

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

A.2 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

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

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

Note

No different program block versions

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

Requirements

IPv6

IPv6 is only supported by Ethernet CPs.

Secure OUC

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

- STEP 7: As of V16
- CPU firmware
  - CPU-1200: As of V4.3
  - CPU 151xSP: As of V2.0
- CP firmware
  - CP 1200: As of V3.2

    (The CP 1242-7 does not support Secure OUC.)
  - CP 1542SP-1 IRC: As of V2.1

Supported program blocks

The following instructions of the Open User Communication are available in the specified minimum version:

- **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 module. Configure the time-of-day synchronization.

To change the configuration data of the module during runtime:

- **T_CONFIG V1.0**

  Program-controlled configuration of the CP IP parameters

  Refer to the information on T_CONFIG and on the SDTs "IF_CONF_..." in the section Changing the IP address during runtime (Page 164).

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

Note

No feedback from the CP

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

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

Connection descriptions in system data types (SDTs)

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

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

Creating an SDT for the data blocks

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

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

The corresponding SDT is then created with its parameters.

Usable SDTs

- **TCON_IP_V4**

  For transferring frames via TCP or UDP

- **TCON_QDN**

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

- **TCON_IP_RFC**

  For transferring frames via ISO-on-TCP (direct communication between two S7 stations)

- **TADDR_Param**

  For transferring frames via UDP

- **TMail_V4**

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

  Recommendation for mobile wireless applications:
  Set the parameter "WatchdogTime" from "MAIL_ADDR_PARAM" to a value higher than 3 minutes.

- **TMail_V6**

  Only Ethernet CP

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

- **TMail_FQDN**

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

- **TCON_IP_V4_SEC**

  Only CP 1200

  For the secure transfer of data via TCP

- **TCON_QDN_SEC**

  Only CP 1200

  For the secure transfer of data via the host name

- **TMail_V4_SEC**

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

- **TMail_V6_SEC**

  Only Ethernet CP

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

- **TMail_QDN_SEC**

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

Note on TMail_Vx_SEC / TMail_QDN_SEC:
With these SDTs, the mail server certificate is checked, but not the ID of the "TLSServerCertRef" (STEP 7 internal reference) certificate.

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

Connection establishment and termination

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

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

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.

A.3 SMS messages via OUC

Sending e-mails / SMS messages via OUC

You only require the program blocks and system data types (SDTs) described below to transfer SMS messages using Open User Communication (OUC).

The event-driven sending of e-mails or SMS messages using telecontrol communication, however, is independent of program blocks and is configured in STEP 7 in the message editor.

SMS messages via program blocks

Sending SMS messages to one partner

To do this, create the following blocks or system data types (alternatives):

- TCON + TDISCON + TSEND + TCON_Phone
- TSEND_C + TCON_Phone

Receiving SMS messages from one partner

To do this, create the following blocks or system data types (alternatives):

- TCON + TDISCON + TRCV + TCON_Phone
- TRCV_C + TCON_Phone

If you do not enter a phone number in the "PhoneNumber" parameter of the TCON_Phone system data type, the CP cannot receive any SMS messages.

Receiving SMS messages from several partners

As an alternative, you can create a separate block set for each partner as described above for 1 partner or a single block set with the following special feature in the TCON_PHONE block:

If you enter an asterisk (*) after the phone number body in the "PhoneNumber" parameter of the TCON_Phone block, the asterisk acts as a placeholder for all authorized phone numbers with this phone number body.

You configure the phone numbers authorized for access to the CP in STEP 7 in the "Security" parameter group of the CP.

Message text to be sent in the "DATA" parameter

You enter the message text as a string in the "DATA" parameter of TSEND or TSEND_C.

A message can contain up to 160 characters. If the message text contains more than 160 characters, the text is distributed over two or more SMS messages.

Reading out the message text from the "DATA" parameter

To receive an SMS message, parameterize the message text to be read out in the TRCV / TRCV_C blocks in the "DATA" parameter via a data block (DB).

Create a DB of the data type "Struct". Open the properties dialog of the DB (shortcut menu of the DB) and disable optimized block access in the "Attributes" parameter group.

In the structure of the DB, create the following data types for the SMS messages:

- DTL

  12 bytes for the time stamp of the received SMS message (time stamp from the network)

- String[22]

  String of 22 bytes for the phone number of the sender (+ 2 byte string header)

- String[160]

  String of 160 bytes for the message text (+ 2 byte string header)

  The SMS message text can contain max. 160 characters.

Per SMS message the structure requires memory space of 198 bytes.

Storing the last 10 received SMS messages

You can output up to 10 received SMS messages from the receive block by making the entry "SMSSTORE" for the "PhoneNumber" parameter of TCON_PHONE.

To store the received data from 10 SMS messages , you need to create an adequately large structure (2000 bytes) for the "DATA" parameter of the receiving block. As described above, the structure has the following organization:

- Received data SMS 1 (DTL, String[22], String[160], Byte)
- Received data SMS 2 (DTL, String[22], String[160], Byte)

  ... to

- Received data SMS 10 (DTL, String[22], String[160], Byte)

The received data of every SMS message gas the following structure:

- DTL

  12 bytes for the time stamp of the received SMS message (time stamp from the network)

- String[22]

  String of 22 bytes for the phone number of the sender (+ 2 byte string header)

- String[160]

  String of 160 bytes for the message text (+ 2 byte string header)

- Byte

  Status of the SMS message

  If more than one SMS message is received the status of every SMS is stored in this status byte:

  – 0 = Invalid

    1 = Unread

    2 = Read

When receiving multiple SMS messages, per SMS message the structure requires memory space of 200 bytes.

Length information at "LEN" and "DATA" for the blocks "TRCV" / "TRCV_C"

When receiving SMS messages via the blocks TRCV or "TRCV_C" if you enter length information in the "LEN" parameter, this can lead to incorrect information in the data storage of the received information.

Recommendation: Set LEN = 0 and enter the length information in the "DATA" parameter.

Character set for the SMS text

The CP supports the following ASCII character set (hexadecimal value and character name) for SMS message texts sent via program blocks:

- 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

- 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

A.4 Changing the IP address during runtime

Changing the IP address during runtime

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

- IP address
- Subnet mask
- Router address

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.

Note

Changing the IP parameters with a dynamic IP address

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

Requirements - 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.

Requirements - STEP 7 version

- STEP 7 ≥ V14

Requirements - Firmware versions

- CP 1243-1
  - CP firmware ≥ V2.1.7x
  - CPU firmware ≥ V4.2
- CP 1542SP-1 IRC
  - CP firmware ≥ V1
  - CPU firmware ≥ V2.0 (CPU 151xSP)

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).

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

- **T_CONFIG**

  Along with:

  – IF_CONF_V4

  – IF_CONF_NTP

  – IF_CONF_V6

  – IF_CONF_DNS

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

Note

No feedback from the CP

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

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

SINEMA Remote Connect

B

B.1 Validity and requirements

Validity

Communication via SINEMA Remote Connect is supported by the following modules:

- CP 1243-1
  - As of firmware V3.1
- CP 1243-7 LTE
  - As of firmware V3.1
- CP 1243-8 IRC
  - As of firmware V3.1
  - Under ST7 as MSC station as of firmware V3.2
- CP 1542SP-1 IRC
  - As of firmware V2.0
  - Under ST7 as MSC station as of firmware V2.1

The functions are supported by the following software versions:

- SINEMA Remote Connect
  - As of software version V1.3

B.2 Setting the time of day during commissioning

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 Set time for operation with Security / SINEMA RC (Page 117).

B.3 Connection to SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

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

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

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

The CP can also handle telecontrol communication via the SINEMA RC server.

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 supported protocols and configuration, see section Telecontrol via SINEMA RC (Page 169).

Applications

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

- (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 B- 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"

B.4 Telecontrol via SINEMA RC

For information on possible applications of communication via SINEMA Remote Connect, see section Connection to SINEMA RC (Page 168).

Requirements

Perform the necessary configuration of SINEMA Remote Connect - Server (not in STEP 7) before configuring the CP in STEP 7. The CP and the communications partner of the CP must be configured in the SINEMA RC Server.

Configuration of the telecontrol communication via SINEMA Remote Connect

Follow the steps below when configuring the module for use of telecontrol communication via SINEMA RC:

1. In the "Communication types" parameter group activate telecontrol communication and select the protocol.

   The option for communication via SINEMA RC is not yet visible.

2. Change to the "Security" parameter group and enable the security functions.

   (In the "Communication types" parameter group the SINEMA RC option appears disabled and grayed out)

3. Open the "Security > VPN" parameter group and enable VPN.

4. For the parameter "VPN connection type" select the option "Automatic OpenVPN configuration via SINEMA Remote Connect Server" if this is not preset.

   (In the "Communication types" parameter group the SINEMA RC option becomes usable.)

5. Change to the "Communication types" parameter group and enable the option "Telecontrol communication via SINEMA Remote Connect".
6. Create the remaining configuration of the SINEMA RC connection of the CP under "Security > VPN".

   For information on the configuration, see section Security > VPN > SINEMA Remote Connect (Page 170).

B.5 Security > VPN > SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect Server

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

- Exporting the CA certificate (optional)

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

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

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

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

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

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

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- CA Certificate

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

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

- Fingerprint

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

Authentication

- Device ID

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

- Device password

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

  Max. number of characters: 127

Optional settings

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

- **Update interval**

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

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

- **"Connection type"**

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

  – Auto

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

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

  – PLC trigger

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

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

Note

Connection abort

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

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

- **PLC tag for connection establishment**

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

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

Bibliography

C

Where to find Siemens documentation

- Article numbers

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

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

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

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

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

- Manuals on the Internet

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

  Link: (https://support.industry.siemens.com/cs/ww/es/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 NET - TeleControl
Siemens AG
Configuration manuals of the protocols:
- TeleControl Basic
- SINAUT ST7
- DNP3
- IEC 60870-5
Link: (https://support.industry.siemens.com/cs/ww/en/ps/21764/man)

/2/

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

/3/

SIMATIC NET
CP 1242-7 GPRS V2
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15921/man)

/4/

SIMATIC NET
CP 1243-7 LTE
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15924/man)

/5/

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

/6/

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)

/7/

SIMATIC
S7-1200 Automation System
system manual
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/ps/13683/man)

/8/

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

/9/

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

/10/

SIMATIC NET
Industrial Ethernet / PROFINET
System manual
Siemens AG

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

/11/

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

/12/

SIMATIC NET
TS Gateway (Version V3)
Operating Instructions
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/en/view/107535103)

Index

S

T

U

V

W