

SIMATIC NET

S7-1200 - TeleControl SIMATIC CP 1243-8 IRC

Operating Instructions

Preface

Application and functions	1
LEDs and connectors	2
Installation, wiring, commissioning, removal	3
Configuration	4
Program blocks	5
Diagnostics and upkeep	6
Technical data	7
Approvals	A
Dimension drawings	B
Accessories	C
Encryption methods (Ciphers)	D
Documentation references	E

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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

 WARNING
Siemens products may only be used for the application described in the catalog and the associated usage information. 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 Aktiengesellschaft. 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.

Preface

Validity of this manual

This document contains information on the following product:

- **CP 1243-8 IRC**

Article number 6GK7 243-8RX30-0XE0

Hardware version 3

Firmware version V3.6

The CP is the communications processor for connection of the SIMATIC S7-1200 via public or private infrastructures to a telecontrol master station. For the supported telecontrol protocols, see section Properties of the CP (Page 13).

With the help of VPN technology and the firewall, the CP allows protected access to the S7-1200.

The CP can also be used as an additional Ethernet interface of the CPU for S7 communication.



Figure 1 CP 1243-8 IRC

Behind the top hinged cover of the module housing, you will see the hardware product version to the right of the article number printed as a placeholder "X". If the printed text is, for example, "X 2 3 4", "X" would be the placeholder for hardware product version 1.

You will find the MAC address under the lower hinged cover of the housing.

Purpose of the manual

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

You will also find instructions for operation and information about the diagnostics options of the device.

Configuration

The necessary configuration steps are described in the form of an overview.

- **CP without telecontrol communication**
The relevant configuration steps for these applications are described in this manual.
- **CP with telecontrol communication**
You will find the complete description of the configuration and diagnostics for these applications in the respective configuration manual /4/ TeleControl configuration manuals (Page 174).

Refer to the information below in the section "Structure of the documentation".

Product names and abbreviations

The following short forms are used in this document:

- **CP**
The short form is used instead of the full product name "CP 1243-8 IRC".
- **IRC**
Industrial Remote Communication
- **STEP 7**
Short form for the following versions of the configuration tool STEP 7:
 - STEP 7 V5
 - STEP 7 Basic

The short form "STEP 7" is only used when the product is self-explanatory in the particular context.
For information on the product versions, refer to the section Requirements for operation (Page 25).
- **Proxy**
"PROXY CP1243-8 IRC", substitute module for the CP 1243-8 IRC in the catalog of STEP 7 V5 / HW Config.
- **ST7**
Short form for the telecontrol protocol "SINAUT ST7"

New in this edition

- New firmware version V3.6 with functional improvements

Restriction:

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

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

Replaced manual edition

Edition 05/2024

Current manual edition on the Internet

You can also find the current edition of the manual on the Internet at:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21162/man>)

With the "E-mail on update" option, you can enable an automatic notification when new documents are published in SiePortal for the products you selected in the product tree.

Structure of the documentation

The documentation of the CP consists of the following manuals and content:

- **Operating instructions**
 - Application and functions (without telecontrol)
 - 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
- **SINAUT ST7 system manual**
 - **Volume 3 - Configuration in STEP 7 Professional (TIA Portal)**

Valid for all ST7-capable communications modules
- **Configuration manual DNP3**
 - Configuration and diagnostics in STEP 7 Professional (TIA Portal)

Valid for all SIMATIC NET communications modules that support the DNP3 protocol.
- **Configuration manual IEC 60870-5**
 - Configuration and diagnostics in STEP 7 Professional (TIA Portal)

Valid for all SIMATIC NET communications modules that support the protocol IEC 60870-5-101/104.

You can find the Internet links for the manuals in the appendix Documentation references (Page 173).

Required experience

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

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

Requirements for use of the module

You will find the requirements for using the module in the section Requirements for operation (Page 25).

Cross-references

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

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

Product discontinuation

Note

Discontinuation of modules (product discontinuation)

Note the following products to be discontinued in October 2023.

- TS MODULE MODEM (6ES7972-0MM00-0XA0)
- TS MODULE RS232 (6ES7972-0MS00-0XA0)

For more information, see the product notifications about this on the Internet:

Link: (<https://support.industry.siemens.com/cs/us/en/pv/6ES7972-0MM00-0XA0/pi?dl=de>)

Link: (<https://support.industry.siemens.com/cs/us/en/pv/6ES7972-0MS00-0XA0/pi?dl=de>)

License conditions

Note

Open source software

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

You will find the license conditions on the supplied data medium:

- OSS_CP1243x_99.pdf

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit
<https://www.siemens.com/cybersecurity-industry>.

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 customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
<https://new.siemens.com/cert>.

See also:
Security functions (Page 21)
Security recommendations (Page 49)

Firmware

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

Note on firmware/software support

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

Device defective

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

Decommissioning

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

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

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

Recycling and disposal



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

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

Keep to the local regulations.

You will find information on returning the product on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/109479891>)

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

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

Training, Service & Support

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

Table of contents

	Preface	3
1	Application and functions	13
1.1	Properties of the CP	13
1.2	Communications services.....	14
1.3	PUT/GET: Restrictions in the CPU.....	18
1.4	Communication via SINEMA RC	19
1.5	Other services and properties.....	20
1.6	Security functions	21
1.7	Performance data and configuration limits	23
1.8	Requirements for operation.....	25
1.9	Configuration examples - Intended operating environment.....	26
1.9.1	TeleControl	27
2	LEDs and connectors.....	29
2.1	Opening the covers of the housing.....	29
2.2	LEDs	30
2.3	Electrical connectors	35
2.3.1	Power supply	35
2.3.2	Ethernet interface X1P1	36
2.3.3	Serial connection for TS module	36
3	Installation, wiring, commissioning, removal	37
3.1	Important notes on using the device	37
3.1.1	Notices about use in hazardous areas	37
3.1.2	Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex.....	38
3.1.3	Notes on use in hazardous areas according to UL HazLoc and FM	39
3.2	Installation, removal and repairs in hazardous areas	39
3.3	Installing, connecting and commissioning.....	41
3.4	Note on operation.....	46
3.5	Disassembly.....	46
4	Configuration.....	49
4.1	Security recommendations.....	49
4.2	Configuration in STEP 7	52
4.3	Basic settings	53
4.4	Communication types	53

4.5	Time-of-day synchronization	54
4.6	Ethernet interface	60
4.6.1	Ethernet addresses.....	60
4.6.2	IPv6	60
4.6.3	CP identification	61
4.6.4	Time-of-day synchronization	61
4.6.5	Advanced options	61
4.6.6	MTU size.....	61
4.6.7	Access to the Web server.....	62
4.7	Serial interface.....	62
4.8	DNS configuration.....	62
4.9	Communication with the CPU	63
4.9.1	Communication with the CPU	63
4.9.2	CP diagnostics.....	63
4.10	SNMP	65
4.11	Security	65
4.11.1	Security user	66
4.11.2	Parameter overview	66
4.11.3	Firewall.....	67
4.11.3.1	Pre-check of messages by the MAC firewall.	67
4.11.3.2	Firewall settings for configured connection connections via a VPN tunnel	67
4.11.3.3	Settings for online security diagnostics and downloading to station with the firewall activated	67
4.11.3.4	Notation for the source IP address (advanced firewall mode)	68
4.11.4	Time-of-day synchronization	68
4.11.5	Log settings - Filtering of the system events.....	69
4.11.6	VPN	69
4.11.6.1	VPN (Virtual Private Network).....	69
4.11.6.2	Addressing the CP when using VPN	70
4.11.6.3	Creating a VPN tunnel for S7 communication between stations	70
4.11.6.4	VPN communication with SOFTNET Security Client (PC / engineering station).....	72
4.11.6.5	CP as passive subscriber of VPN connections.....	73
4.11.6.6	SYSLOG	73
4.11.6.7	SINEMA Remote Connect	73
4.11.7	SNMP	76
4.11.8	E-mail configuration.....	77
4.11.9	Certificate manager.....	78
4.11.10	Handling certificates	79
4.12	Data points	82
4.13	Messages.....	82
4.14	Character set for user names, passwords and messages	87
4.15	CloudConnect	88
4.15.1	Cloud communication.....	88
4.15.2	Configuring the cloud access.....	90
4.15.2.1	Overview of configuration.....	90
4.15.2.2	Notes on data structuring and configuration.....	90
4.15.2.3	Configuration rules	92

4.15.2.4	"CloudConnect" parameter group	94
4.15.2.5	Operand areas and tags	98
4.15.3	Configuring topics and data points	99
4.15.3.1	Configuring topics	99
4.15.3.2	Configuring the data points	100
4.15.3.3	Data types	100
4.15.3.4	Trigger	101
4.15.3.5	Payload formats	106
4.15.3.6	Import / export of payload	109
4.15.4	Properties dialog of the topics	115
4.15.4.1	Opening the properties dialog	115
4.15.4.2	Quality of Service (QoS)	116
4.15.5	Additional information	117
4.15.5.1	Connection abort and data buffering	117
4.15.5.2	JSON escape sequences	119
4.15.5.3	Permitted Characters	120
5	Program blocks	123
5.1	Program blocks for OUC	123
5.2	Changing the IP address during runtime	126
6	Diagnostics and upkeep	129
6.1	Diagnostics options	129
6.2	Web server S7-1200: Connection establishment	132
6.3	Online security diagnostics via port 8448 of the CP	133
6.4	SNMP	134
6.5	Processing status of messages	135
6.6	Downloading firmware	137
6.7	Module replacement	138
7	Technical data	139
7.1	Technical specifications of the CP	139
7.2	Pin assignment of the socket for the external power supply	140
7.3	Pinout of the Ethernet interface	141
A	Approvals	143
B	Dimension drawings	149
C	Accessories	151
C.1	TS modules	151
C.1.1	The TS modules	151
C.1.2	TS Module Modem	153
C.1.3	TS Module RS232	155
C.2	Modems and routers	156
C.2.1	IP-based routers	156
C.2.2	Dedicated line and dialup network modems	157
C.2.3	MODEM MD720	158

C.3	Antennas	162
C.4	Connecting cables	163
C.4.1	Connecting cables for connecting the CP to Ethernet	163
C.4.2	Connecting cables for connecting the modem of the TS Module RS232.....	164
C.4.3	Connecting cables of the MDx modem	166
C.4.4	Accessories for RS-485 connection	167
D	Encryption methods (Ciphers)	169
E	Documentation references	173
E.1	/1/ S7-1200 system manual	173
E.2	/2/ CP 1243-8 IRC	173
E.3	/3/ SINAUT ST7 system manual	174
E.4	/4/ TeleControl configuration manuals	174
E.5	/5/ SCALANCE M812/M816.....	174
E.6	/6/ SCALANCE M874/M876.....	174
E.7	/7/ SCALANCE S.....	174
E.8	/8/ TS Adapter	175
E.9	/9/ SNMP	175
	Index	177

Application and functions

1.1 Properties of the CP

Application, protocols and communications partners

The CP is intended for operation in a SIMATIC S7-1200 automation system. The CP is the communications processor for connection of the S7-1200 via public or private infrastructures to a telecontrol master station.

The CP can send configured e-mails independent of whether telecontrol communication is enabled.

Supported telecontrol protocols

Depending on the firmware version, the CP supports the following protocols:

- **Firmware version V2.1**
 - SINAUT ST7
- **Firmware version as of V3**
 - SINAUT ST7
 - DNP3
 - IEC 60870-5

Application

The CP can be used in the following systems:

- **SINAUT ST7 system**

In existing SINAUT systems in which the ST7 protocol is used, the CP can be used with the functions of TIM 3V-IE Advanced.
If used for this purpose note the instructions below on configuration.
- **New ST7 systems**

New systems with S7-1200 stations in which the ST7 protocol is used.
- **Existing DNP3 or IEC systems**

In existing systems in which the DNP3 or the IEC protocol is used, the CP can be used as the communications processor of the SIMATIC S7-1200.

Communications partners

The interfaces of the CP support the network node type "station". A master station can be connected as the communications partner of the CP.

- **Firmware version V2.1**

The following master station applications are possible:

- SINAUT ST7cc
- SINAUT ST7sc
- SIMATIC PCS 7 / WinCC TC
- SIMATIC WinCC OA
- A SINAUT master station or node station

- **Firmware version V3**

Depending on the protocol used, the CP supports the following communications partners.

DNP3 or IEC 60870-5

- Communications partners of the CP are the master.
- As of firmware V3.2, the CP also supports direct communication with other stations.

SINAUT ST7

The master station applications and station types specified above under V2.1 can be connected.

Configuration of the CP

- **New systems (ST7, DNP3, IEC)**

To configure the CP in new systems with one of the telecontrol protocols named above use STEP 7 Basic.

In these systems, use a CP with a firmware version as of V3.

- **ST7 systems with STEP 7 V5 configuration**

In existing SINAUT systems with SIMATIC stations of the families S7-300/400 and the TIM modules for remote transfer, the CP can be used for expansions by S7-1200 stations.

In these systems that were configured with STEP 7 V5, use a CP with firmware version V2.1. To configure the CP, you require the two following STEP 7 products:

- STEP 7 V5
and
- STEP 7 Basic

For information on the required STEP 7 versions, see section Requirements for operation (Page 25).

1.2 Communications services

The following communications services are supported:

E-mail

Independent of whether telecontrol communication is activated, the CP can send configured e-mails to PCs with Internet connection, triggered by events. The use of program blocks is not necessary for this.

For information on the configuration, refer to sections E-mail configuration (Page 77) and Messages (Page 82).

Telecontrol communication

The CP is the communications processor for connection of the SIMATIC S7-1200 via public or private infrastructures to a telecontrol master station. You will find the possible application of the telecontrol master station in the section Properties of the CP (Page 13).

The telecontrol protocol "ST7"

For telecontrol communication, the CP uses the ST7 protocol on the application layer (OSI layer 7) for communication via different telecontrol networks.

You will find an overview of the possible transmission options of the serial interface in the configuration manual /3/ SINAUT ST7 system manual (Page 174), SINAUT ST7 Volume 3.

Functions and services of the telecontrol protocol

- **Communication with the control center**
An S7-1200 station with a CP 1243-8 IRC communicates via LAN/WAN with the master station.
- **SMS**
The CP can send SMS messages to cell phones event-driven. SMS messages can be sent if the CP is connected to a mobile wireless network via the RS-232 interface. The use of program blocks is not necessary for this.
For information on configuration, see configuration manual /3/ SINAUT ST7 system manual (Page 174), SINAUT ST7 Volume 3.
- **Inter-station communication**
In dedicated line networks and with communication via the mobile wireless network and the Internet (GSM/MSR), the CP supports inter-station communication between S7-1200 stations via the master station.
With inter-station communication, the CP establishes a connection to the master station. The master station forwards the frames to the destination station.
The partners for inter-station communication must already have been created in the STEP 7 V5 project.
- **Direct communication**
In dial-up networks and Ethernet networks, there is direct communication between the subscribers.

Security protocols

Simple communication via the mobile wireless network (GSM) and the Internet can be achieved with the MSC transmission protocol. If the security requirements are higher, the transmission protocols (OSI layer 3) listed below can be used.

- **MSC**
Can be used with S7 communication
Simple Internet communication (DSL)
The MSC protocol supports authentication of the communications partners and simple encryption of data. A user name and a password are included in the encryption. An MSC tunnel is established between the MSC station and MSC master station.
- **MSCsec**
Can be used with S7 communication
Secure Internet communication (DSL)
MSCsec supports authentication of the communications partners and data encryption with a user name and password. In addition to this, the shared automatically generated key is renewed between the communications partners at configurable intervals.
- **IPsec (VPN)**
Highly secure communication via the Internet (DSL)
Communication via a mobile wireless network combined with the Internet is made possible by the router SCALANCE M. The SCALANCE M product series provides various VPN routers with IPsec and encryption software and their own firewall.
For a description of the configurable Security functions, refer to the section Security (Page 65).

DNP3

Communication is based on the DNP3 SPECIFICATION Version 2.x (2007/2009).

The CP is a communications processor of the SIMATIC S7-1200 for system connection to control centers using the DNP3 protocol for telecontrol applications.

An S7-1200 with a CP functions as a DNP3 station (Outstation).

The CP supports implementation level 1 - 4 (DNP3 Application Layer protocol Level). For additional functions, see /4/ TeleControl configuration manuals (Page 174).

IEC 60870-5

The communication is based on the specification IEC 60870-5 Part 1 - 5 (1990 - 1995) and Part 104 (2000).

The CP is a communications processor of the SIMATIC S7-1200 for system connection to control centers using the IEC 60870-5 protocol for telecontrol applications.

An S7-1200 with a CP functions as a substation (slave).

Supported network types

The CP makes telecontrol communication possible via the following network types:

- Industrial Ethernet
- Mobile wireless networks
The CP supports the following mobile wireless standards:
 - GSM/GPRS (2G)
With 2.5G router SCALANCE M874-2
 - UMTS (3G)
With 3G router SCALANCE M874-3
 - LTE
With router SCALANCE M876-4
- Classic WAN networks via serial interface
 - Dedicated line
 - Analog dial-up network, ISDN network
 - Wireless network
- IP-based wireless networks

You can find an overview of the connection possibilities of the CP's interfaces in the configuration manuals.

Communication via SINEMA Remote Connect

Supported as of firmware version V3.1. See section Communication via SINEMA RC (Page 19).

S7 communication and PG/OP communication

Reading/writing data from/to a CPU 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).
- **S7 routing**
Communication between stations via S7 connections
- **PG functions**
- **Operator control and monitoring functions (HMI)**

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

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

Communication via Open User Communication (OUC)

Via the Ethernet interface of the CP and the program blocks of the Open User Communication on the CPU the CP has the following communication options:

- Communication with SIMATIC stations
- Sending e-mails
In contrast to the corresponding service of telecontrol communication (see above), to transfer e-mails via OUC, the TMAIL_C program block needs to be used, see section Program blocks (Page 123).

1.3 PUT/GET: Restrictions in the CPU

Communications services without connections

The CPU can be a server for a series of communications services without connections being configured for the CPU. Other communications partners can access CPU data. This means that it is no longer possible for the local CPU to control communication with the clients.

You need to grant permission for these communications services at the following location in the CPU configuration:

- Parameter group "Protection & Security > Connection mechanisms"
Enable the option "Permit access with PUT/GET communication from remote partner".

A prerequisite for enabling this option is enabling an access option in the "Access Control > Access level" parameter group. Set the option "Read access" or "Full access".

Note: This setting is connected with security restrictions.

When the "No access (complete protection)" option is enabled, PUT/GET communication cannot be enabled.

"Permit access with PUT/GET communication from remote partner"

Parameter group "Protection & Security > Connection mechanisms" > option "Permit access with PUT/GET communication from remote partner"

The activation of communication services described below applies to the use of the communications module together with a CPU V4.0 to V4.6.

- Option enabled
Access to CPU data from the client side via the communications module using PUT/GET is possible.
- Option disabled
Access to CPU data from the client side via the communications module using PUT/GET is not possible.

Read and write access to CPU data is only possible with communication connections that require configuration or programming both for the local CPU and for the communications partner.

Connections for which the local CPU is only a server (no configuration/programming of communication with the partner) are not possible.

Configuring PUT/GET

You can find additional information on the following Siemens Industry Customer Support page in the documentation specified in the "Download" section:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/82212115>)

1.4 Communication via 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.

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

Parameter groups

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

- Communication via SINEMA RC:
 - > "Security > VPN"
- Telecontrol communication via SINEMA RC:
 - > "Communication types"

For information on the configuration, refer to the telecontrol configuration manuals /4/ TeleControl configuration manuals (Page 174).

Applications

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

Application example:

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

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

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

Table 1-1 Use cases and parameters to be activated

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

* Explanation of the parameter abbreviations:

SRC - Security > VPN (activated) > "VPN connection type":

"Automatic OpenVPN configuration via SINEMA Remote Connect Server"

TC - Communication types > Telecontrol communication enabled

TC-SRC - Communication types >

"Activate telecontrol communication via SINEMA Remote Connect"

1.5 Other services and properties

Other services and properties

- **Data point configuration**

Due to the data point configuration in STEP 7 Basic, programming program blocks in order to transfer the process data is unnecessary. The process data is configured as individual data points and transferred one-to-1 to the master station.

- **IP configuration**

Characteristics of the IP configuration of the Ethernet interface of the CP:

- The CP supports IP addresses according to IPv4.
- Address assignment:
The IP address, the subnet mask and the address of a gateway can be set manually in the configuration.
As an alternative, the IP address can be obtained from a DHCP server or by other means outside the configuration.

- **Time-of-day synchronization**

For information on the method and configuration, refer to the section Time-of-day synchronization (Page 54).

- **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 the event of a power failure.
- **Event-driven transfer of process data**
The CP transmits the data from the send buffer individually or bundled to the communications partner. The transfer can be triggered by various triggers.
- **Analog value processing**
Analog values can be preprocessed on the CP according to various methods.
- **Online functions**
From an engineering station (ES) on which STEP 7 is installed, you can use the online functions of STEP 7 via the Ethernet interface of the CP to access the S7-1200 CPU if the station is located in the same IP subnet.
The following online functions are available:
 - Downloading project or program data from the STEP 7 project to the station
 - Querying diagnostics data on the station
 - Downloading firmware files to the CP

For a remote station located in a different IP subnet or that can be reached via the Internet, these functions can only be used if the ES (with CP 1628 or via SCALANCE S) is connected to the station via a VPN tunnel.
- **SNMP**
As an SNMP agent, the CP supports data queries using SNMP (Simple Network Management Protocol).
For more detailed information, refer to section SNMP (Page 134).

1.6 Security functions

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected.

Read the information in the section Security recommendations (Page 49) for planning and configuring your networks.

Security functions of the telecontrol and transmission protocols

For the telecontrol communication, the following Security functions can be activated:

- **ST7**
The transmission protocols that can be used by the CP for telecontrol communication via the ST7 protocol support the following Security functions:
 - **MSC**
The MSC protocol supports authentication of the communications partners and simple encryption of data. A user name and a password are included in the encryption. An MSC tunnel is established between the MSC station and MSC master station.
 - **MSCsec**
MSCsec supports authentication of the communications partners and data encryption with a user name and password. In addition to this, the shared automatically generated key is renewed between the communications partners at configurable intervals.
- **DNP3**
The security functions specific to DNP3 can be used.

Further configurable security functions of the CP

The following security functions can be used independently of telecontrol communication. Due to the activation of the security functions of the CP in the configuration, the following functions are accessible to the S7-1200 station on the interface to the external network:

- **Firewall**
 - IP firewall with stateful packet inspection (layer 3 and 4)
 - Firewall also for "non-IP" Ethernet frames according to IEEE 802.3 (layer 2)
 - Limitation of the transmission speed to restrict flooding and DoS attacks ("Define IP packet filter rules")
 - Global firewall rule sets

The protection provided by the firewall can cover individual devices, several devices or even entire network segments.
- **VPN**
The following alternatives can be used:
 - Secured communication via IPsec tunnels
VPN communication allows the establishment of secure IPsec tunnels for communication with one or more security modules. The CP can be grouped together with other modules to form VPN groups during configuration. IPsec tunnels are created between all security modules of a VPN group.
The CP supports IKEv1 and IKEv2.
 - 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).
- **Logging**
To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a Syslog server.

- **NTP (secure)**
NTP with support of RFC5905 and RFC5906 with shared key for secure transfer during time-of-day synchronization
- **STARTTLS / SMTPS**
For secure sending of e-mails
- **HTTPS**
For secure access to the Web server of the CPU
- **SNMPv3**
For secure transfer of network diagnostic information

For the range of performance of the security functions refer to the section Performance data and configuration limits (Page 23).

For a description of the configuration, refer to the section Security (Page 65).

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

1.7 Performance data and configuration limits

Number of CMs/CPs per station

In each S7-1200 station, up to three CMs/CPs can be plugged in and configured, of which a maximum of one CP 1243-8 IRC.

Connection resources

- **Telecontrol connections**
The CP can establish connections to up to 4 communications partners.
The partners can be linked redundantly.
When using the ST7 protocol, in addition to this, inter-station communication with up to 4 S7 stations can be operated via the master station.
- **TCP connections**
The CP can establish connections to up to 4 communications partners (S7 stations).
- **Online functions**
1 connection resource is reserved for online functions.
- **S7 connections**
8 connection resources for S7 connections (BSEND/BRCV)
These connections are used for SINAUT ST7 communication.

- **S7 routing**
Max. 4 connections at the same time
- **PG/OP connections**
 - 2 connection resources for PG connections
 - 1 connection resource for OP connections

PG routing between telecontrol modules is supported with telecontrol communication enabled.

Number of data points for the data point configuration

Maximum number of configurable data points (all protocols): 500

Frame memory (send buffer)

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

The send buffer has a maximum size of 64000 frames. The size of the frame memory is divided equally among all configured communications partners. It can be set in STEP 7 Basic, see parameter group "Communication with the CPU".

You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in /4/ TeleControl configuration manuals (Page 174).

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

SMS messages are supported with enabled telecontrol communication and use of the serial interface.

IPsec tunnel (VPN)

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

Firewall rules

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

The firewall rules are divided up as follows:

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

1.8 Requirements for operation

Hardware

The following hardware is required in the S7-1200:

- CP
The requirement for the firmware version V3.3 is a CP with hardware version 2.
- CPU
 - The CP up to firmware version V2.1 (hardware version 1) is compatible with a CPU up to firmware version V3.0.
 - The CP up to firmware version V3.0 (hardware version 2) is compatible with a CPU as of V4.1.
 - The full functionality of the CP with the current firmware version is only available with a CPU as of V4.6.

Configuration software

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

- To use the full range of functions of the current firmware version (see preface):
STEP 7 Basic V19 Update 1

Program blocks for Open User Communication and S7 communication

For Open User Communication and S7 communication, program blocks are required, see section Program blocks (Page 123).

Additional requirements when using telecontrol communication (ST7)

Hardware

When using the serial interface of the CP:

- For communication via WAN networks (dedicated line, dial-up / GSM / wireless network): A TS module
You will find the TS modules in the telecontrol accessories program, refer to the appendix TS modules (Page 151).
A TS basic device (TS Adapter) is not required.
- When using the TS Module RS232: The suitable modem
For information on modems, refer also to the appendix Modems and routers (Page 156).
- When using the TS Module GSM: An external antenna for the CP
Only use antennas from the telecontrol accessories program, refer to the appendix Antennas (Page 162).

1.9 Configuration examples - Intended operating environment

Software

When using the CP to expand SINAUT projects that were configured in STEP 7 V5, you also need:

- STEP 7 as of V5.5
- SINAUT Engineering Software as of V5.5

Usage is described in the configuration manual /3/ SINAUT ST7 system manual (Page 174) SINAUT ST7 Volume 3.

Requirements for using mobile wireless services

- A contract with a suitable mobile wireless network provider
The contract must allow the transfer of data.
- IP address:
For communication with the master station, a private (fixed) or public (dynamic) IP address assigned by the mobile wireless network provider can be used.
- The SIM card and PIN belonging to the mobile wireless contract
The SIM card is inserted in the TS module GSM.
With mobile wireless contracts in which the network provider does not assign a PIN, no PIN is configured for the CP in STEP 7.
- Local availability of a mobile wireless network in the range of the station.

1.9 Configuration examples - Intended operating environment

You will find example system configurations as intended operating environment for use of the CP below.

For protection of the company and plant network, the following security components are recommended:

- External firewalls with Intrusion Detection System (IDS) protect the company network against external attacks.
- DMZ firewalls in the backbone level protect the plant network.
- Security modules protect each individual automation cell.

Note

Security information

To protect your system, refer to the information in the section Security recommendations (Page 49).

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.

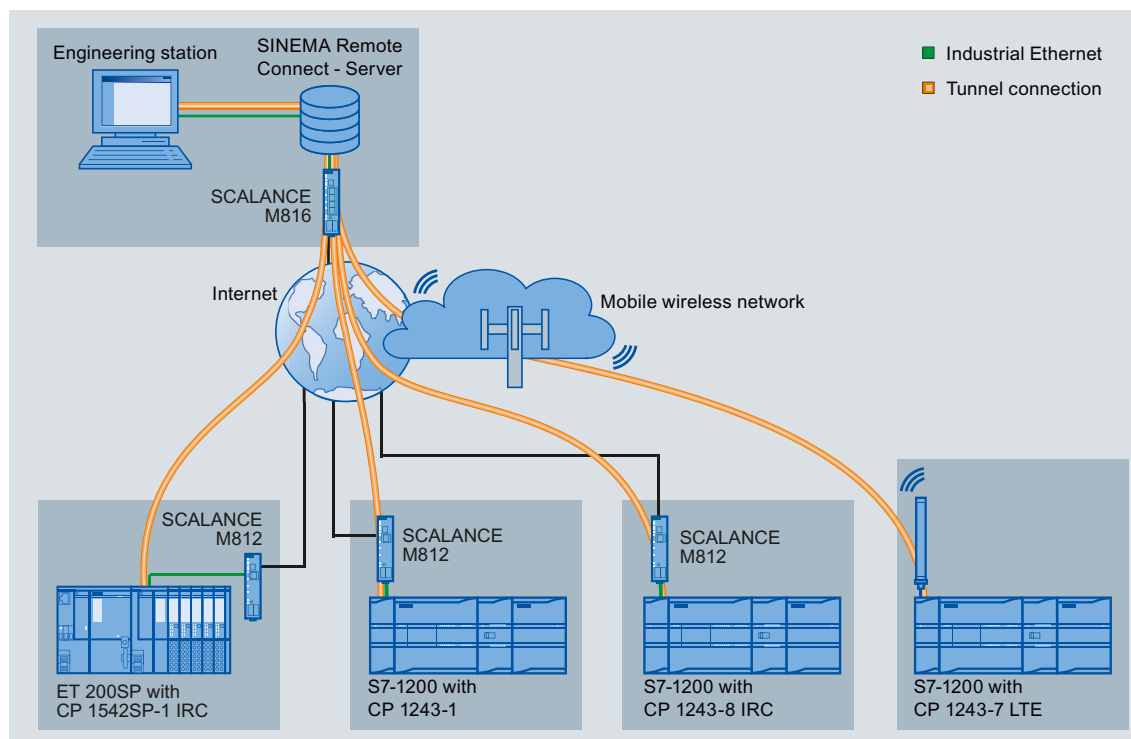


Figure 1-1 Connection of stations to engineering station via SINEMA RC

1.9.1 TeleControl

You will find configuration examples for telecontrol applications in the configuration manuals /4/ TeleControl configuration manuals (Page 174).

LEDs and connectors

2.1 Opening the covers of the housing

Location of the display elements and the electrical connectors

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

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

Opening the covers of the housing

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

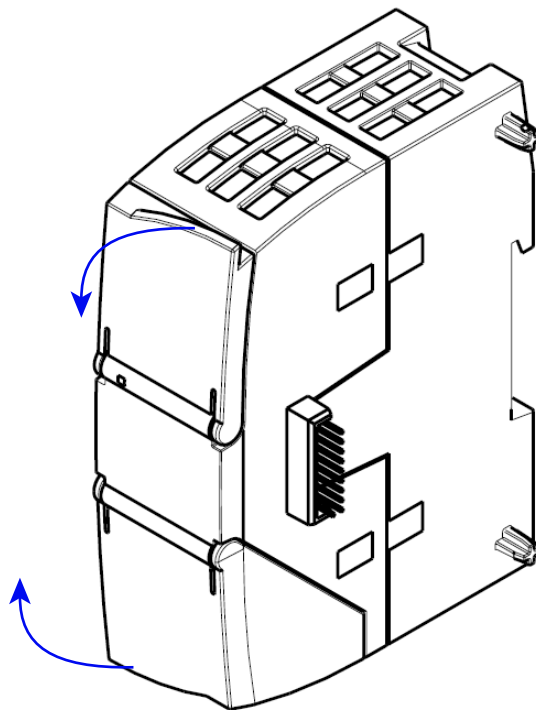


Figure 2-1 Opening the covers of the housing

2.2 LEDs

LEDs of the module

The module has various LEDs for displaying the status:

- **LED on the front panel**
The "DIAG" LED that is always visible shows the basic statuses of the module.
- **LEDs below the upper cover of the housing**
The LEDs below the upper cover provide more detailed information on the module status.

Table 2-1 LED on the front panel

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

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

LED (color)	Name	Meaning
 (red / green)	LINK	• Status of the connection to Industrial Ethernet • Status of the CPU
 (green)	CONNECT ETH	Status of the connections to the partner via Ethernet
 (green)	VPN	Status of the VPN or SINEMA Remote Connect configuration
 (green)	CONNECT RS232	Status of the connections to the partner via the serial interface

LED colors and illustration of the LED statuses

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

Table 2-3 Meaning of the LED symbols

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

Note**LED colors when the module starts up**

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

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

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

DIAG (red / green)	Meaning (if more than one point listed: alternative meaning)
Basic statuses of the CP	
	- Power OFF - Incorrect startup
 green	Running (RUN) without serious error
 flashing green	Partner not connected
 flashing red	- Starting up - Module fault - Backplane bus error - Invalid STEP 7 project data
 flashing red-green	Loading firmware.

Display of the operating and communications statuses

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

Table 2-5 Display of the operating and communications statuses

DIAG (red / green)	LINK (red / green)	CONNECT ETH (green)	VPN (green)	CONNECT RS232 (green)	Meaning (if more than one point listed: alternative meaning)
Module startup (STOP → RUN) or error statuses					
					Power OFF
 red	 green				Startup - phase 1

2.2 LEDs

DIAG (red / green)	LINK (red / green)	CONNECT ETH (green)	VPN (green)	CONNECT RS232 (green)	Meaning (if more than one point listed: alternative meaning)
 flashing red	-				Startup - phase 2
 green	-	-	-	-	Running (RUN) without serious error
 red	-		-	-	Invalid STEP 7 project data
 flashing red	-	-	-	-	Missing STEP 7 project data
 flashing red	-		-		Backplane bus error with configured Ethernet connections
 flashing red	-		-		Backplane bus error with configured connections via the serial interface
 flashing red	-		-		Backplane bus error with configured connections via the Ethernet and the serial interface
Connection to Industrial Ethernet, status of the CPU					
-	 green	-	-	-	Connection to Industrial Ethernet exists CPU in RUN.
-	 flashing green	-	-	-	Connection to Industrial Ethernet exists CPU in STOP
-		-	-	-	No connection to Industrial Ethernet
-	 flashing red	-	-	-	Duplicate IP address detected in the Ethernet network
Connections via Ethernet					
 green	-		-		Configuration of the telecontrol communication via Ethernet error-free and enabled. Connections established to all partners.
 green	-		-		Configuration of the telecontrol communication via Ethernet error-free and enabled. Connection established to at least one partner.
 flashing green	-		-		Configuration of the telecontrol communication via Ethernet error-free and enabled. No connection established.

DIAG (red / green)	LINK (red / green)	CONNECT ETH (green)	VPN (green)	CONNECT RS232 (green)	Meaning (if more than one point listed: alternative meaning)
Connections via the serial interface					
 green	-		-	 *	Configuration of the telecontrol communication via the serial interface error-free and enabled. Connections established to all partners or all partners reachable.
 green	-		-		Configuration of the telecontrol communication via the serial interface error-free and enabled. Connection established to at least one partner.
 flashing green	-		-		Configuration of the telecontrol communication via the serial interface error-free and enabled. No connection established.
Connections via Ethernet and the serial interface					
 green	-		-	 *	Configuration of the telecontrol communication via both interfaces error-free and enabled. All connections established or partners reachable.
 green	-		-	 *	Configuration of the telecontrol communication via both interfaces error-free and enabled. At least one connection established via Ethernet. Connections established to all partners via the serial interface or all partners reachable.
 green	-		-		Configuration of the telecontrol communication via both interfaces error-free and enabled. Connections established to all partners via Ethernet. At least one connection established via the serial interface.
 green	-		-		Configuration of the telecontrol communication via both interfaces error-free and enabled. At least one connection established on every interface but not all.
 flashing green	-		-		Configuration of the telecontrol communication via both interfaces error-free and enabled. No connection established.

2.2 LEDs

DIAG (red / green)	LINK (red / green)	CONNECT ETH (green)	VPN (green)	CONNECT RS232 (green)	Meaning (if more than one point listed: alternative meaning)
 flashing green	-		-		Configuration of the telecontrol communication via both interfaces error-free and enabled. Connection established via Ethernet to at least one partner. No connection established via the serial interface.
 flashing green	-		-		Configuration of the telecontrol communication via both interfaces error-free and enabled. Connection established via the serial interface to at least one partner. No connection established via Ethernet.
VPN/SINEMA Remote Connect connection					
-	-	-		-	VPN/SINEMA Remote Connect connection established
-	-	-		-	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				Loading firmware. The "DIAG" LED flashes alternately red and green.
 flashing green (2x)	 flashing green				Firmware was successfully loaded. The LED "DIAG" flashes green twice.
 flashing red	 flashing green				Error loading the firmware. Remedy: Power OFF → ON

* With configured dial-up network connections, a connection is shown as being established or the partner as being reachable if the connection has been established at least once and then not aborted.

2.3 Electrical connectors

2.3.1 Power supply

Power supply

The 3-pin socket for the external 24 V DC power supply is located on the top of the module. The matching plug ships with the product.

You will find the pin assignment of the socket in section Pin assignment of the socket for the external power supply (Page 140).

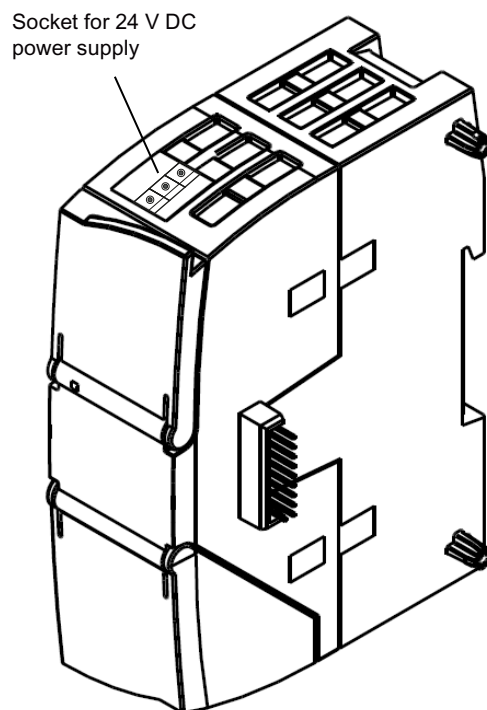


Figure 2-2 Socket for the 24 V DC power supply

Note

You only need to connect the external power supply if you use a TS module on the CP.

2.3.2 Ethernet interface X1P1

Ethernet interface

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

The pin assignment and other data relating to the Ethernet interface can be found in the section Technical data (Page 139).

2.3.3 Serial connection for TS module

Connector for TS module

The connector for a TS module is located on the left-hand side of the CP under the cover, see Installing, connecting and commissioning (Page 41).

Installation, wiring, commissioning, removal

Safety notices on the use of the device

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

3.1 Important notes on using the device

Overvoltage protection

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

3.1.1 Notices about use in hazardous areas

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

3.1 Important notes on using the device

 WARNING

EXPLOSION HAZARD

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

 WARNING

LAN connection (Local Area Network)

A LAN or LAN segment with all the interconnected devices should be contained completely in a single low voltage power distribution system in a building. The LAN is designed either for "Environment A" according to IEEE802.3 or "Environment 0" according to IEC TR 62102.

Do not connect any electrical connectors directly to the telephone network (Telephone Network Voltage) or a WAN (Wide Area Network).

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

 WARNING

Requirements for the cabinet

To comply with EU Directive 2014/34 EU (ATEX 114), UK Regulation SI 2016/1107 or the conditions of IECEx or CCC-Ex, the housing or cabinet must meet the requirements of at least IP54 (according to EN/IEC 60529, GB/T 4208) in compliance with EN IEC/IEC 60079-7, GB 3836.8.

 WARNING

Suitable cables at high ambient temperatures in hazardous area

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

 WARNING

Transient overvoltages

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

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

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

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

 WARNING

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

 WARNING

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

 WARNING

EXPLOSION HAZARD

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

 WARNING

EXPLOSION HAZARD

Replacing components may impair suitability for Class 1, Division 2 or Zone 2.

3.2 Installation, removal and repairs in hazardous areas

 WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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

 WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

 WARNING

Improper installation of shielded cables

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

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

 WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

 WARNING

Unprotected cable ends

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

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

 WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

 WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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

3.3 Installing, connecting and commissioning

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

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

 WARNING

Open equipment

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

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

Prior to installation and commissioning

 CAUTION

Read the system manual "S7-1200 Programmable Controller"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller", refer to the documentation in the Appendix.

When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".

Pulling/plugging the module

NOTICE

Turning off the station when plugging/pulling the module

Before pulling or plugging the module, always turn off the power supply to the station.

Dimensions for installation

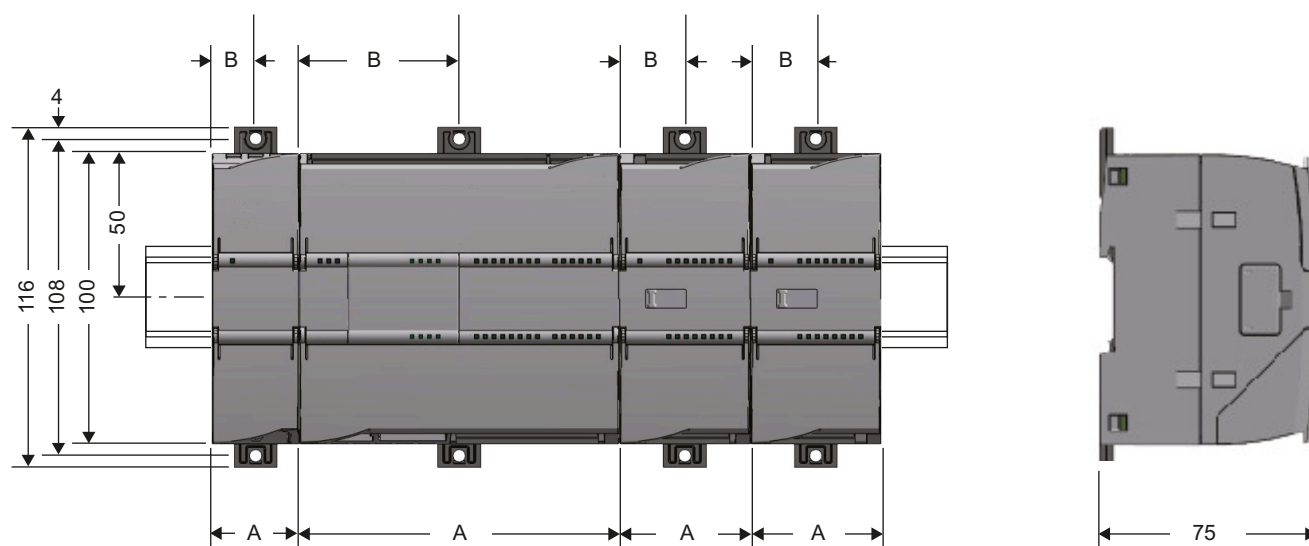


Figure 3-1 Dimensions for installation of the S7-1200

Table 3-1 Dimensions for installation (mm)

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

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

You will find detailed dimensions of the module in the section Dimension drawings (Page 149).

DIN rail clamps, control panel installation

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

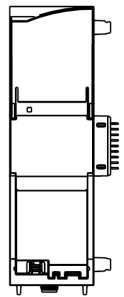
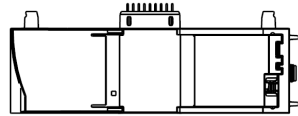
Installation location

NOTICE

Installation location

The module must be installed so that its upper and lower ventilation slits are not covered, allowing adequate ventilation. Above and below the device, there must be a clearance of 25 mm to allow air to circulate and prevent overheating.

Remember that the permitted temperature ranges depend on the position of the installed device. You will find the permitted temperature ranges in the section Technical data (Page 139).

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

WARNING

Power supply

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

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

- Only safety extra low voltage (SELV) with limited power source (LPS) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

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

Connecting up the device and installing it

Below you will find a description of mounting the CP and a TS module on a DIN rail. For mounting the control panel of the S7-1200, refer to /1/ S7-1200 system manual (Page 173).



CAUTION

Connection with power off

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



CAUTION

Slot to the left of the CP only for TS module

To the left of the CP 1243-8 IRC only a TS module can be inserted.

If you insert another module to the left of the CP, this will damage this module.



CAUTION

Ground the connecting cable of a TS module separately

Connect the connecting cable of a TS module to the periphery (e.g. modem) separately to functional ground.

Note

Prior to mounting a TS module

For information on mounting a TS module, also read the appropriate sections in the device manual, see /8/ TS Adapter (Page 175).

Note

Power supply from the power outputs of the CPU

The external power supply of the CP must be supplied via the power outputs of the CPU for the sensor supply.

Keep within the maximum load of the power output of the CPU, see /1/ S7-1200 system manual (Page 173).

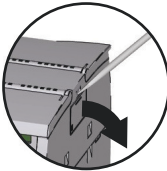
You will find data relating to the current consumption and power loss of the CP in the section Technical data (Page 139).

Note

Turning off the station when plugging/pulling the CP

Do not only turn off the power supply to the CP. Always turn off the power supply for the entire station.

Table 3-2 Procedure for installation and connecting up

Step	What to do	Notes and explanations
1	Secure the DIN rail.	
2	Remove the cover on the left-hand side of the CPU. 1. Insert the tip of a slotted screwdriver in the gap above the cover. 2. Lever the cover carefully from its holder. When using a TS module: Remove the cover on the left-hand side of the CP as described above.	 Recommendation: Store the covers in a safe place for possible later use.
3	Connect the CPU and CP and - if used - the TS module. Push the modules carefully together until the side contacts are completely closed between the two modules.	Permitted slots: • CPU: Right: • CP: In the middle (to the left of the CPU) For the CP, only one slot to the left beside the CPU is permitted. Only one CP 1243-8 IRC can be inserted. • TS module: Left (to the left of the CP) To the left of the CP only a TS module can be inserted.
4	Connecting the power supply • Secure the power supply wires to the power output of the CPU. • Secure the wires of the power supply to the plug supplied with the CP and insert the plug in the socket on the top of the CP.	The pinning of the power output of the CPU is printed on the terminal on the top of the housing of the CPU, see I1/S7-1200 system manual (Page 173). The pinning of the power input of the CP is printed on the top of the housing of the CP beside the socket. You will also find this in the section Pin assignment of the socket for the external power supply (Page 140).
5	Connect the data cable to the CP: • The Ethernet-cable when using Ethernet-based communication. • The relevant cable when using a TS module.	You will find the pinout of the interface in the section Pinout of the Ethernet interface (Page 141).
6	Close the front covers of the modules.	
7	If the DIN rail clamps on the rear of the modules have been pulled out, push in all the DIN rail clamps so that they are locked in place.	
8	Place the connected modules on the DIN rail.	Use a 35 mm DIN rail.
9	Press the connected modules onto the DIN rail until the lower DIN rail clamps have locked in place.	Note If you install devices vertically in an environment with vibration or if you use a TS module GSM, mount end retainers (8WA1 808) on the rail to ensure that the devices remain connected together.
10	Turn on the power supply.	

Commissioning the module

The remaining steps in commissioning involve downloading the STEP 7 project data. One requirement for the full commissioning of the module is the completeness of the STEP 7 project data, see Configuration (Page 49).

The STEP 7 project data of the CP is transferred when you load to the station. To load the station, connect the engineering station on which the project data is located to the Ethernet interface of the CPU.

3.5 Disassembly

You will find more detailed information on loading in the following sections of the STEP 7 information system:

- "Loading project data"
- "Using online and diagnostics functions"

Manual setting the time of day during commissioning

Note

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

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

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

Recommendation:

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

3.4 Note on operation

NOTICE

Closing the front panels

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

3.5 Disassembly



WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

Uninstalling



WARNING

Keep to the order when dismantling

Remove the plugs of the data cable from the TS module and from the CP before you remove the power plug from the CP and therefore disconnect the ground connection of the devices.

1. Switch off the power supply for the entire station.
2. Pull down the two lower DIN rail clamps on the rear of the devices into the extended position using a slotted screwdriver.
This releases the locking mechanism.
3. Swing the devices out of the DIN rail profile to the front.

3.5 Disassembly

Configuration

4.1 Security recommendations

Observe the following security recommendations to prevent unauthorized access to the system.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Check regularly for new features on the Siemens Internet pages.
 - You can find information on Industrial Security here:
Link: (<http://www.siemens.com/industrialsecurity>)
 - You can find a selection of documentation on the topic of network security here:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/92651441>)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
Information regarding product news and new firmware versions is available at the following address:
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21162/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 of the CP to the Internet is required, use the security variants of the telecontrol protocols or use protection mechanisms in front of the CP. Protection mechanisms are for example a SCALANCE M router or a SCALANCE S security module 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
 - Using the security functions of the telecontrol protocols.
 - Use the secure protocol variants, for example NTP (secure) or SNMPv3.
 - Use the secure Open User Communication (Secure OUC) via the appropriate program blocks.
 - Leave access to the Web server deactivated.

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).
The HTTP protocol provides a secure alternative with HTTPS when accessing the Web server.

Table: Meaning of the column titles and entries

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

- **Protocol / function**
Protocols that the device supports.
- **Port number (protocol)**
Port number assigned to the protocol.

- **Default of the port**

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

-

- **Port status**

- Open
The port is always open and cannot be closed.
- Open after configuration
The port is open if it has been configured.
- Open (login, when configured)
As default the port is open. After this port is configured, the communications partner needs to log in.
- Closed after configuration
The port is closed because the CP is always client for this service.

- **Authentication**

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

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
DNP3	20000 (TCP/UDP) Can be set	Closed	Open after configuration	Yes, when Secure Authentication is enabled.
DNP3 with TLS	19999 (TCP) Can be set	Closed	Open after configuration	Yes, when Secure Communication is enabled.
IEC 60870-5-104	2404 (TCP) Can be set	Closed	Open after configuration	Yes, when Secure Authentication is enabled.
IEC 60870-5-104 with TLS	19998 (TCP) Can be set	Closed	Open after configuration	Yes, when Secure Communication is enabled.
S7 and online connections	102 (TCP)	Open	Open *	No
Online security diagnostics	8448 (TCP)	Closed *	Open after configuration *	Yes
IPsec	500 (UDP)	Closed	Open after configuration	Yes
Communication via SINEMA RC	443 (TCP), 5243 (UDP)	Closed	Open after configuration	Yes
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 of the CP (Page 133).

Ports of communication partners and routers

Make sure that you enable the required client ports in the corresponding firewall on the communication partners and in intermediary security modules.

These can be:

- MSC / 26382 (TCP) - configurable with a central interface: 1024 .. 65535
- DNS / 53 (UDP)
- NTP / NTP (secure) / 123 (UDP)
- DHCP / 67, 68 (UDP)
- SINEMA RC Autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)
- Syslog / 514 (UDP)
- Broker port - can be set
 - MQTT unsecured / 1883 (TCP)
 - MQTT via TLS / 8883 (TCP)

4.2 Configuration in STEP 7

Configuration in STEP 7

You configure the modules and networks in SIMATIC STEP 7. You will find the required version in the section Requirements for operation (Page 25).

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

The following description applies to applications without telecontrol communication.

Configuration of the telecontrol communication

You will find the description on configuring the telecontrol communication in the configuration manuals /4/ TeleControl configuration manuals (Page 174).

Overview of the configuration steps in STEP 7

Follow the steps below when configuring:

1. Create a STEP 7 project.
2. Create the necessary SIMATIC stations with the required modules and CPs.
3. Create an Ethernet network.
4. Connect the stations to the Ethernet subnet.
5. Configure the CPs including the messages (e-mail).

6. If required, create the program blocks for S7 communication and Open User Communication and configure them as needed.
7. Save and compile the project.
8. Download the project data to the stations.
Using the "Download to device" function, the STEP 7 project data including the configuration data of the CPs is downloaded to the relevant CPU.

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

Loading and storing the configuration data

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

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

4.3 Basic settings

This parameter group can only be configured when telecontrol communication is enabled.

You will find a description of the telecontrol-specific parameters in the configuration manuals, see /4/ TeleControl configuration manuals (Page 174).

4.4 Communication types

"Communication types" parameter group

In this parameter group, you enable the communications services of the CP.

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

- **Enable telecontrol communication**

Enables telecontrol communication on the CP.

Select the telecontrol protocol via the drop-down list "Protocol type".

- ST7
- DNP3
- IEC 60870-5

Note that if you change the telecontrol protocol later, all protocol-specific data will be deleted. This includes the data point and partner information.

You will find more details in the relevant configuration manual, see /4/ TeleControl configuration manuals (Page 174).

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

You can find additional information in the configuration manuals /4/ TeleControl configuration manuals (Page 174).

For information on remote maintenance via SINEMA Remote Connect, see section SINEMA Remote Connect (Page 73).

- **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.

- **Enable S7 communication to the CPU**

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

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

Please note:

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

Open User 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.

4.5 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 Installing, connecting and commissioning (Page 41).

Validity

The basic instructions for time-of-day synchronization apply generally to the CP and the connected networks.

For a CP with firmware version V2.1 the time-of-day synchronization is specified by the configuration in STEP 7 V5.

The following explanations of the configuration apply to the CP as of firmware version V3. The adoption of the time of day from the CPU is supported by the CP as of firmware version V2.1.77 along with a CPU as of version V4.2.

Basics of time-of-day synchronization

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

If security functions are activated, the module also requires the current time.

The CP can obtain the time of day from an external source; for the method, see below. When using an external time source, the connected S7 station can obtain the current time of day both via the CPU as well as via a CP.

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 a CP, disable time-of-day synchronization of the CPU.

If you have the time synchronized on the CP and the CPU via NTP, when possible use the same NTP server to maintain a consistent time of day within the station.

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

Time-of-day concept

Before configuring time-of-day synchronization, specify the following:

- Specify the time source in the network.
- Specify the time master in the network.
- Specify the network or networks via which the time of day will be forwarded by the time master to the time slaves.

Synchronization method with disabled telecontrol communication

If telecontrol communication is disabled, the following methods of time-of-day synchronization are available:

- **NTP / NTP (secure)**
 - NTP
NTP with support of RFC5905
NTP servers can be configured manually in the table.
 - NTP (secure)
NTP with support of RFC5905 and RFC5906 with shared key
The secure method NTP (secure) can be used if the security functions are enabled. It uses authentication with symmetrical keys. Various configurable hash algorithms are available for the integrity check.
- **Time from CPU**
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 $\geq$ 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 time of the CP can be synchronized under the following condition:
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.

CP-1200 time during startup

The CP has no valid time during startup.

For CPs with firmware version $\leq$ V2.0, the CP reads the CPU time once during startup, even if the option "No time source" is selected as time source. The subsequent time synchronization then depends on the configured synchronization method.

This option can only be used when telecontrol communication is enabled in the "From WAN" setting:

- Use PLC time before first synchronization by master
You can find details on the function in the respective configuration manual.

"Time" parameter group: UTC and time zone settings

Validity:

The functions of this parameter group are valid for the CP as of firmware version V3.5.

Parameter:

- Take time zone values with daylight saving time from PLC
When the option is enabled, the communications module takes the time zone from the CPU.
When the option is disabled, the time zone of the communications module can be configured independent of the CPU.
- Time zone
Here you set the UTC time zone that the communications module will use.
If the "Take time zone values with daylight saving time from PLC" option is enabled, then this option is disabled and the module takes the values of the CPU.
- Use UTC
Only valid for the CP with ST7 or IEC 60870-5 protocol; see configuration manual.

If the communications module does not take the time from the CPU, you can configure the changeover between daylight saving time and standard time:

- Activate daylight saving time
Enables the time changeover (daylight saving/standard time)
If the "Take time zone values with daylight saving time from PLC" option is enabled, then this option is disabled and the module takes the values of the CPU.
- Difference between standard and daylight saving time
Time difference in minutes between standard and daylight-saving time
Default setting: 60 minute time offset for daylight-saving time
- Beginning of daylight saving time / standard time
Here you configure when each time changeover starts:
 - Week of the month
Example:
"First" means "First Sunday in March", if "Sunday" is configured as day of the week and "March" as month.
 - Day of the week
 - "in" = Month
 - "at" = time of changeover

Synchronization method with enabled telecontrol communication

Depending on the protocol used, the following methods are available:

- **DNP3 / IEC**
 - NTP / NTP (secure)
(see above)
 - Time from CPU
 - Time from partner
- **SINAUT ST7**
 - NTP / NTP (secure)
(see above)
 - From local station
The CP adopts the time-of-day of the CPU
 - From WAN
The CP adopts the time-of-day from the connected WAN. This can be an Ethernet network or a classic WAN.
Time masters can be, for example, a synchronized CPU, a device with time receiver or a master station PC (e.g. ST7cc/ST7sc) connected to the network.

Time synchronization via the classic WAN network (ST7)

Time-of-day synchronization via a classic WAN network is only possible when using the serial interface.

Enable time-of-day synchronization via classic networks directly on the network using the parameter group there. You also specify the synchronization cycle. The settings for synchronization are then adopted by all communications modules connected to this network.

The send direction of the time-of-day frames is derived automatically from the network node type of the connected interfaces:

Master station ⇒ Node station ⇒ Station

The settings for the network are not possible with time-of-day synchronization via Ethernet.

The CP can only be a time slave in the connected subnet. In contrast, it can also be time master to the CPU.

Configuration:

1. Network an interface of the CP with a network to which a module is connected that can forward the time or that is time master.
Receiving the time is supported for the Ethernet interface and for the serial interface.
2. Enable the receipt of the time from the required time transmitter.
 - From NTP server
(only when telecontrol communication is disabled)
 - From local station
(adoption of the time from the local CPU)
 - Receive time from WAN
If the CP is connected to a classic WAN network and time-of-day synchronization is enabled in the network, the CP automatically takes the time from the WAN network with the settings made there.

Forwarding the time from the CP to the CPU

Note

Forwarding the time to the CPU

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

- 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 behaviour.

- **CP firmware < V3**
With this firmware version the CP can make the time-of-day available to the CPU as an option via a PLC tag. When this PLC tag is read cyclically by the CPU, the CPU adopts the CP time. In the parameter group "Communication with the CPU", you can set whether or not the current time of day of the CP will be made available to the CPU via a PLC tag. For TLC tags, see parameter group "Communication with the CPU" of the CP.
- **CP firmware ≥ V3.0 and CPU firmware ≥ V4.2**
If both modules in a station have one of the mentioned firmware versions, the time of the CP can be forwarded automatically to the CPU.
A condition for this is: The "CPU synchronizes the modules of the device" option is selected for the CPU under "PROFINET Interface > Time-of-day synchronization".
Then all intelligent modules of the station are synchronized with the CPU time.
Since the CPU automatically adopts the CP time, you no longer require the forwarding option using the PLC tag.

4.6 Ethernet interface

4.6.1 Ethernet addresses

Ethernet addresses

In the following parameter groups you network the Ethernet interface and configure the IP address parameters.

Please note:

A fixed IP address (IPv4/IPv6) is required for the following applications:

- When using S7 communication
- When receiving data via Open User Communication
- When using VPN
- When using SINEMA Remote Connect

You configure the port interconnection and transmission properties in the parameter groups under Advanced options > Port [Xn P1].

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

4.6.2 IPv6

Manual configuration of IPv6 addresses

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

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

Communication partner and IPv6

Note

Internet communication via IPv6

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

OUC communication via IPv6

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

4.6.3 CP identification

The parameter group is available only when telecontrol communication is enabled. You can find additional information in the configuration manuals /4/ TeleControl configuration manuals (Page 174).

4.6.4 Time-of-day synchronization

Time-of-day synchronization

For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 54).

4.6.5 Advanced options

TCP connection monitoring

The settings of the two parameters at the Ethernet interface apply to all TCP connections via this interface.

With mobile wireless CPs, the Ethernet interface is a placeholder for the mobile wireless interface.

- **TCP connection monitoring time**

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

Default setting: 180 s

Monitoring is disabled with the setting zero (0).

The permissible range depends on the module type.

- **TCP keepalive timeout**

After sending a keepalive frame, the module expects a response from the communications partner within the keepalive timeout. If the module does not receive a response after three keepalive frames, it closes the connection.

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.

Default setting: 10 s

The permissible range depends on the module type.

4.6.6 MTU size

MTU size

Option for interface-specific reduction of the maximum packet size on OSI Layer 3 (Maximum Transmission Unit - MTU)

If the frame size (e.g. segments) is limited in your plant, you can reduce the size of the packages sent by the communications module with this option.

Range of values: 1000 .. 1500 Byte

Default setting: 1500

Transmission settings

The protocol-specific transmission settings are visible only when telecontrol communication is enabled. You can find additional information in the configuration manuals /4/ TeleControl configuration manuals (Page 174).

4.6.7 Access to the Web server

Access to the Web server of the CPU

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

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

You will find information on the Web server of the S7-1200 in the manual /1/ S7-1200 system manual (Page 173).

4.7 Serial interface

The serial interface can only be used when telecontrol communication is enabled (SINAUT ST7). You will find a description in the configuration manual SINAUT ST7 Volume 3, see /4/ TeleControl configuration manuals (Page 174).

4.8 DNS configuration

DNS server

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

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

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

4.9 Communication with the CPU

4.9.1 Communication with the CPU

Communication with the CPU

The first four parameters are only relevant for telecontrol communication.

Watchdog bit

- **CP monitoring**
The CP checks the connection with the CPU via the watchdog bit.
The CP transfers the bit to the CPU every 5 seconds and resets it in the next CPU sampling cycle. The bit is not transferred in the event of connection faults. This signals the connection fault to the CPU.
The PLC tag of the watchdog bit must be evaluated by the user program.

CP time

- **CP time to CPU**
The function allows the CPU to read the time of day of the CP. Using this approach, the CP can synchronize the CPU time.
Procedure:
 - The CPU sets the input "Time trigger variable" (BOOL) to 1 with the user program.
 - The CP then writes its time to the "CP time variable" (DTL) and resets the "Time trigger variable" value to 0.
 - The user program reads the "CP time variable" to set the CPU time.
Recommendation:
Set the "Time trigger variable" no more frequently than once per second to avoid placing an unnecessary communication load on the backplane bus.

Note

Refer to the information in the section Time-of-day synchronization (Page 54).

4.9.2 CP diagnostics

The functions are supported by a CP as of firmware version V3.

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. You can also use the value of diagnostic tags to send the states of the CP to communication partners via messages.

- **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.

- **Frame memory overflow**
PLC tag (data type Byte) for the send buffer overflow pre-warning. Bit 0 is set to 1 when 80% of the fill level of the send buffer is reached.
- **Frame memory 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.
- **VPN IPsec status**
The PLC tag (BOOL) indicates whether a VPN IPsec tunnel is established:
 - 0 = No tunnel established
 - 1 = Tunnel established
- **Connection to SINEMA Remote Connect**
The PLC tag (BOOL) indicates whether there is a connection to the SINEMA RC server:
 - 0 = No connection established
 - 1 = Connection established

4.10 SNMP

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 SNMP (Page 76).

Configuration

- **"Enable SNMP"**

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

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

4.11 Security

The configurability of the individual options depends on the telecontrol protocol being used.

You will find an overview of the range and use of the security functions in section Security functions (Page 21).

For the configuration limits of the security functions refer to the section Performance data and configuration limits (Page 23).

To be able to configure the security functions, you need to create a security user; see section Security user (Page 66).

4.11.1 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 Administrator" in the "Assigned roles" area below.

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

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

4.11.2 Parameter overview

Parameter groups

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

- **CP identification**
Only with the TeleControl Basic protocol
Here, you configure parameters for authenticating the CP with the telecontrol server. You will find details on the parameters in the TeleControl Basic configuration manual, /4/ TeleControl configuration manuals (Page 174).
- **Firewall**
See section Firewall (Page 67).
- **Time-of-day synchronization**
For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 68).
- **Authorized phone numbers**
(only mobile wireless CPs)
- **E-mail configuration**
See section E-mail configuration (Page 77).
- **Log settings**
Here you make the settings for logging events relevant for security.
See section Log settings - Filtering of the system events (Page 69).
- **VPN**
Here you configure the VPN communication; refer to the section VPN (Page 69).
- **SNMP**
(only Ethernet CPs)
Here you make the settings for the SNMP agent on the CP.

- **Certificate manager**
See section Certificate manager (Page 78).
- **CloudConnect**
See section CloudConnect (Page 88).

Global security settings

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

- **VPN groups**
You create VPN groups and assign devices to them.
- **Users and roles**
Here you configure the users, roles and rights.

4.11.3 Firewall

4.11.3.1 Pre-check of messages by the MAC firewall.

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

4.11.3.2 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 67) for information on this.

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

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.

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.

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

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

- Separate the two IP addresses only using a hyphen.
Correct: 192.168.10.0-192.168.10.255
- Do not enter any other characters between the two IP addresses.
Incorrect: 192.168.10.0 - 192.168.10.255

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

4.11.4 Time-of-day synchronization

Time-of-day synchronization

For the configuration of the time-of-day synchronization read the section Time-of-day synchronization (Page 54).

4.11.5 Log settings - Filtering of the system events

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

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

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

4.11.6 VPN

4.11.6.1 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.

4.11.6.2 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.

4.11.6.3 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 or an ST7cc/sc PC 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.

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 local security settings 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 "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 or an ST7cc/sc PC runs as follows along with the time of day synchronization of the CP:

On the engineering station or the ST7cc/sc PC, 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 ST7cc/sc PC 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 in the "Properties" > "General" tab of the Inspector window under "Authentication".
2. You configure the pre-shared key or the certificate under the properties of the VPN group. 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 automatically when you assign the security module to a VPN group. You cannot deselect the check box.

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

4.11.6.4 VPN communication with SOFTNET Security Client (PC / engineering station)

Setting up VPN tunnel communication between the SOFTNET Security Client and CP has essentially same requirements and procedure as described in the section Creating a VPN tunnel for S7 communication between stations (Page 70).

VPN tunnel communication works only if the internal node is disabled

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

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

To establish successful VPN tunnel communication to the CP, you need to disable the internal subscriber of the CP as follows.

Follow the steps below in the SOFTNET Security Client tunnel overview:

1. Deactivate the option "Learn internal nodes" under "settings" > "SOFTNET Security client-settings".
The lower-level node initially disappears from the tunnel list.
2. In the tunnel overview , select the required connection to the CP.
3. With the right mouse button, select "Activate connection to the internal subscribers" in the shortcut menu.
The lower level node appears temporarily in the tunnel overview.
4. Select the lower-level node in the tunnel overview.
5. Select "Delete Entry" in the shortcut menu.

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

4.11.6.5 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

VPN subscriber (active) $\Leftrightarrow$ gateway (dyn. IP address) $\Leftrightarrow$ Internet $\Leftrightarrow$ gateway (fixed IP address) $\Leftrightarrow$ CP (passive)

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

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

4.11.6.6 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.

4.11.6.7 SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- **Configuration of SINEMA Remote Connect Server**
Configure SINEMA RC Server as necessary (not in STEP 7). The communications module and its communications partners must be configured in the SINEMA RC Server.
- **Exporting the CA certificate (optional)**
If you want to use the server certificate as authentication method of the communications module during connection establishment, export the CA certificate from SINEMA RC Server. Then import the CA certificate from SINEMA RC Server to the engineering station. Alternatively, you can use the fingerprint of the server certificate as authentication method of the communications module. The fingerprint's duration of validity may be shorter than that of the certificate.
Please note that you need to repeat the import of a certificate in the event of a module replacement.

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

SINEMA Remote Connect Server

Enter the address and port number of the server.

Server Verification

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

- **CA Certificate**
Under "CA certificate", select the CA certificate from SINEMA RC Server that was previously imported and assigned in the local certificate manager.
The module generally checks the CA certificate of the server and its validity period. The two options cannot be changed.
- **Fingerprint**
When you select this authentication method, you enter the fingerprint of the server certificate of SINEMA RC Server.

Authentication

- **Device ID**
Enter the device ID generated for the module in SINEMA RC.
- **Device password**
Enter the device password of the module configured in SINEMA RC.
Max. number of characters: 127

Optional settings

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

- **Update interval**
With this parameter you set the interval at which the CP queries the configuration on the SINEMA RC Server.
Note that with the setting 0 (zero) changes to the configuration of the SINEMA RC Server may result in the CP no longer being capable of establishing a connection to the SINEMA RC Server.
- **"Connection type"**
The two options of the parameter have the following effect on the connection establishment:
 - **Auto**
The module establishes a connection to the SINEMA RCServer. The OpenVPN connection is retained until the connection parameters are changed by the SINEMA Remote Connect Server. If the connection is interrupted, the CP automatically re-establishes the connection.
If the connection parameters are changed by the SINEMA Remote Connect Server, the CP requests the new connection data after the update interval configured above has elapsed.
 - **PLC trigger**
The option is intended for sporadic communication of the module via the SINEMA RC Server.
You can use this option when you want to establish temporary connections between the module and a PC. The temporary connections are established via a PLC tag and can be used in servicing situations, for example.

Note

Connection abort

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

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

- **PLC tag for connection establishment**
If the option "PLC trigger" is selected, the module establishes a connection when the PLC tag (Bool) changes to the value 1. During operation the PLC tag can be set when necessary, for example using an HMI panel.
When the PLC tag is reset to 0, the connection is terminated again.

4.11.7 SNMP

SNMP

You will find the range of functions of the device for SNMP in the section SNMP (Page 134).
If the security functions are enabled, you have the following selection and setting options.

SNMP

- **"Enable SNMP"**
If the option is enabled, communication via SNMP is released on the device. As default, SNMPv1 is enabled.
If the option is disabled, queries from SNMP clients are not replied to either via SNMPv1 or via SNMPv3.
- **"Use SNMPv1"**
Enables the use of SNMPv1 for the device. For information on the configuration of the required community strings see below (SNMPv1).
- **"Use SNMPv3"**
Enables the use of SNMPv3 for the device. For information on the configuration of the required algorithms see below (SNMPv3).

SNMPv1

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

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

- **"Reading community string"**
The string is required for read access.
Leave the preset string "public" or configure a string.
- **"Allow write access"**
If the option is enabled write access to the device is released and the corresponding community string can be edited.
- **"Writing community string"**
The string is required for write access and can also be used for read access.
Leave the preset string "private" or configure a string.

Note

Security of the access

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

SNMPv3

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

- **"Authentication algorithm"**
Select the authentication method to be used from the drop-down list.
- **"Encryption algorithm"**
Select the encryption method to be used from the drop-down list.

User management

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

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

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

4.11.8 E-mail configuration

Configuring e-mails in STEP 7

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

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

You configure the individual e-mails in the message editor (entry "Messages"), see section Messages (Page 82)

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

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

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

- Port no. 587
By using STARTTLS, the module sends encrypted e-mails to the SMTP server of your e-mail service provider.
Recommendation: If your e-mail provider offers both options (STARTTLS / SSL/TLS), you should use STARTTLS with port 587.
- Port no. 465
By using SSL/TLS (SMTPS), the module sends encrypted e-mails to the SMTP server of your e-mail service provider.

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

Importing the certificate with encrypted transfer

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

Use the certificate by taking the following steps:

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

For the procedure, refer to the section Certificate manager (Page 78).

4.11.9 Certificate manager

Certificate manager of SIMATIC NET devices

SIMATIC NET communications modules generally use the global certificate manager. You can find this in the project navigation under "Security settings > Security features".

All certificates that are created and displayed by the configuration with the SIMATIC NET communications module can also be found in the global certificate manager.

Certificates for authentication

If you have configured secure communication with authentication for the communications 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.

Examples of services and functions that require certificates:

- Communication of the TIM 1531 IRC with the higher-level CPU
The connection of the TIM to the CPU uses secure communication via TLS for all telecontrol protocols supported by the TIM.
For communication via TLS, you need to use a newly created CPU certificate and specify it to the TIM in the "Subscriber numbers" parameter group.
For information on the procedure, refer to the section Handling certificates (Page 79).
- Secure transfer of e-mails
An SSL certificate is created for the module to transfer data via SSL/TLS. It is visible in STEP 7 in the local certificate manager and under "Global security settings > Certificate manager > Device certificates" with the "WebServer" service.

If a STEP 7 communications module is to communicate securely with non-Siemens partners, the relevant certificates of the communications partners must be exchanged. To do this, follow these steps:

1. Import the third-party certificates of the external communications partner
Global security settings of the project > "Trusted certificates and root certification authorities"
2. Assigning a certificate to the communications module

Assigning certificates

If you create certificates for modules in STEP 7 retroactively or import third-party certificates into STEP 7, you need to assign them to the respective module, either via:

- Local certificate manager of the communications module > "Certificates of the partner devices"
- Global security settings of the project > "Trusted certificates and root certification authorities"

For information on the procedure, refer to the section Handling certificates (Page 79).

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

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

4.12 Data points

You will find a description of the telecontrol-specific parameters in the configuration manuals, see /4/ TeleControl configuration manuals (Page 174).

4.13 Messages

SMS messages can only be sent with enabled telecontrol communication and use of the serial interface.

Configuring e-mails

If important events occur, the CP can send messages. E-mails are configurable. The recipient can be a PC with an Internet connection or an S7 station.

You configure the messages with the message editor of the CP. Alternatively, you will find it:

- The shortcut menu of the CP (with selected module)
- Via the project navigation: Directory of the station > Local modules > CP

You will find the characters permitted for message texts and additional parameters in the section Character set for user names, passwords and messages (Page 87).

Project overview 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.

Information required to use e-mails:

- 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 perform 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 77).
- 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"

Configuration in the message editor

You configure the messages in STEP 7 in the data point and message editor. Alternatively, you can open the editor:

- By 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.

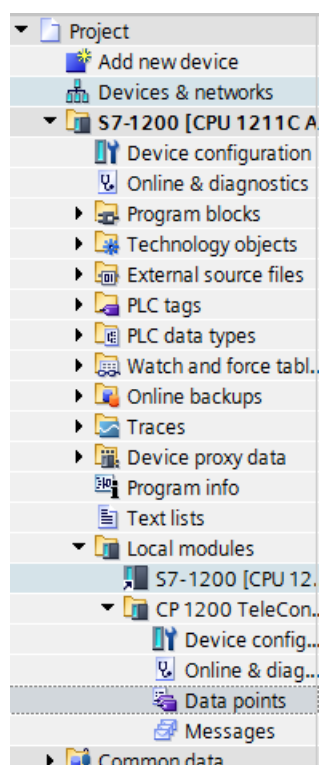


Figure 4-1 Opening the message editor via the project navigation

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



Figure 4-2 Switching over between the two editors

The data point editor is only relevant for the telecontrol communication.

Creating objects

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

You can change the default name to suit your purposes, but it must be unique within the module.

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:

- **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 right-click on a column header: "Optimize width", "Optimize width of all columns"
 - If you move the cursor close to the right limit of a column header, the following symbol appears:



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

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

Copy messages

You can copy and paste messages. 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.

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

Tab for configuring the messages

Select a message in the "Messages" table. You configure the parameters of this selected message in the tabs below the table.

"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**

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 telecontrol connection returns.

- **Connection establishment to partner failed**

Triggers the sending of the message when the connection to the telecontrol server could not be established.

- **TeleService session started**

Triggers the sending of the message when the TeleControl Basic communication type is enabled and a TeleService connection is established.

- **TeleService session ended**

Triggers the sending of the message when the TeleControl Basic communication type is enabled and a TeleService connection has been terminated.

- **VPN connection established**

Triggers the sending of the message when the VPN connection is established or returns.

- **VPN connection terminated**

Triggers the sending of the message when the VPN connection is interrupted.

- **SINEMA RC connection established**

Triggers the sending of the message when the OpenVPN connection is established or returns.

- **SINEMA RC connection terminated**

Triggers the sending of the message when the 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 the "PLC tag for processing status". If there are problems delivering messages, you can determine the status via the Web server of the CPU by displaying the value of the PLC tag there.
For the significance of the status output in hexadecimal, refer to the section Processing status of messages (Page 135).
- **PLC tag for processing status**
PLC tag of the type DWORD for the processing status
- **Include value**
When the option is enabled, the CP sends a value from the memory area of the CPU for the placeholder \$\$ 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, UInt, DInt, Real, String,
 - Arrays of the data types above
- **PLC tag for value**
PLC tag in which the value to be sent is written.

4.14 Character set for user names, passwords and messages

Character set for user names, passwords and message texts

The following permitted characters apply to:

- E-mail server:
 - User name and password
- Messages in the message editor:
 - Message texts

Entered as ASCII character sets (hexadecimal value and character name):

- 0x20
Space
- 0x21 ... 0x5F
!"#\$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMN OPQRST
UVWXYZ[\]^_
- 0x61 ... 0x7E
abcdefghijklmnopqrstuvwxyz{|}~
- 0x7C, 0x7E
|~

In addition for message texts:

- Manual line break (↵)
In message texts, you can insert a line break using <Shift>+<Enter>.

4.15 CloudConnect

4.15.1 Cloud communication

Protocols for the cloud connection

The CP supports the following protocols for communication with a cloud broker or cloud server:

- MQTT
According to OASIS standard version 3.1 / 3.1.1

Cloud systems and communication functions

The CP supports the connection to cloud systems that support broker functionality with the MQTT protocol.

The configuration of cloud access ("Cloud operator") is adapted to communication with the following cloud systems:

- Possible cloud systems are:
 - AWS (Amazon)
Service: IoT Core
 - Azure (Microsoft)
Service: IoT Hub
 - IBM Cloud (IBM)
Service: Watson IoT Platform
- Function of the CP:
 - Publisher
 - Subscriber
For details, see below.

Functions of the CP for cloud communication

The following table summarizes the support of functions with various cloud providers valid at the time of printing of the manual.

Ask your cloud provider which functions it supports.

Meaning of the symbols:

- +: Supported
- -: Not supported

Function	AWS (Amazon)	Azure (Microsoft)	IBM Cloud (IBM)
Publisher function of the CP	+	+	+
Subscriber function of the CP	-	-	+
QoS = 2			
MQTT via TLS	+	+	+

Communication partner of the CP

- Publisher
A publisher publishes data to a cloud broker.
Together with the CP as a subscriber, the following devices can act as a publisher:
 - CP 1200
 - Third-party device
Third-party devices, the configuration and payload format of the messages of which are compatible with the CP.
- Subscriber
A subscriber logs on to the cloud broker and subscribes to data of the publisher.
Together with the CP as a publisher, the following devices can act as subscribers:
 - CP 1200
 - Third-party device
Third-party devices, the configuration and payload format of the messages of which are compatible with the CP.

For details on the compatibility of communications processor and third-party devices, see section Configuration rules (Page 92).

Secure communication certificate -

If you want to use secured cloud communication, select "MQTT over TLS" option under "Security > CloudConnect > Broker configuration".

In this parameter group you specify the broker certificate to be used, which you have previously imported in the global security settings and assigned to the CP.

If a partner (Publisher / Subscriber) that communicates with the CP via the cloud requires certificates for secure communication, use the certificate of the partner at the CP in the "Client certificate" drop-down list.

For information on the configuration, see CloudConnect (Page 88).

4.15.2 Configuring the cloud access

4.15.2.1 Overview of configuration

Configuring cloud access - Overview

1. To allow the cloud application to access the process image, create the required DBs and DB tags in the local CPU.
The data points of the topics (see below) access these DB tags; see section Operand areas and tags (Page 98).
2. Create at least one user with the role "NET Administrator" in the Global Security settings.
3. Enable the option "Activate security features" for the CP under the parameter group "Security".
4. Enable the option "Activate CloudConnect" for cloud communication of the CP.
For the supported cloud providers, refer to the section Cloud communication (Page 88).
Configure the other parameters; see section "CloudConnect" parameter group (Page 94).
5. If you configure encrypted communication (MQTT over TLS) with the broker, you need at least the relevant certificate and possibly a key of the cloud provider.
Obtain this from your cloud provider, possibly from its Internet pages, and import the files into the STEP 7 project and the CP. For the procedure, refer to the section Configuring topics (Page 99).
6. Then expand the project tree:
Station > Local modules > CP > Cloud connection
See section Quality of Service (QoS) (Page 116) for more on this.
Create a topic.
7. Open the topic, insert data points and configure them.
8. Open the properties dialog of the topic via the "Properties" shortcut menu.
 - Configure the name and optional "Author" and "Comment" of the topic.
 - Configure the "Required Quality of Service (QoS)". See section Quality of Service (QoS) (Page 116) for more on this.
 - If required, configure a time trigger for the topic.

4.15.2.2 Notes on data structuring and configuration

Data structures

To access the process data for cloud communication, the CP accesses the DB tags of the CPU. The data that is referenced in the DB tag is configured in the CP via data points.

The data can be structured differently for transfer to the broker:

- Topics
A topic is the channel for the transfer of values of one or more data points.
You can create several topics.

Topic names

Configuration of the topic names:

The topic names are configurable.

4.15.2.3 Configuration rules

Configuration rules

Observe the following rules for configuration:

- **Data blocks**

- Size

The number of variables in the DB is not limited.

When you create arrays, only elements/tags of arrays with a maximum size of < 10000 elements can be published.

- **Topics**

- Quantity

Maximum number per CP: 500

- Name

Within a cloud application, the name of a topic must be unique.

This applies to all participating publishers and subscribers.

Also read the information in the Permitted Characters (Page 120) section.

- Size

The number of data points that a topic may contain is additionally limited by the total amount of the payload, see below.

Data points

- Quantity

Maximum number of data points per CP: 500

Maximum number of data points per topic: 500

The number of data points that a topic may contain is additionally limited by the total amount of the payload, see below.

- Name

Within a topic, the name of a data point must be unique.

Also read the information in the Permitted Characters (Page 120) section.

Payload amount

- Total amount of payload per topic

Maximum 500000 Byte (corresponds to 500000 ASCII characters)

- Total amount of payload per CP

Maximum 500000 Byte (corresponds to 500000 ASCII characters)

The amount of payload in the configuration depends on the payload format used. The size of the standard payload format with one data point and a data point name length of 21 ASCII characters is:

- JSON : 258 Byte

- XML : 363 Byte

If you use longer names or additional code components (e.g. additional attributes), you need to add these.

Example for the calculation of the payload amount:

With an amount of payload format of 500 ASCII characters for a data point, one data point per topic and 500 configured topics, the total amount of payload would be 250000 bytes.

Note:

Because the variables are replaced by values when the messages are published, the amount of payload on the network can be different to the amount of payload in the configuration.

Consistency check of the subscriber

Note

Consistency check of parameters for Publisher and Subscriber

If the CP as a subscriber receives data from a publisher during runtime, the subscriber checks the following parameters supplied by the publisher in the user data for each value received:

- Topic name
- Data point name
- Data type

The station name of a publisher is not evaluated by the CP as a subscriber.

Evaluation

Result of the consistency check:

- Parameters identical
If these three parameters of the publisher are identical with the parameters configured in the subscriber and if the QualityCode of the message is "GOOD", the subscriber writes the received data into the data block of its CPU.
 - Parameters not identical
If one or more of these three publisher parameters do not match the parameters configured in the subscriber, the subscriber discards the data.
-

Recommendations

When transferring data in a hierarchically structured system, it is generally advisable to name the components according to this hierarchical structure.

The later assignment and evaluation of the published data is facilitated if the names refer to the process data of the stations.

Examples:

- Topic name
You want to name a topic "Motor5". The data is assigned to the S7 station "Station1".
Example of a topic name:
"Station1_Motor5"
- Example of a data point:
"Plant1_Unit1_Aggregate1_DB_1_Signal1"

Data points and DBs

Within a cloud application, individual publishers can publish data for multiple subscribers. Individual subscribers can subscribe to data from multiple publishers.

For better clarity of the data and to reduce the possibility of identical names, the following procedure is recommended for configuration:

- Data blocks
In a CPU, create separate DBs only for the publisher function and only for the subscriber function.
- Data point name / DB number
If you use the number of the data block (DB) that the data point accesses as part of the data point name, it is easier to assign the data point.
- Publisher
 - Create a separate DB for every subscriber for the CP as a publisher.
 - If a CP subscribes to data from multiple publishers, configure a different DB number for the respective DB intended for this subscriber with the different publishers.
This prevents tags from different publishers from having an identical data point name if the data point names use the DB number as part of the name.
- Subscriber
Create a separate DB for each publisher for the CP as a subscriber.
Comment:
Subscribed data can only be written in DB tags. For further processing, the user program must access the DB tags. This prevents subscribed data from changing the process image directly during receiving.

The described recommendations are not mandatory but increase the clarity when assigning data and reduces the possibility of identical names.

4.15.2.4 "CloudConnect" parameter group

Requirement

Activation of the security functions is a requirement for the configurability of cloud communication.

If you disable the security functions later, note that all previously configured cloud data will be lost, except for the data points and topics.

General

- **Activate CloudConnect**
Activates communication with a cloud system via the Ethernet interface of the CP.
- **Scan cycle of variables**
Cycle (ms) in which the DB tags of the CPU are queried.
Range of values: 100..4294967295 ms

Note

Volume of transferred data

The value of the parameter has direct effects on the transferred data volume.

When the trigger condition of a value trigger is met, the data is transferred to the broker with each scan cycle of variables. See also the note in section Trigger (Page 101).

Data loss

If you configure a very short scan cycle of variables together with a very large number of data points, it can occur with some brokers that not all of the published data can be read from the input buffer of the cloud server.

Note also the function of the frame memory, see section Connection abort and data buffering (Page 117).

- **Topics with time stamp**
When this option is enabled, the current time stamp is added to each value at the time of each publication.

Diagnostics

You can optionally configure diagnostics data here.

- **Status broker connection**
The tag (Bool) is set to 1 when the connection to the broker is established.
The value is equal to 0 if no connection is established.
- **Send buffer usage**
The tag (Bool) specifies the usage of the frame memory as a percentage.
In case of disruptions in the connection between CP and broker, the CP saves the frames in the frame memory.
- **CPU sampling error**
The tag (UDInt) specifies the number of scan errors since the last reset of the diagnostic trigger tag.
The number of tags whose values could not be read for the cloud communication during the last scan cycle, for example due to a high communication load at the backplane bus, are counted.
If the CPU sets the diagnostics trigger tag back to 1, the counter of the diagnostics tag is reset to zero.

Broker configuration

- **MQTT / MQTT via TLS**
Alternatively, select one of the following protocol variants:
 - MQTT (unencrypted transmission)
 - MQTT via TLS (encrypted transmission)
- **Minimum TLS version**
Defines the TLS version used by the CP and the partner.
- **Broker certificate**
The parameter is only active when you have enabled encrypted transmission "MQTT via TLS".
In this case, you need a certificate from your cloud provider.
Default setting: "Automatic". With the "Automatic" setting, a certificate from the trusted certificates is assigned.
To manually assign the certificate, follow these steps.
 - Import the partner certificate:
Global security settings > Certificate manager > Trusted certificates > right mouse click
 - Assign the certificate to the CP:
Select certificate in the "Trusted certificates" list > right mouse click
The certificate appears in the "Certificates of the partner devices" list on the CP in the parameter group "Security > Certificate manager".
 - Now select the imported certificate in the "Broker certificate" drop-down list.
- **Broker address**
Address of the broker server (IPv4 address or host name)
- **Broker port**
Port number of the broker server
 - Port 1883 is preset for unencrypted transmission (MQTT).
 - Port 8883 is preset for encrypted transmission (MQTT via TLS).
- **Client ID**
Enter the client ID that was assigned by your service provider or that you defined.
Max. 255 characters from the ASCII band (hex) 0x20 .. 0x7F

- **Client certificate**

The CP certificate is only used for secure cloud communication (MQTT via TLS).

When a partner (Cloud / Publisher / Subscriber) that communicates with the CP requires certificates for secure communication, use the certificate of the CP. The client certificate is automatically created by STEP 7, used for the CP, and displayed in the output field of the parameter.

Handling the certificates:

The corresponding certificates must be exchanged for secure communication:

- Exporting the certificate of the CP or the STEP 7 project
For the CP certificate to be used, the CA certificate of the TIA project must be imported to the cloud server as trusted certificate. To do so, export the CA certificate with the matching hash algorithm from the global security settings:
"Security settings > Security features > Certificate manager > Certificate Authority (CA)" > selection of certificate > shortcut menu "Export"
Then transfer the certificate to the cloud server.
- Importing the certificate of the communication partner
You must import the respective certificate from the communication partner as a trusted certificate into your STEP 7 project. To do this, follow these steps:
Save the certificate in the file system of the STEP 7 project computer. Import the certificate into the global security settings:
"Security settings > Security features > Certificate manager > Trusted certificates and root certification authorities" > selection of an empty table row > shortcut menu "Import"
The procedure depends on the cloud being used.
For some clouds, such as AWS, for example, you must assign this certificate to the CP as device certificate. To do this, follow these steps:
- Assigning the cloud certificate to the CP (depending on the cloud)
Requirement: You have imported the certificate of the cloud in the global security settings as described above.
Select the certificate in the "Trusted certificates and root certification authorities" list, click on the shortcut menu "Assign" and select the CP in the next dialog.
The certificate is now displayed in the local Certificate manager of the CP in the "Certificates of the partner devices" list.

- **Clean session**

When this option is enabled, the session information is deleted when the connection is terminated.

When the option is disabled, the session information is retained when the connection is terminated.

Note

Recommendation: Enable "Clean session"

It is recommended that you enable the parameter.

If QoS is configured with a value > 0 and "Clean session" is disabled, unclear situations can arise in the event of connection aborts with respect to pending acknowledgments.

Broker monitoring

- **Keepalive interval**

Monitoring time of the connection with the broker

If no further data is pending for transmission within the configured monitoring time after the data is sent or if the CP does not receive a packet from the broker, the CP sends a keep-alive packet (PINGREQ) to the broker.

If the broker does not acknowledge the PINGREQ frame within 1.5 times the configured keepalive interval with a PINGRESP, the CP terminates the connection.

Note the effect of the parameter on the response to connection aborts, see section Connection abort and data buffering (Page 117).

Changes to the value after commissioning are applied after another "Download to device".

Broker authentication

- **Enable authentication**

When this option is enabled, the connection to the broker is established with authentication.

If possible, use TLS to transmit the user name and password.

When the option is disabled, the connection is established anonymously.

- **User name**

Enter the user name that was assigned by your service provider or that you defined.

- **Password**

Enter the password that was assigned by your service provider or that you defined.

4.15.2.5 Operand areas and tags

Operand area

Tags from the following operand areas of the CPU can be used for the transfer of data of the S7 station:

- Data block (global DB)

Note during the configuration in the properties dialog of the DB:

- Enable the attribute "DB accessible from OPC UA".

Configuring the DB tags

Select the following options when configuring the DB tags:

- "Accessible from HMI/OPC UA"
- "Writable from HMI/OPC UA" (required for write access)

You can find the data types that can be used for the cloud connection in the section Data types (Page 100).

4.15.3 Configuring topics and data points

4.15.3.1 Configuring topics

Structure of the data

You create productive data as follows:

- Topics
You can create several topics.
- Data points
A topic can contain multiple data points.

Select the station in the project tree and expand it:

> Station > Local modules > CP > Cloud connection > Published topics / Subscribed topics

Take note of which function (Publisher / Subscriber) is supported together with your cloud provider, see section Cloud communication (Page 88).

Click "Add topic". A topic is created and the Topic editor opens.

For information on the further configuration of topics, see section Configuring the data points (Page 100).

Opening the Topic editor

Open the Topic editor as follows:

1. Expand the project tree:
Station > Local modules > CP > Cloud connection > Published topics / "Subscribed topics"
2. You can open the Topic editor in two ways:
 - By double-clicking "Add topic"
 - By double-clicking on an existing topic

Opening the payload editor

When the Topic editor is open, you can see the following two tabs in the upper right corner:

- Topic editor
- Payload editor

You can switch between the two editors by clicking on the tabs.

In the Payload editor, you define the format of the payload to be published, see section Payload formats (Page 106).

To edit the payload format outside STEP 7, see section Import / export of payload (Page 109).

Note**Configuring the payload format for publishers only**

Note that the payload format is only configured for data that is published.

4.15.3.2 Configuring the data points

Inserting data points in a topic

Open a topic with a double-click.

In the topic, click in the "PLC tag" field in the first free row of the table.

Select the desired DB tag of a DB of the CPU via the object selection dialog. For the DB tags, see Operand areas and tags (Page 98).

The DB tag is transferred to the table as a data point, the properties and parameters are displayed below.

The table lists all configurable data points.

Configuring data points

- **Name**
Configured name of the data point
- **Tag**
Configured name of the DB variable
- **Data type**
Configured data type of the data point
For the supported data types, see Data types (Page 100).
- **Trigger**
For information on the configuration, see Trigger (Page 101).

4.15.3.3 Data types

Supported data types

The table lists the configurable data types.

If needed, check whether the data types are supported by your broker.

<DATAPOINT_TYPE> indicates the data type on publication. For the publication of the payload and the tag, <DATAPOINT_TYPE> see section Payload formats (Page 106).

Table 4-1 Data types available for Cloud access

S7 data types (bits)	<DATAPOINT_TYPE>	Remarks
BOOL (1)	BOOL	Values transferred: 0, 1
BYTE (8)	UINT8	
CHAR (8)	CHAR	No WCHAR
USINT (8)	UINT8	
INT (16)	INT16	
UINT (16)	UINT16	
WORD (16)	UINT16	
REAL (32)	SINGLE_FLOAT	
DWORD (32)	UINT32	
DINT (32)	INT32	
UDINT (32)	UINT32	
LREAL (64)	DOUBLE_FLOAT	
STRING (2..256 Char)	S7_STRING	No WSTRING
DATE_AND_TIME (64)	S7_DT	
DTL (96)	S7_DTL	

4.15.3.4 Trigger

Time and volume of the transmitted data

Requirements for the transmission of data to the cloud

The following conditions must be met to transfer a value:

- The data point is assigned to a topic in the configuration.
- At least one trigger condition is met.

Time of transfer

You specify the time when the values of data points are transferred to the broker for each data point with the "Trigger".

When configuring a value trigger and a time trigger, both have equal rights. As soon as one of the two trigger conditions is met, the transfer is triggered.

Volume of transferred data

The values of all data points of the topic are transferred to the broker as soon as the value of a data point is pending for transfer.

Duration of transfer (value trigger)

Note

Volume of the transferred data

Note that the settings for all triggers have an effect on the amount of data transferred.

Value trigger

The data of a topic is transferred as long as the trigger condition is fulfilled.

Value trigger + time trigger

Different value triggers and an additional time trigger each initiate the transfer of the entire topic.

Note

Transfer in "Scan cycle of variables"

When the trigger condition of a value trigger is met, the data is transferred to the broker with each scan cycle of variables.

You configure the "Scan cycle of variables" on the CP in the parameter group "Security > CloudConnect > ", see section "CloudConnect" parameter group (Page 94).

Trigger

You use the triggers to specify the conditions that initiate transmission of the saved value to the Cloud or the broker.

The following trigger types are available:

- **Time trigger**
A time trigger is applied to all data points of the topic.
The time trigger is configured in the properties dialog of the topic.
The following types of triggers are available:
 - Cyclic
 - Time (daily / weekly / monthly)

Note

Time trigger with migration of the CP V1.0

Projects from predecessor versions that contain the CP with firmware version 1.0 demonstrate the following behavior for the time trigger with migration of the CP to firmware version 1.1:

Time triggers of the data points configured in predecessor versions are transferred to the topic with CP V1.1. If multiple time triggers were configured in a topic, the first found time trigger is applied.

- **Value trigger**
One value trigger can be configured for each tag:
The following types of triggers are available:
 - Deviation (transfer on deviation)
 - Threshold LOW / Threshold HIGH
 - Range inside / Range outsideSee below for the meaning.

Trigger types

Time trigger

- Cyclic
Cyclic transmission - configurable in milliseconds
The value is transmitted cyclically.
- Once daily
The value is transferred once a day at the configured time.
- Once weekly
The value is transferred once a week.
- Once monthly
The value is transferred once a month.
Note:
If a month has fewer days than the configured day (e.g. the 31st), no value is transferred at the end of the month.

Value trigger

For all value triggers, note the value range of the data type of the respective data point. The respective trigger value is configured depending on the value range.

- **Deviation**
The value is transferred as soon as it deviates by the configured amount from the last value stored in the CPU.
The transfer is triggered on occurrence of the following conditions:
 - New value > (last saved value + positive deviation)
 - New value < (last saved value - positive deviation)
 - New value > (last saved value - negative deviation)
 - New value < (last saved value + negative deviation)
- **Threshold LOW**
The value is transferred as soon as it drops below the configured value.
The transfer is triggered on occurrence of the following conditions:
 - New value < configured threshold LOW
- **Threshold HIGH**
The value is transferred as soon as it exceeds the configured value.
The transfer is triggered on occurrence of the following conditions:
 - New value > configured threshold HIGH
- **Range within**
The value is transferred as soon as it is inside the configured range.
The transfer is triggered on occurrence of the following conditions:
 - Low range limit < New value < High range limit
- **Range outside**
The value is transferred as soon as it is outside the configured range.
The transfer is triggered on occurrence of the following conditions:
 - Low range limit > New value
 - High range limit < New value

The value ranges of the value triggers depend on the data type of the data point.

Data and trigger types

Not every data type supports all the trigger types. The table lists the configurable data types and specifies the supported trigger types for each data type.

Meaning of the symbols:

- +: Supported
- -: Not supported

Table 4-2 Trigger support of data types

S7 data type type (bits / bytes)	Supported triggers	
	Time trigger	Value trigger
Bool (1)	+	x (only value 0)
Byte (8)	+	+
Char (8)	+	+
USInt (8)	+	+
Int (16)	+	+
UInt (16)	+	+
Word (16)	+	+
Real (32)	+	+
DWord (32)	+	+
DInt (32)	+	+
UDInt (32)	+	+
LReal (64)	+	+
String (2..256 Char)	+	-
Date_And_Time (8)	+	-
DTL (12)	+	-

Value ranges of the data types

Threshold values are configured for the trigger types "Deviation", "Threshold LOW", "Threshold HIGH", "Range within" and "Range outside".

The most important data types that are suitable for threshold triggers have the following value ranges:

- Bool: 0 / 1
- Byte: 0...255 / -128...+127
- Char: 0...255
- USInt: 0...255
- Int: -32768...+32767
- UInt: 0...65535
- Word: -32768...+32767 / 0...65535
- DInt: -2147483648...+2147483647
- UDInt: 0...4294967295
- DWord: -2147483647...+2147483647 / 0...4294967295
- Real: +1.175495e-38...+3.402823e+38
- LReal: +12.2250738585072014e-308...+1.7976931348623157e+308

Value ranges of S7 analog input modules

With a positive integer (Int: 0...32767), 270 corresponds to about 1% of the raw value of an S7 analog input module (27648 = 100%).

4.15.3.5 Payload formats

Compatibility between CPs with firmware version V1.0 and V1.1

If you use the Subscriber function of the CP with firmware version V1.1, you can use the publisher data (JSON) of a CP with firmware version V1.0 for subscribing data.

Payload format

Different cloud systems use different formats when transferring user data. The CP outputs the user data in the following formats, depending on the connected cloud system ("Cloud provider" parameter):

- MindConnect IoT Extension
(not used)
- JSON
Default format
Cloud services that expect JSON format for processing topics.
- XML
(not used)
- Free format
If this option is selected, the text box is cleared and can be edited.

The CP uses the UTF-8 character encoding for formatting the user data.

Payload format "JSON"

```
{
  "Timestamp" : "{{PUBLISH_TIMESTAMP}}",
  "DataItems" : [
    {
      "Variable" : "{{Pub_data point_1.NAME}}",
      "Type" : "{{Pub_data point_1.TYPE}}",
      "Value" : "{{Pub_data point_1.VALUE}}",
      "QualityCode" : "{{Pub_data point_1.QUALITY_CODE}}"
    },
    {
      "Variable" : "{{Pub_data point_2.NAME}}",
      "Type" : "{{Pub_data point_2.TYPE}}",
      "Value" : "{{Pub_data point_2.VALUE}}",
      "QualityCode" : "{{Pub_data point_2.QUALITY_CODE}}"
    }
  ]
}
```

Code components

The code for formatting the user data consists of the components listed below.

The following description of the individual code components is structured as follows:

- **Code component**
 - <Syntax>
 - Meaning
 - Examples (not for all components)

Code components: Syntax and meaning

- **Time stamp**
 - {{PUBLISH_TIMESTAMP}}
 - Meaning: Time of the publication
 - Example:
 - Syntax: "{{PUBLISH_TIMESTAMP}}"
 - Results in string: "2018-08-20T13:58:16.192313634+00:00"
- **Data point / Variable**
 - {{Pub_data_point_n.NAME}}
 - Name of the data point
- **Value**
 - {{Pub_data_point_n.VALUE}}
 - Value of the data point
- **Data type**
 - {{Pub_data_point_n.TYPE}}
 - Data type of the data point output by the device
 - For the output of the data types, see section Operand areas and tags (Page 98).
- **QualityCode**
 - {{Pub_data_point_n.QUALITY_CODE}}
 - Quality status of the value
 - See below for the meaning.

Sequences not permitted in the payload content

The following sequences are not permitted in the payload content:

- {{#
- {{^
- {{/
- {{>
- {{&
- {{{

Example of transferred payload (JSON)

Below you will find an example of the transferred user data of a topic.

The topic contains three variables of an S7 station for the data points "DP1", "DP2" and "DP3".

The value of the "DataItems" key is an array with the objects of the three variables.

```
{
  "Timestamp" : "{{PUBLISH_TIMESTAMP}}",
  "DataItems" : [
    {
      "Variable" : "{{DP1.NAME}}",
      "Type" : "{{DP1.TYPE}}",
      "Value" : "{{DP1.VALUE}}",
      "QualityCode" : "{{DP1.QUALITY_CODE}}"
    },
    {
      "Variable" : "{{DP2.NAME}}",
      "Type" : "{{DP2.TYPE}}",
      "Value" : "{{DP2.VALUE}}",
      "QualityCode" : "{{DP2.QUALITY_CODE}}"
    },
    {
      "Variable" : "{{DP3.NAME}}",
      "Type" : "{{DP3.TYPE}}",
      "Value" : "{{DP3.VALUE}}",
      "QualityCode" : "{{DP3.QUALITY_CODE}}"
    }
  ]
}
```

Escape sequences

Escape sequences which adapt the code according to the protocol used can be used to convert certain special characters.

Special characters can occur within the following name components, for example:

- Station name
- Topic name

The following escape sequences are supported by the CP:

- JSON PubSub
Standard JSON escape sequences
For the escape sequences used, see JSON escape sequences (Page 119).
- XML
Standard XML escape sequences
- CSV
Standard CSV escape sequences

The publisher converts the respective special characters into escape sequences.

For the subscriber, the escape sequences are converted into the reverse direction.

QualityCode

Transmission and QualityCode

The "QualityCode" quality status of a data point is also transferred with the user data. The status indicates the validity of the value.

The status is set by the CP as a publisher and has the following value range:

- GOOD
The value is valid.
- BAD
The value of the variable is not valid or not current. Possible causes:
 - CPU in STOP
 - Value not current
 - Error while reading the variable

The value of the status has the following effect on the transmission:

- Publisher → Cloud
The publication of CP messages as a publisher is independent of the value of the status.
- Cloud → Subscriber
The receipt of messages by the CP as a subscriber is independent of the value of the status. However, when a message with the status "BAD" is received, the value is not written to the CPU by the CP as subscriber.

4.15.3.6 Import / export of payload

Editing the payload format outside STEP 7

If you want to define the format of your payload outside STEP 7 or if you want to continue using or editing the format defined in the STEP 7 project, you can import and export the format.

You can import/export the data in XML format.

Exporting and importing payload

Proceed as follows to export/import:

1. Expand the project tree:
Station > Local modules > CP
2. Select the "Cloud connection" entry.
3. In the shortcut menu, click on "Export CloudConnect Data" or "Import CloudConnect data".
The window for importing or exporting the file in *.XML format is opened.

Notes:

- When you omit an optional element/attribute, it will receive the respective default value.
- If the *.XML file contains invalid entries, a corresponding error message is displayed.
- Only published topics (and possibly subscribed topics) may be present.
Topics may not be imported or exported at the same time.
- For you to import tags into data points, the tags must be available in the CPU of the target device.
If the tag name contained in the XML file is not found during the import, the respective field will remain empty after the import. To still be able to use the data point, you must select a tag for the data point.

Note

No syntax check

Imported user data files are not checked for syntax errors by STEP 7 or the CP. An incorrect syntax can prevent cloud communication.

If you edit the user data yourself, then pay close attention to the correctness of the syntax.

XML syntax and permitted values

Syntax	Element / Attribute	Permissible data types / value range	Meaning / remark
<PublishedTopics>			
<General Comment>	• Comment • Author • Name	• String • String • String	• Optional • Optional • Required
<QoS>		Integer / 0...2	Optional

Syntax	Element / Attribute	Permissible data types / value range	Meaning / remark
<code><TimeTrigger></code> <code><Cyclic></code> or <code><TimeTrigger></code> <code><Date></code>	- CycleTime - Frequency - TimeOfTheDay - Weekday - DayOfTheMonth	- Integer / 10...4294967295 ms - String / Daily, Weekly, Monthly - Integer / 0...1439 minutes (00:00 ... 23:59) - String / Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday - Integer / 1...31	- Required for element <code>TimeTrigger > Cyclic</code> - Required for element <code>TimeTrigger > Date</code> - Optional - Optional - Optional
<code><DataPoints></code> <code><DataPoint></code> <code><General Name></code> <code><DataPoints></code> <code><DataPoint></code> <code><General> <Tag></code>	Name	- String - String	- Required - Optional
<code><DataPoints></code> <code><DataPoint></code> <code><ValueTrigger></code>	- Type - Value - RangeLow - RangeHigh	- String / Deviation, Lower Threshold, Upper Threshold, Outside Range, Inside Range - String - String - String	- Required for element <code>ValueTrigger</code> - Optional - Optional - Optional
<code><Payload></code>	- Format - Customize	- String / XML, JSON, Custom - Bool / true, false <code><![CDATA[Contents]]></code> To allow content, see section Payload formats (Page 106).	- Required - Optional - Optional
<code><SubscribedTopics></code>			
<code><General></code>	- Comment - Author - Name	- String - String - String	- Optional - Optional - Required
<code><QoS></code>		Integer / 0...2	Optional
<code><DataPoints></code> <code><DataPoint></code> <code><General></code> <code><DataPoints></code> <code><DataPoint></code> <code><General> <Tag></code>	Name	- String - String	- Required - Optional

XML structure with example values

```

<?xml version="1.0" encoding="UTF-8"?>
<CloudConnectData>
  <PublishedTopics>

```

```

<PublishedTopic>
  <General Name="Published Topic_1" Author="Ben Utzer"
    Comment="My published topic"/>
  <QoS>1</QoS>
  <TimeTrigger>
    <Date Frequency="Daily" TimeOfDay="720"/>
  </TimeTrigger>
  <DataPoints>
    <DataPoint>
      <General Name="Published_datapoint_1">
        <Tag>"Data_block_1"."Enabled"</Tag>
      </General>
    </DataPoint>
    <DataPoint>
      <General Name="Published_datapoint_2">
        <Tag>"Data_block_1"."LastStatusMsg"</Tag>
      </General>
    </DataPoint>
    <DataPoint>
      <General Name="Published_datapoint_3">
        <Tag>"Data_block_1"."ErrorCount"</Tag>
      </General>
      <ValueTrigger Type="Deviation" Value="1"/>
    </DataPoint>
  </DataPoints>
  <Payload Format="XML" Customize="true">
    <![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<root>
  <!-- Custom plant identification number -->
  <MyCustomXMLTag>0123456789</MyCustomXMLTag>
<DataItems>
  <DataItem>
    <Variable>{{Published_datapoint_1.NAME}}</Variable>
    <Type>{{Published_datapoint_1.TYPE}}</Type>
    <Value>{{Published_datapoint_1.VALUE}}</Value>

```

```
</DataItem>
<DataItem>
  <Variable>{{Published_datapoint_2.NAME}}</Variable>
  <Type>{{Published_datapoint_2.TYPE}}</Type>
  <Value>{{Published_datapoint_2.VALUE}}</Value>
</DataItem>
<DataItem>
  <Variable>{{Published_datapoint_3.NAME}}</Variable>
  <Type>{{Published_datapoint_3.TYPE}}</Type>
  <Value>{{Published_datapoint_3.VALUE}}</Value>
  <QualityCode>{{Published_datapoint_3.QUALITY_CODE}}</QualityCode>
</DataItem>
</DataItems>
</root>]]>
  </Payload>
</PublishedTopic>
<PublishedTopic>
  <General Name="Published Topic_2" Author="Ben Utzer"
    Comment="Another published topic"/>
  <QoS>2</QoS>
  <TimeTrigger>
    <Cyclic CycleTime="500"/>
  </TimeTrigger>
  <DataPoints>
    <DataPoint>
      <General Name="Published_datapoint_1">
        <Tag>"Data_block_1"."Actuation_Speed"</Tag>
      </General>
      <ValueTrigger Type="Inside Range" RangeLow="150"
        RangeHigh="300"/>
    </DataPoint>
    <DataPoint>
      <General Name="Published_datapoint_2">
        <Tag>"Data_block_1"."X-Position"</Tag>
      </General>
    </DataPoint>
  </DataPoints>
</PublishedTopic>
```

```

        <ValueTrigger Type="Outside Range" RangeLow="0"
RangeHigh="200"/>
    </DataPoint>
</DataPoints>
    <Payload Format="XML"/>
</PublishedTopic>
<PublishedTopic>
    <General Name="Published Topic_3" Author="Ben Utzer"
        Comment="Yet another published topic"/>
    <QoS>0</QoS>
    <TimeTrigger>
        <Date Frequency="Weekly" Weekday="Wednesday"/>
    </TimeTrigger>
    <DataPoints>
        <DataPoint>
            <General Name="Published_datapoint_1">
                <Tag>"Data_block_2"."ManufacturedItems"</Tag>
            </General>
            <ValueTrigger Type="Lower Threshold" Value="50"/>
        </DataPoint>
        <DataPoint>
            <General Name="Published_datapoint_2">
                <Tag>"Data_block_1"."RejectedQuality"</Tag>
            </General>
            <ValueTrigger Type="Upper Threshold" Value="3"/>
        </DataPoint>
    </DataPoints>
</PublishedTopic>
</PublishedTopics>
<SubscribedTopics>
    <SubscribedTopic>
        <General Name="Subscribed Topic_3" Author="Ben Utzer"
            Comment="My subscribed topic"/>
        <QoS>2</QoS>
        <DataPoints>
            <DataPoint>

```

```
<General Name="Subscribed_datapoint_1">
  <Tag>"Data_block_2"."In_Storage"</Tag>
</General>
</DataPoint>
<DataPoint>
  <General Name="Subscribed_datapoint_2">
    <Tag>"Data_block_2"."Required"</Tag>
  </General>
</DataPoint>
</DataPoints>
</SubscribedTopic>
</SubscribedTopics>
</CloudConnectData>
```

4.15.4 Properties dialog of the topics

4.15.4.1 Opening the properties dialog

When you open the CP in the navigation area below the local modules, the properties dialog may be opened in two ways:

- When selecting a topic via the shortcut menu (right click)
- When the Topic editor is open, use the "Properties" button above the data point table

The following parameter groups are available:

- General
- Quality of Service (QoS)
For information on the configuration, refer to section Quality of Service (QoS) (Page 116).
- Trigger
A time trigger is applied to all data points of the topic.
For configuration of the Time trigger, see section Trigger (Page 101).

4.15.4.2 Quality of Service (QoS)

Properties of a topic - Quality of Service (QoS)

The parameter becomes accessible when you expand the CP in the navigation area under the local modules and open the properties dialog of a topic via the shortcut menu.

- **Required Quality of Service (QoS)**

This is where you define the desired transmission behavior (Quality of Service) of this topic. The configured value should be fulfilled by the broker if possible. Check which reaction is performed by the broker you use if it does not meet the required QoS level. Some brokers select the level closest to the required level in this case. Other brokers output an error message.

- QoS 0

Transfer no more than once

The CP sends the topic once to the broker. The CP does not expect an acknowledgment. If the topic is not received by the broker, it is lost.

- QoS 1

Transfer at least once

The CP sends the topic to the broker until it receives a PUBACK packet as acknowledgment from the broker.

- QoS 2

Transfer exactly once

The CP sends the topic and waits until it receives the two-step acknowledgment from the broker as specified.

This version represents the highest level of quality, but it is also associated with the highest administrative burden for the client as well as the server.

Default setting: 0

4.15.5 Additional information

4.15.5.1 Connection abort and data buffering

Reaction of the CP to connection aborts

The response to connection aborts is as follows:

- **Connection abort between CP and CPU (CPU in STOP)**
 - During the connection abort:
The CP publishes messages with empty strings for the values and the QualityCode "BAD".
 - After the connection has returned:
When the trigger condition is met, the CP publishes messages with current values and the QualityCode "GOOD".
- **Connection abort between CP and cloud - cable pulled on CP**
 - During the connection abort:
The CP does not publish any messages.
 - After the connection has returned:
For information on the behavior, see the following section.
- **Connection abort between CP and cloud - cloud server not reachable**
For information on the behavior, see the following section.

Response to connection abort depending on the QoS value

The response of the CP to an aborted connection with the cloud server depends on the configured QoS value.

- QoS = 0
 - During the connection abort:
The CP publishes messages with the current values.
After each time a message is sent, the CP starts the "Keepalive interval" to monitor the connection with the broker. If the CP does not receive a packet from the CP within this monitoring time, it sends a PINGREQ packet to the broker.
If the CP does not receive a PINGRESP packet from the broker, it terminates the connection after 1.5 times the keepalive interval. The CP then attempts to establish the connection again.
The CP does not buffer any published messages.
 - After the connection has returned:
The CP publishes messages with the current values.
- QoS = 1 / 2
 - During the connection abort:
The CP publishes messages with current values and waits for acknowledgments from the broker for each message. The CP only deletes published messages from its send buffer after acknowledgment from the broker.
Depending on the QoS value that the broker uses, it sends the following acknowledgments:
 - QoS = 1: PUBACK
 - QoS = 2: PUBREC + PUBRELIf the CP does not receive an acknowledgment from the broker for any of the most recently published messages (max. 16), it does not send any further messages.
If the CP does not receive a packet from the broker within the monitoring time (keepalive interval), it sends a PINGREQ packet to the broker. If the CP does not receive a PINGRESP packet from the broker, it terminates the connection after 1.5 times the keepalive interval. The CP then attempts to establish the connection again.
 - After the connection has returned:
After the connection is re-established, the CP waits for the acknowledgments still pending.
After the acknowledgments are received, the CP first publishes the messages from the frame memory and then the newly accumulated messages.

Data buffering in the frame memory

The CP saves accumulating messages that have not yet been published in its frame memory. This has a capacity of 3500 messages.

The frame memory operates chronologically; in other words, the oldest data is sent first (FIFO principle). When the maximum capacity is exceeded, the oldest messages are overwritten.

4.15.5.2 JSON escape sequences

JSON escape sequences

When using the JSON format for the payload, the following characters are converted into escape sequences by the CP as a publisher.

With the CP as a subscriber, the escape sequences are converted in the reverse direction.

Characters	JSON escape sequence	Note
\n	\\n	New line *
\r	\\r	Line break *
\t	\\t	Tab *
\"	\\"	Quotation marks
\\	\\\\	Double backslash
\\u0000	\\u0000	
\\u0001	\\u0001	
\\u0002	\\u0002	
\\u0003	\\u0003	
\\u0004	\\u0004	
\\u0005	\\u0005	
\\u0006	\\u0006	
\\u0007	\\u0007	
\\b	\\u0008	
\\t	\\u0009	
\\n	\\u000A	
\\u000b	\\u000B	
\\f	\\u000C	
\\r	\\u000D	
\\u000e	\\u000E	
\\u000f	\\u000f	
\\u0010	\\u0010	
\\u0011	\\u0011	
\\u0012	\\u0012	
\\u0013	\\u0013	
\\u0014	\\u0014	
\\u0015	\\u0015	
\\u0016	\\u0016	
\\u0017	\\u0017	
\\u0018	\\u0018	
\\u0019	\\u0019	
\\u001a	\\u001a	
\\u001b	\\u001b	
\\u001c	\\u001c	
\\u001d	\\u001d	

Characters	JSON escape sequence	Note
\u001e	\\u001e	
\u001f	\\u001f	
\u007F	\\u007F	

* Not configurable in STEP 7 as name component

4.15.5.3 Permitted Characters

Characters not allowed for names

The following characters are not permitted for names:

- 0x22 (")
Quotation marks are generally not permitted.
- 0x20 (SP)
Spaces are allowed within most names. Exception: CloudConnect data point
Leading and trailing spaces are automatically deleted.

Permitted characters

See below for ASCII character sets.

Parameter	Characters	Number of characters
Name of: • DB variable *	Permitted characters: • Standard characters (numbers, letters) • Special characters 0x21 .. 0x7E • Special characters $\geq$ 0x80	
CloudConnect * • Data point name	Permitted characters: • Standard characters (numbers, letters) • Special characters $\geq$ 0x80 • Special characters 0x21 .. 0x60 with exceptions The following are not permitted: • Space • ! / . < > ^ \ # ! & = { } • Tabs The following strings are also not permitted: • PUBLISH_TIMESTAMP • DATAPOINT_ARRAY • GROUP	

Parameter	Characters	Number of characters
CloudConnect * • Topic name	Permitted characters: - Standard characters (numbers, letters) - Special characters $\geq 0x80$ - Special characters $0x21 \dots 0x7E$ with exceptions The following are not permitted: # + / \$ as first character in the name	
Name of: - NTP server - Host - S7 station, CPU, CP	Permitted characters according to RFC1035 and RFC1123: - Standard characters (numbers, letters) No station names with digits only $0x2D$ (-) .. $0x2E$ (.)	
User names, passwords	Permitted characters: - Standard characters (numbers, letters) - Following special characters: $0x2D$ (-) $0x2E$ (.) $0x40$ (@) $0x5F$ (_)	

* Cloud messages in JSON format: The escape sequences of the JSON standard apply to special characters in station names, topic names and data point names.

ASCII character sets

The ASCII characters are listed with their hexadecimal code and the corresponding characters.

Standard characters

- 0x30 .. 0x39**
0 1 2 3 4 5 6 7 8 9
- 0x41 .. 0x5A**
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

Special characters < 0x80

- 0x21 .. 0x2F**
! " # \$ % & ' () * + , - . /
- 0x3A .. 0x40**
: ; < = > ? @

- **0x5B .. 0x60**
[\] ^ _ `
- **0x7B .. 0x7E**
{ | } ~

Special characters ≥ 0x80 (ISO/IEC 8859-1)

- **0x80, 0x82 .. 0x89, 0x8A .. 0x8C, 0x8E, 0x91 .. 0x9C, 0x9E .. 0x9F**
€ , f „ ... † ‡ ^ % ¢ Š ‹ Œ Ž ‘ ’ “ ” • – — ~ ™ š › œ ž Ÿ
- **0xA1 .. 0xAC, 0xAE .. 0xB5, 0xB8 .. 0xBF**
ı ¢ £ ¤ ¥ ¦ § ¨ © ª « ¬ ® ¯ ° ± ² ³ ´ µ ¶ · ¸ ¹ º » ¼ ½ ¾ ¿
- **0xC0 .. 0xFF**
À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ
ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

Program blocks

5.1 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

You can use the instructions (program blocks) listed below for direct communication between S7 stations.

In contrast to other communication types, Open User Communication does not need to be enabled in the configuration of the CP because corresponding program blocks need to be created for this. You will find details on the program blocks in the information system of STEP 7.

Note

Different program block versions

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

Requirements for Secure OUC

Requirements for the use of the secure transmission via Secure OUC:

- STEP 7: As of V16
- CPU firmware: As of V4.4
- CP firmware: As of V3.2

Supported program blocks for OUC

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

- **TSEND_C V3.0 / TRCV_C V3.0**
Compact blocks for:
 - Connection establishment/termination and sending data
 - Connection establishment/termination and receiving data

As an alternative, use:

- **TCON V4.0 / TDISCON V2.1**
Connection establishment / connection termination
- **TUSEND V4.0 / TURCV V4.0**
Sending and receiving data via UDP

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

Sending and receiving data via TCP or ISOonTCP

- **TMAIL_C V4.0**

Sending e-mails

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

Note

Personal data unencrypted in TMAIL_C

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

For changing configuration data of the CP during runtime:

- **T_CONFIG V1.0**

Program-controlled configuration of the 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 126).

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
- **TMail_V6**
For transferring e-mails addressing the e-mail server using an IPv6 address
- **TMail_FQDN**
For transferring e-mails addressing the e-mail server using its name (FQDN)
- **TCON_IP_V4_SEC**
For the secure transfer of data via TCP
- **TCON_QDN_SEC**
For the secure transfer of data via the host name
- **TMail_V4_SEC**
For secure transfer of e-mails addressing the e-mail server using an IPv4 address
- **TMail_V6_SEC**
For secure transfer of e-mails addressing the e-mail server using an IPv6 address
- **TMail_QDN_SEC**
For secure transfer of e-mails addressing the e-mail server using the host name

Note on TMail_Vx_SEC / TMail_QDN_SEC:

With these SDTs, the mail server certificate is checked, but not the ID of the "TLSServerCertRef" (STEP 7 internal reference) certificate.

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

Connection establishment and termination

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

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

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

Note

Connection abort

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

5.2 Changing the IP address during runtime

Changing address parameters during runtime via T_CONFIG

Using the T_CONFIG block, you can change the following address parameters program-controlled during runtime:

- IP address of the CP
- Subnet mask of the CP
- Router address of the CP
- Address parameters of DNS servers (IF_CONF_DNS)
- Address parameters of NTP servers (IF_CONF_NTP)

Requirement in the CP configuration

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

Note

Changing the IP parameters with a dynamic IP address

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

Program blocks / STEP 7 versions

Program-controlled changing of the IP parameters is supported by the T_CONFIG program block, which accesses address data stored in a suitable system data type (SDT).

You can use T_CONFIG together with the following system data types (SDTs):

- IF_CONF_V4
- IF_CONF_V6
- IF_CONF_DNS
- IF_CONF_NTP

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.

Requirements

STEP 7 version

You can use T_CONFIG as of STEP 7 Basic V14.

Configured IP address

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.

Firmware version

Requirements for program-controlled changing of the IP parameters are as follows:

- CP firmware $\geq$ V2.1.7x
and
- CPU firmware $\geq$ V4.2

Diagnostics and upkeep

WARNING

Cleaning the housing

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

Do not use any liquids or solvents.



CAUTION

Hot surfaces

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

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

6.1 Diagnostics options

The following diagnostics options are available:

LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 30).

If there are connection problems between the master station and station, you can, for example see whether or not the transmission path is disturbed or whether the CPU is in STOP status by checking the LEDs.

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

If you access the CP via Ethernet, you obtain the following information about the selected module:

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

Access via WAN networks does not provide any information.

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

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

If you want to operate online diagnostics with the station via the CP, you need to select the type of communication "Enable online functions"; see section Communication types (Page 53).

"Diagnostics" group

The diagnostics pages are divided into the following groups:

- **General**
This group displays general information on the module.
- **Diagnostics status**
This group displays status information of the module from the view of the CPU.
 - Device-specific events
Information on internal module events is displayed here.
- **Ethernet interface**
Address and statistical information
- **Industrial Remote Communication**
The group has the following diagnostics pages:
 - Partner
Information about the address settings of the partner, connection statistics, configuration data of the partner and other diagnostics information.
 - Data point list
Various information on the data points such as configuration data, value, connection status etc.
 - Protocol diagnostics
With the button "Enable protocol trace", the frames received and sent by the module are logged for several seconds.
With the function "Disable protocol trace", the logging is stopped and the data is written to a log file.
With the function "Save", you can save the log file on the engineering station and then analyze it.

- **Time of day**
Information on the time on the device
- **Security**
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

- **Firmware update**
For a description, see section Downloading firmware (Page 137).
- **Assign IP address**
- **Assign PROFINET device name**
- **Save service data**
The function is used for logging of internal module processes in situations in which you cannot eliminate unexpected or unwanted behavior of the module yourself.
The log file is created with the "Save service data" button. The data is saved in a file with the format "*.dmp" that can be evaluated by the Siemens hotline.

Diagnostics e-mail

If configurable events such as a CPU STOP occur, the CP can send a diagnostics e-mail. For information on configuration, see "Messages".

Partner status

When using telecontrol communication, the CP can signal the status of the connection to the communications partner to the CPU via a variable. You can display the status of the variable via the Web server of the CPU. You configure the variable in the parameter group "Communication with the CPU".

STEP 7 V5

Here, the known diagnostics tools are available to you.

When accessing via WAN networks, you can use the functions of PG routing. You will find details in the SINAUT system manual volume 2; see /3/ SINAUT ST7 system manual (Page 174).

Diagnostics options via the Web server of the CPU

You will find details on the diagnostics options of the Web server in the S7-1200 system manual, see /1/ S7-1200 system manual (Page 173).

6.2 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.

6.3 Online security diagnostics via port 8448 of the CP

Security diagnostics via port 8448

Requirements:

- With an activated firewall, access must be enabled.

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

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

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

For more information, refer to section Settings for online security diagnostics and downloading to station with the firewall activated (Page 67).

6.4 SNMP

SNMP (Simple Network Management Protocol)

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

The information on the properties of SNMP-compliant devices is 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:

- Address 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 /9/ SNMP (Page 175).

Configuration

For information on the configuration, refer to:

- With security functions disabled (SNMPv1): SNMP (Page 65)
- With security functions enabled (SNMPv1 / SNMPv3): SNMP (Page 76)

6.5 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 6-1 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 6-2 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.
8411	Sending the e-mail failed. Cause: There was not enough memory space for sending.

Status	Meaning
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.

6.6 Downloading firmware

New firmware versions of the CP

If a new firmware version is available for the module, you will find this on the Internet pages of Siemens Industry Online Support under the following address:
LEDs (Page 30)

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 Link:
(<https://support.industry.siemens.com/cs/ww/en/ps/21162/dl>).

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.

6.7 Module replacement

Module replacement



CAUTION

Read the system manual "S7-1200 Programmable Controller"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1200 Programmable Controller" (refer to the documentation in the Appendix).

When installing and connecting up, keep to the procedures described in the system manual "S7-1200 Programmable Controller".

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

The STEP -7 project data of the CP is stored on the local CPU. If there is a fault on the device, this allows simple replacement of the CP without needing to download the project data to the station again.

When the station starts up again, the new CP reads the project data from the CPU.

Technical data

7.1 Technical specifications of the CP

Table 7-1 Technical specifications of the CP 1243-8 IRC

Technical specifications		
Article number	6GK7 243-8RX30-0XE0	
Attachment to Industrial Ethernet		
Quantity	1	
Design	RJ-45 jack	
Properties	100BASE-TX, IEEE 802.3-2005, half duplex/full duplex, autocrossover, autonegotiation, galvanically isolated	
Transmission speed	10/100 Mbps	
Permitted cable lengths (Ethernet)	(Alternative combinations per length range) *	
0 ... 55 m	- Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180 - Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet	
0 ... 85 m	- Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180 - Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet	
0 ... 100 m	- Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180 - Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet	
Electrical data		
External power supply	Power supply	24 VDC
	Permitted range	19.2 ... 28.8 V
	Design	Terminal block with plug, 3 terminals
	Cable cross-section	
	Minimum	0.14 mm² (25 AWG)
	Maximum	1.5 mm² (15 AWG)
	Max- tightening torque of the screw terminals	0.45 Nm (4 lb-in)
	Electrical isolation:	
Power supply unit to internal circuit	710 VDC for 1 minute	
Current consumption (typical)	From 24 VDC (external)	100 mA
	From the S7-1200 backplane bus	250 mA
Effective power loss (typical)	From 24 VDC (external)	2.4 W
	From the S7-1200 backplane bus	1.25 W
Permitted ambient conditions		

7.2 Pin assignment of the socket for the external power supply

Technical specifications		
Ambient temperature	During operation with the rack installed horizontally	-20 °C ... +70 °C
	During operation with the rack installed vertically	-20 °C ... +60 °C
	During storage	-40 °C ... +70 °C
	During transportation	-40 °C ... +70 °C
Relative humidity	During operation	≤ 95 % at 25 °C, no condensation
Design, dimensions and weight		
Module format	Compact module for S7-1200, single width	
Degree of protection	IP20	
Weight	122 g	
Dimensions (W x H x D)	30 x 110 x 75 mm	
Installation options	• 35 mm DIN rail • Switch panel	
Product functions **		

* For details, refer to the IK PI catalog, cabling technology

**You will find further characteristics and performance data in the section Application and functions (Page 13).

7.2 Pin assignment of the socket for the external power supply

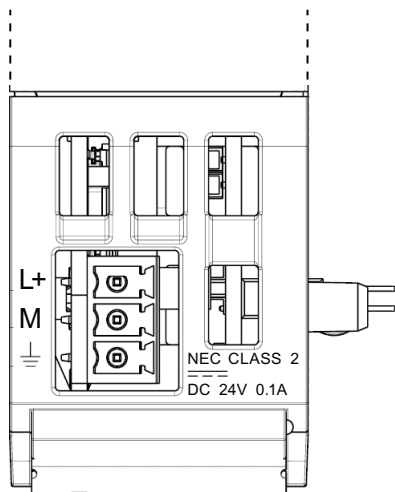


Figure 7-1 Socket for the external 24 VDC power supply (view from above)

Table 7-2 Pin assignment of the socket for the external power supply

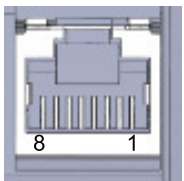
Pin	Labeling	Function
1	L+	+ 24 VDC
2	M	Ground reference for + 24 VDC
3		Ground connector

7.3 Pinout of the Ethernet interface

Pinout of the Ethernet interface

The table below shows the pin assignment of the Ethernet interface. The pin assignment corresponds to the Ethernet standard 802.3-2005, 100BASE-TX version.

Table 7-3 Pin assignment of the Ethernet interface

View of the RJ-45 jack	Pin	Signal name	Assignment
	1	TD	Transmit data +
	2	TD_N	Transmit data -
	3	RD	Receive data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive data -
	7	GND	Ground
	8	GND	Ground

7.3 Pinout of the Ethernet interface

Approvals

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21162/cert>)

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

Address for declarations of conformity

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

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

EC declaration of conformity



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

- **2014/34/EU (ATEX explosion protection directive)**
Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356
- **2014/30/EU (EMC)**
EMC directive of the European Parliament and of the Council of 26 February 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, p. 79-106
- **2011/65/EU (RoHS)**
Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment

UK Declaration of Conformity



Importer UK:

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

The product meets the requirements of the following directives:

- UKEX Regulations
SI 2016/1107 The Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016, and related amendments.
- EMC Regulations
SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related amendments.
- RoHS Regulations
SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

ATEX / IECEx / UKEX / CCC-Ex

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

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

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 38).

The product meets the explosion protection requirements outlined below.

IECEx

Classification: Ex ec IIC T4 Gc, Certificate no.: IECEx DEK 18.0019X

The product meets the requirements of the standards:

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

ATEX

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

The product meets the requirements of the standards:

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

UKEX

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

The product meets the requirements of the standards:

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

Importer UK: Siemens plc (see above)

CCC-Ex

Classification: Ex na IIC T4 Gc, Certificate no.: 2020322310002625

The product meets the requirements of the following standards:

- GB 3836.1
Hazardous areas - Part 0: Equipment - General requirements
- GB 3836.8
Explosive atmospheres - Part 15: Equipment protection by type of protection 'n'

EMC

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

Applied standards:

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

RoHS

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

Applied standard:

- EN IEC 63000

cULus

Underwriters Laboratories Inc. complied with



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

cULus HAZ.LOC.

Underwriters Laboratories Inc. complied with



- UL 1604 (Hazardous Location)
- CSA C22.2 No. 213 (Hazardous Location)

APPROVED for Use in:



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

FM



Factory Mutual Research (FM)

Factory Mutual Approval Standard Class No. 3600, 3611

Approved for use in:

Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C

Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

C-Tick



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

EAC (Eurasian Conformity)



Customs union of Russia, Belarus and Kazakhstan

Declaration of conformity according to the technical regulations of the customs union (TR CU)

MSIP 요구사항 - For Korea only**A급 기기(업무용 방송통신기자재)**

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

Note that in terms of the emission of interference, this device corresponds to limit class A. This device can be used in all areas except for residential environments.

Current approvals

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

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

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21162/cert>)

Overview of the approvals for SIMATIC NET products

You will find an overview of the approvals for SIMATIC NET products including approvals for shipbuilding on the Internet pages of Siemens Industry Online Support under the following address:

Link: (<https://support.industry.siemens.com/cs/attachments/57337426/CertificationOverview.pdf>)

Dimension drawings

All dimensions in the drawings are in millimeters

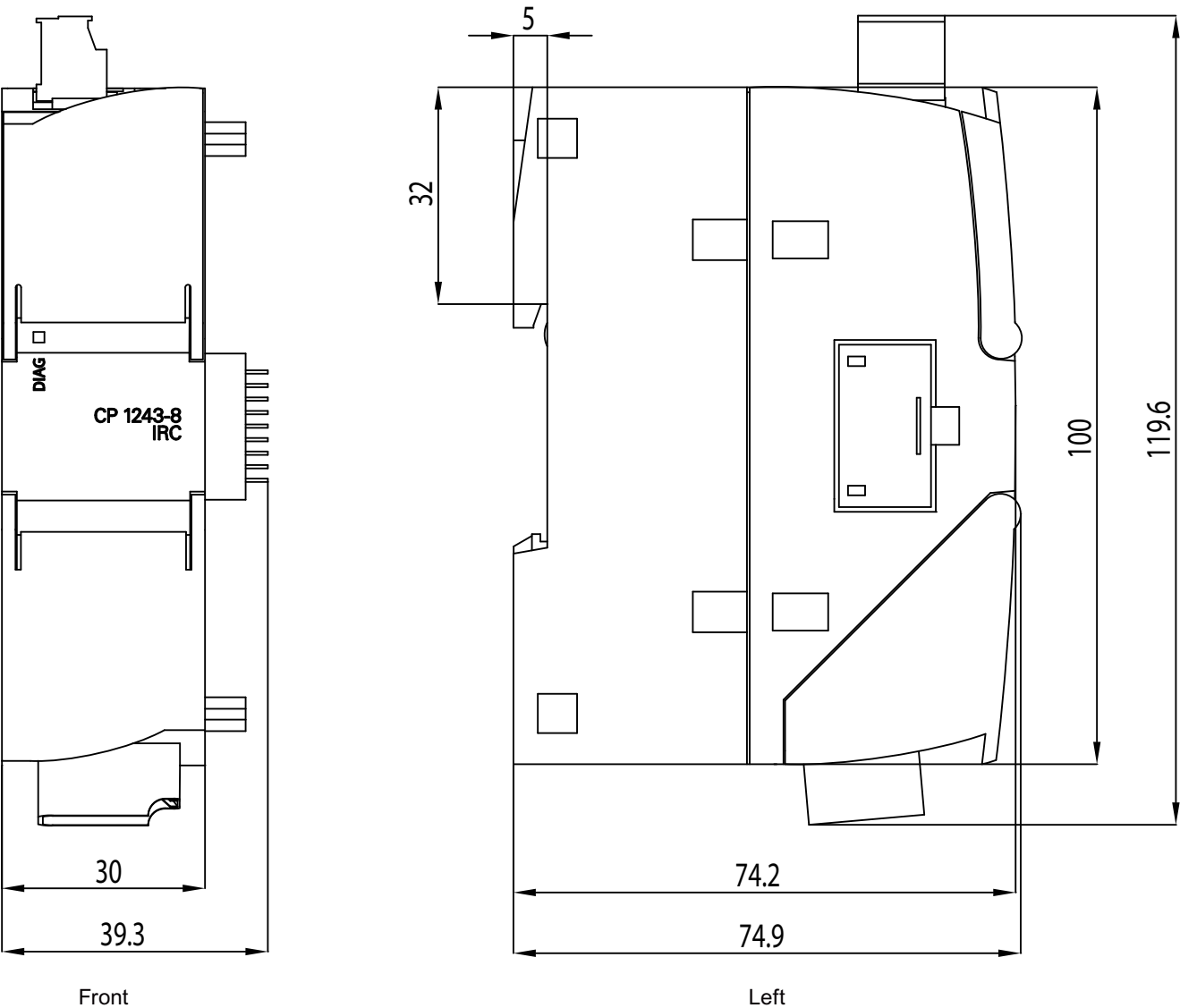


Figure B-1 Front view and side view left

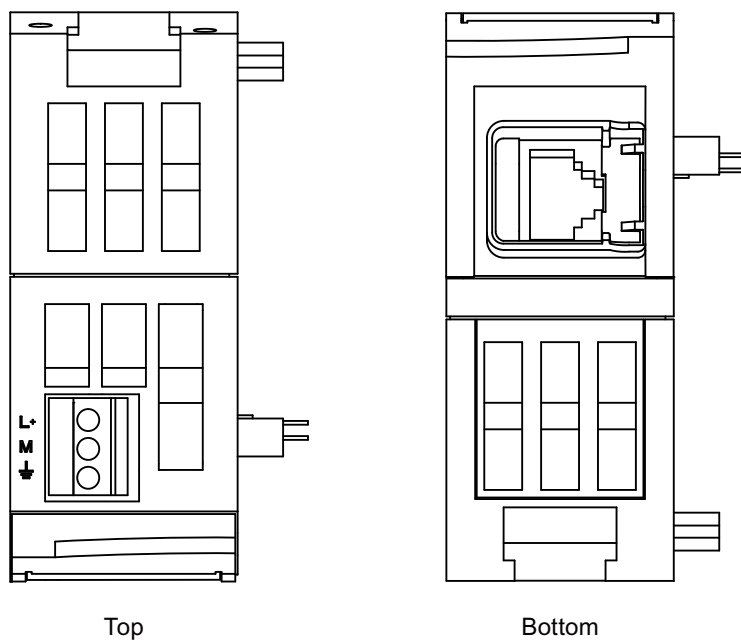


Figure B-2 Top view and view from below

Accessories

C.1 TS modules

C.1.1 The TS modules

Structure of a TS module

The TS modules have the module format of a compact module S7-1200, single width.
You can see the structure of a TS module in the figure.



- ① TS module, here: TS Module Modem
- ② Plug-in connection between TS module and CP
- ③ Interface to the WAN (under the front panel)

Figure C-1 TS module

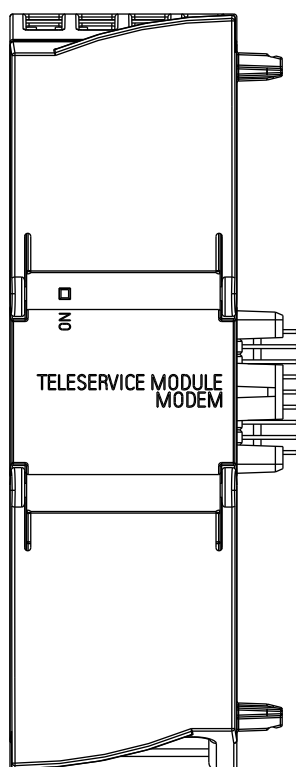


Figure C-2 Drawing of a TS module based on the example of the TS Module Modem

TS modules

The TS modules form the electrical interface to the WAN. The TS modules are supplied with voltage by the CP via the plug-in connection.

The following TS modules exist:

TS module	Article number	Description
TS Module Modem	6ES7 972-0MM00-0XA0	The TS Module Modem contains an analog modem for connection to the analog telephone network.
TS Module RS232	6ES7 972-0MS00-0XA0	The TS Module RS232 has a COM interface (RS-232) for connection of an external modem. The TS module can be used for connection to a dedicated line, among other things.
Mounting rail-adapter	6ES7 972-0SE00-7AA0 6ES7 972-0SE10-7AA0	Adapter for S7 mounting rail (optional for S7-300 rack): 60 mm rail 75 mm rail

You will find a brief description of the TS modules below.

You will find the detailed description and the general technical specifications of the TS modules in the manual, see /8/ TS Adapter (Page 175).

C.1.2 TS Module Modem

Product package

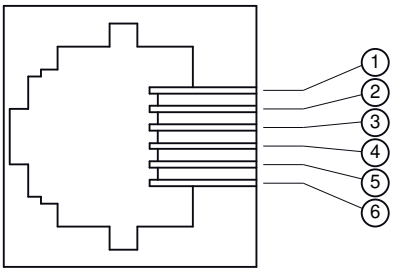
Designation	Article number
TS Module Modem	6ES7 972-0MM00-0XA0
Analog telephone cable with two RJ-11 connectors Length 3 m	A5E00243688
TAE connector	A5E00243701

Properties

The TS Module Modem has an internal analog modem.

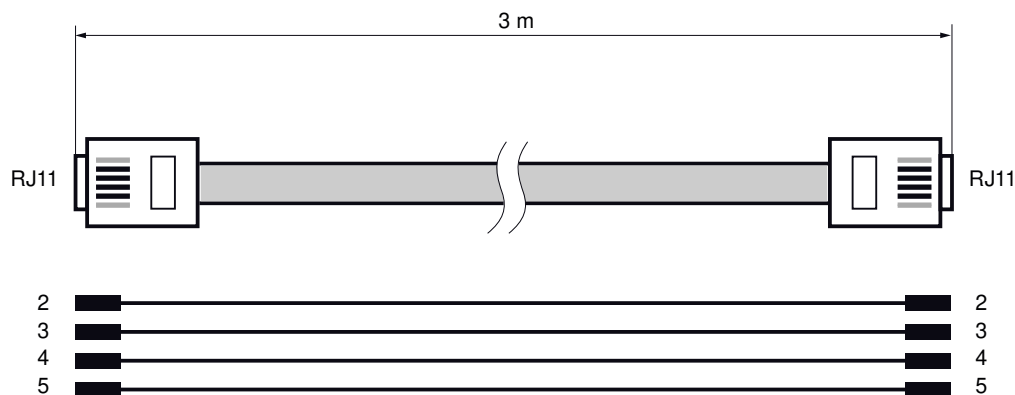
The analog modem port is the 6-pin RJ11 socket behind the lower front panel.

Pin assignment and signal description of analog modem port

Figure	Pin no.	Signal name	Signal direction	Comments
	1	-		
	2	-		
	3	b1	Bi-directional	Incoming wire pair
	4	a1		
	5	-		
	6	-		

Analog phone cable

Using the supplied analog phone cable, you connect the RJ11-socket to a phone socket.



Note

Use the supplied cable with ferrite to comply with EMC values and make sure that the ferrite is on the module side.

To use the TS Module Modem outside Germany, you can fit a country-specific TAE connector onto the RJ11 connector of the phone cable. For Germany, a TAE6N connector is supplied. In some countries, telephone jacks with RJ-11 sockets are available, so that the telephone cable can be used without TAE connectors.

Specifications

- Dimensions (WHD): 30 x 100 x 75 mm
- Weight: 98 g
- ITU transmission standards:
V.21, V.22, V.22bis, V.23, V.32, V.32bis, V.34, V.34x, K56flex, V.90, V.92
- ☐ Error correction and data compression
- a/b port
- Hayes command set (AT)
- All data formats
- Dialing mode: Multifrequency signaling (DTMF), pulse dialing

National approvals

The TS Module Modem is designed so that worldwide use is possible. When installing and operating the TS Module Modem, keep to the country-specific laws and special features.

The TS module has a telecommunications approval in the following countries:

- | | | |
|-----------------|---------------|------------------|
| • Australia | • Iceland | • Poland |
| • Belgium | • Italy | • Portugal |
| • Bulgaria | • Canada | • Romania |
| • Denmark | • Latvia | • Sweden |
| • Germany | • Lithuania | • Switzerland |
| • Estonia | • Luxembourg | • Slovakia |
| • Finland | • Malta | • Slovenia |
| • France | • New Zealand | • Spain |
| • Greece | • Netherlands | • Czech Republic |
| • Great Britain | • Norway | • Hungary |
| • Ireland | • Austria | • USA |
| | | • Cyprus |

For information on approval in other countries, please contact Technical Support.

C.1.3 TS Module RS232

Product package

Designation	Article number
TS Module RS232	6ES7 972-0MS00-0XA0

Properties

The TS Module RS232 has a COM interface for connection of an external modem.

The COM interface, a 9-pin RS232 plug connector, is located behind the lower front panel.

You can operate the following devices from the COM port:

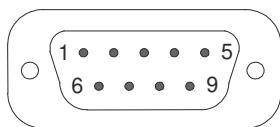
- Standard modems
- ISDN terminal adapters
- GSM wireless modems with an RS232 port

Note

The specifications relating to interference immunity and interference emission apply only when using devices, lines and connectors conforming to industrial requirements in accordance with EN 61000-6-4:2001 and EN 61000-6-2:2001.

Pin assignment and signal description of RS232 port

The RS232 plug connector has the following pin out:



Pin no.	Short description	Meaning	Input / output
1	DCD	Received signal level - the DCE reports the receipt of a carrier or the connection establishment to the DTE. ^{1, 2}	Input
2	RXD	Received data - from DCE to the DTE	Input
3	TXD	Transmit data - from DTE to DCE	Output
4	DTR	Ready to send - the DTE signals this to the DCE.	Output
5	GND	Internal reference ground	
6	DSR	Ready to operate - the DCE signals this to the DTE.	Input
7	RTS	Request to send - the DTE requests the DCE to transmit data on the data cable. The DTE waits for the CTS (ready-to-send) signal from the DCE.	Output
8	CTS	Ready to send - the DCE is able to transfer the data incoming from the DTE.	Input
9	-	-	-

Pin no.	Short description	Meaning	Input / output
Schirm	-	On connector housing	-
; ¹ DCE = data communication equipment Modem or ISDN-TA			
; ² DTE =data terminal equipment CP (or TS adapter)			

Specifications

- Dimensions (WHD): 30 x 100 x 75 mm
- Weight: 100 g
- Type of traffic: Full duplex
- Transmission mode: Asynchronous
- Signals: TXD, RXD, DSR, CTS, RTS, DTR, DCD
- Transmission speed: 2400...115200 bps
- Frame format: 8 data bits (LSB first), no parity bit, 1 stop bit
- Standard: RS-232
- D-sub male connector: 9-pin, male (PC COMx)

C.2 Modems and routers

C.2.1 IP-based routers

Routers for IP-based communication

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

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

Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15982>)

Siemens Industry Mall at:

Link: (<https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10215915?tree=CatalogTree>)

C.2.2 Dedicated line and dialup network modems

Modems for dedicated line and dialup networks

Note**Discontinuation of modules**

The following products have the product status "type discontinued" but if they exist can be operated with the communications module:

- Modem MD2
Dedicated line modems
Product notification on the Internet:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/109740149>)
 - Modem MD3
Modems for analog dialup networks
Product notification on the Internet:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/109740148>)
 - Modem MD4
Modems for ISDN networks
Product notification on the Internet:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/67637816>)
-

When using the serial interface for dedicated line and dialup networks, use suitable products of other vendors.

C.2.3 MODEM MD720

MODEM MD720

Article number: 6NH9720-3AA01-0XX0



Figure C-3 MODEM MD720

Use of the MD720

The MD720 is a GPRS/GSM modem for industrial applications.

It is intended for use in SIMATIC S7 stations that are part of a telecontrol or remote maintenance system and for communication with other stations in the network or an OPC server in the master station. Depending on the configuration, the control center can be either TeleControl Server Basic, SINAUT ST7cc, SINAUT ST7sc or SINAUT MICRO SC.

The MD720 supports the following types of communication:

- IP-based communication with the control center using GPRS and the MSC protocol or the MSCsec secure protocol
- SMS messages from or to a mobile telephone
- CSD communication for maintenance and for data connections

Current manual version and further information on the Internet

You will find the current version of the manual and further information (e.g. FAQs) on the following Internet page of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21820/man>)

Accessories

For the antenna, refer to the section Antennas (Page 162).

Communications functions

The MD720 supports the following functions:

- **Modes**

The MD720 is set to one of the following two modes depending on the type of communication required:

- OPC mode
- Terminal mode

- **OPC mode**

In OPC mode, there is productive data exchange with the control center using GPRS.

- **Terminal mode**

In terminal mode, the MD720 uses CSD communication for the following functions:

- Sending and receiving SMS messages
- Diagnostics and maintenance functions
- Transfer of configuration data

- **Communication with a control center**

In OPC mode, an MD720 connected to an S7 station communicates with a control center via a TCP connection. For the data transfer, the GSM network is used with the GPRS service. Either the MSC protocol or the MSCsec protocol is used (see below).

- **Sending and receiving SMS messages**

The locally connected application (SIMATIC) can transfer data for an SMS message to the MD720 using AT commands. The MD720 sends the SMS message to a subscriber in the GSM network (mobile wireless telephone) or when using a gateway, to a remote fax machine. SMS messages received by the MD720 can be queried by the local application using AT commands.

- **CSD communication**

Service data calls via remote connections in CSD format are used for the following purposes:

- Remote configuration of the MD720
- Diagnostics and maintenance functions using AT commands
- Process data connections between stations with TIM module or CP 1243-8 IRC

The partner for the remote connection can be an analog modem, an ISDN modem or a GSM modem.

- **Controlling the MD720 using AT commands**

You can control the MD720 from a locally connected application or manually with a terminal program connected locally.

- **MSC protocol**
Proprietary protocol used for productive communication via TCP connections in OPC mode. The protocol allows authentication of the communications partner and simple encryption. The MSC protocol is supported by the following control center applications:
 - TeleControl Server Basic (TCSB)
 - SINAUT MICRO SC
- **MSCsec protocol**
Proprietary protocol used for productive communication via TCP connections in OPC mode. In addition to the MSC protocol, it also allows authentication of the messages using an HMAC with the help of a symmetrical encryption method (with pre-shared key). The MSCsec protocol is supported by the following control center applications:
 - TeleControl Server Basic (TCSB)

SIMATIC S7 systems that can be connected locally

The following SIMATIC S7 systems can be connected to the GSM network via the MD720:

- SIMATIC S7- 200 via SINAUT PPI modem cable (6NH9701-0AD)
- SIMATIC S7-1200 via CP 1243-8 IRC / TS Module RS232
- SIMATIC S7- 300 via Ethernet TIM module (using GPRS)
- SIMATIC S7- 400 via TIM 4R IE (using GPRS)
- SIMATIC S7-300/400 via classic or Ethernet TIM module (only using CSD)

For project-specific solutions for connecting a SIMATIC S7-300 to the GSM network, please contact Siemens Industry Online Support. You will find an examples of applications with the corresponding documentation on the following Internet page:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21820/ae>)

Possible partners of the MD720

The MD720 can communicate with the following partners.

- **Communications partners of the MD720 installed in an S7-200:**
 - PC with TeleControl Server Basic (TCSB)
 - PC with SINAUT MICRO SC
 - S7-200 with MD720 (inter-station communication)
The frames are forwarded by TCSB or SINAUT MICRO SC in the master station.

The MD720 operates in OPC mode.
- **Communications partners of the MD720 installed in an S7-300/400:**
 - Station with Ethernet TIM (e.g. central CPU or control system SINAUT ST7cc/ST7sc)

The MD720 operates in OPC mode.

- **Communications partners of the MD720 for SMS messages:**

- Mobile phone
- Fax machine (when using a gateway)

The MD720 operates in terminal mode.

- **Communications partners of the MD720 installed in an S7-200:**

- Engineering station with STEP 7-Micro/WIN
(via GSM network, ISDN network, analog dial-up network)

The MD720 operates in terminal mode.

- **Communications partners of the MD720 installed in an S7-300/400 with TIM:**

- SIMATIC S7-300/400 with TIM module (including classic)
(via GSM network, ISDN network, analog dial-up network)

The MD720 operates in terminal mode.

Connection resources

- **Active connections at runtime**

At runtime, the MD720 can connect to 1 communications partner.
The connection partner is configured in the program blocks.

Technical specifications (excerpt)

Connection to Industrial Ethernet		
X1 interface	Number:	1
	Implementation:	D-sub 9-pin, female
	Characteristics:	RS-232 Control using AT commands
	Transmission speed:	19200 bps Permitted range: 300 ... 57600 bps
Wireless interface		
Antenna connector	Number:	1
	Implementation:	SMA socket
	Impedance:	50 Ω nominal
Frequency bands	GPRS / CSD:	Quad band: 850, 900, 1800, 1900 MHz
GPRS	Characteristics:	Maximum of 5 time slots at the same time, of which: • Up to 2 uplinks • Up to 4 downlinks
	Transmission speed • Uplink (modem → Internet) • Downlink (Internet → modem)	Gross values: • Max. 42 kbps • Max. 54 kbps The net values (user data) are approximately 30% lower.

CSD	Characteristics:	MTC (Mobile Terminated Call)
	Transmission speed:	9600 bps
SMS (TX)	Characteristics:	Text mode

C.3 Antennas

The following antennas are available for use in mobile wireless networks and can be installed both indoors and outdoors. The antennas must be ordered separately.

Antenna ANT794-4MR



Figure C-4 Antenna ANT794-4MR

Short name	Order no.	Explanation
ANT794-4MR	6NH9 860-1AA00	Omnidirectional antenna for LTE networks (4G), GSM networks (2G) and UMTS networks (3G); weather-proof for indoor and outdoor areas; 5 m connecting cable connected permanently to the antenna, SMA connector, including installation bracket, screws, wall plugs.

You will find detailed information in the documentation of the device. You will find this on the Internet on the pages of Siemens Industrial Automation Customer Support under the following entry ID:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/23119005>)

Flat antenna ANT794-3M



Figure C-5 Flat antenna ANT794-3M

Short name	Order no.	Explanation
ANT794-3M	6NH9 870-1AA00	Flat antenna for GSM networks (2G), for tri-band 900 / 1800 / 1900 MHz; weatherproof for indoor and outdoor areas; 1.2 m connecting cable connected permanently to the antenna; SMA connector, including adhesive mounting tape.

You will find detailed information in the documentation of the device. You will find this on the Internet on the pages of Siemens Industrial Automation Customer Support under the following entry ID:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/48729835>)

C.4 Connecting cables

C.4.1 Connecting cables for connecting the CP to Ethernet

Connecting cables for connecting to Ethernet

For the Ethernet attachment of the TIM 4RIE DNP3, you can use a standard Ethernet connecting cable (for example IE TP Cord) from the SIMATIC NET product range (catalog IK PI).

The cable must be suitable for the 10Base-TX or 100Base-TX Ethernet specification.

If the CP is connected to a switch or router, it is advisable to use fully shielded straight-through patch cables with RJ-45 connectors at both ends and 1:1 pin assignment. The cable must be suitable for the 10Base-TX or 100Base-TX Ethernet specification.

You can also use a crossover patch cable with RJ-45 connectors at both ends and the following pin assignment:

Signal / pin no.	Interconnection	Pin no. /signal
TXD (+) 1		1 TXD (+)
TXD (-) 2		2 TXD (-)
RXD (+) 3		3 RXD (+)
4		4
5		5
RXD (-) 6		6 RXD (-)
7		7
8		8

Figure C-6 Pinout of a crossover Ethernet RJ-45 cable

C.4.2 Connecting cables for connecting the modem of the TS Module RS232

Connecting cables for connecting the TS Module RS232 to a modem

A modem or other transmission device can be connected to the 9-pin D-sub connector of the of the RS-232 interface of the TS module.

The following standard connecting cables are available for connection to this D-sub connector.

Table C-1 Connectable standard cables for the RS-232 interface of the TS Module RS232

Order no.	Description	Illustration
6NH7701-4AL	Cable for connecting the TS module with one of the SINAUT ST7 modems MD2, MD3 or MD4 (RS-232) Cable length 1.5 m	
6NH7701-5AN	Cable for connecting the TS module to the GSM modem MD720 (RS-232). Also suitable for third-party modems or wireless devices with a standard RS-232 interface. Cable length 2.5 m	
6NH7701-4BN	Cable with one end without connector for connecting the TS module (RS-232) to a third-party modem or wireless device (RS-232) Cable length 2.5 m	

The following figures show the assembly of the connecting cables.

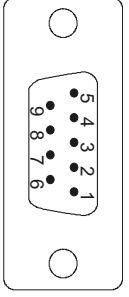
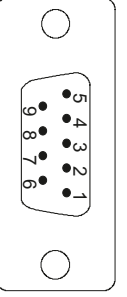
TS Module (RS-232)	Pin no.	Interconnection	Pin no.	Modem MDx (RS-232)
 D-sub socket 9-pin	Housing shield		Housing shield	 D-sub socket 9-pin
	1	DCD	1	
	2	RXD	2	
	3	TXD	3	
	4	DTR	4	
	5	GND	5	
	6	DSR	6	
	7	RTS	7	
	8	CTS	8	
	9	RI / T	9	

Figure C-7 Assembly of the standard connecting cable 6NH7701-4AL

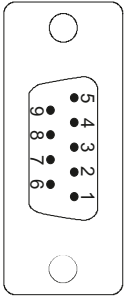
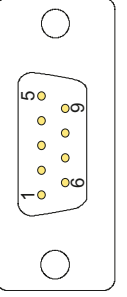
TS Module (RS-232)	Pin no.	Interconnection	Pin no.	MODEM MD720 (RS-232)
 D-sub socket 9-pin	Housing shield		Housing shield	 D-sub socket 9-pin
	1	DCD	1	
	2	RXD	2	
	3	TXD	3	
	4	DTR	4	
	5	GND	5	
	6	DSR	6	
	7	RTS	7	
	8	CTS	8	
	9	RI / T	9	

Figure C-8 Assembly of the standard connecting cable 6NH7701-5AN

C.4 Connecting cables

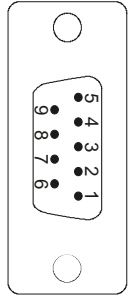
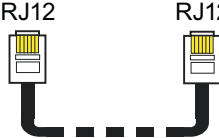
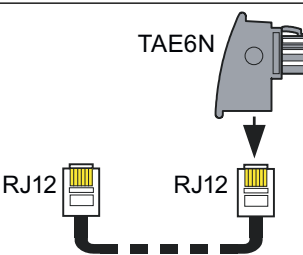
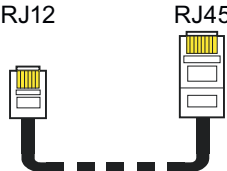
TS Module (RS-232)	Pin no.	Interconnection	Pin no.	Open cable end
	Housing shield		Housing shield	
	1	DCD	1	white
	2	RXD	2	brown
	3	TXD	3	green
	4	DTR	4	yellow
	5	GND	5	gray
	6	DSR	6	pink
	7	RTS	7	blue
	8	CTS	8	red
	9	RI / T	9	black

Figure C-9 Assembly of the standard connecting cable 6NH7701-4BN

C.4.3 Connecting cables of the MDx modem

With every MDx modem, a 6NH7700-xxx connecting cable was supplied for connecting the modem to the WAN network.

Table C-2 Cables for the WAN connection of the modems

Order no.	Description	Illustration
6NH7700-2AR60	Connecting cable with 2 x RJ-12 plugs for connection to an MD2 modem (RJ-12) with an LTOP overvoltage protection module (RJ-12). Cable length 6 m The adapter cable is no longer available as separate spare part.	
6NH7700-3BR60	Connecting cable with 2 x RJ-12 Western plug and snap-on TAE6N plug to connect an MD3 modem (RJ-12) to a telephone jack (TAE6N) or an LTOP overvoltage protection module (RJ-12) if the MD3 modem is being operated as a dedicated line modem. Cable length 6 m The adapter cable is no longer available as separate spare part.	
6NH7700-4AR60	Connecting cable with RJ-12 and RJ-45 plug to connect an MD4 modem (RJ-12) with an ISDN-S ₀ jack (RJ-45). Cable length 6 m The adapter cable is no longer available as separate spare part.	

C.4.4 Accessories for RS-485 connection

Accessories for RS-485 operation of the serial interface

- **Cable**
Excerpt from the Siemens accessories program PROFIBUS or RS-485 operation
 - PROFIBUS FC standard cable GP, bus cable 2-wire, shielded, special design for fast installation, sold by the meter
02YSY (ST) CY, 1x2x0.64 / 2.55-150 VI KF 40 FR
Article number: 6XV1830-0EH10
- **Terminating resistor**
In a network in RS-485 operation, the terminating resistor of the bus cable is turned on or off by the STEP 7 configuration of the communications module.
- **Connector**
Use D-sub connectors with metal or metallized enclosure to comply with the EMC guidelines.

Connector assignment in RS-485 operation

Observe the connector assignment specified by the modem manufacturer.

When the serial interface is connected to a Siemens modem MDx in RS-485 operation, the following assignment applies:

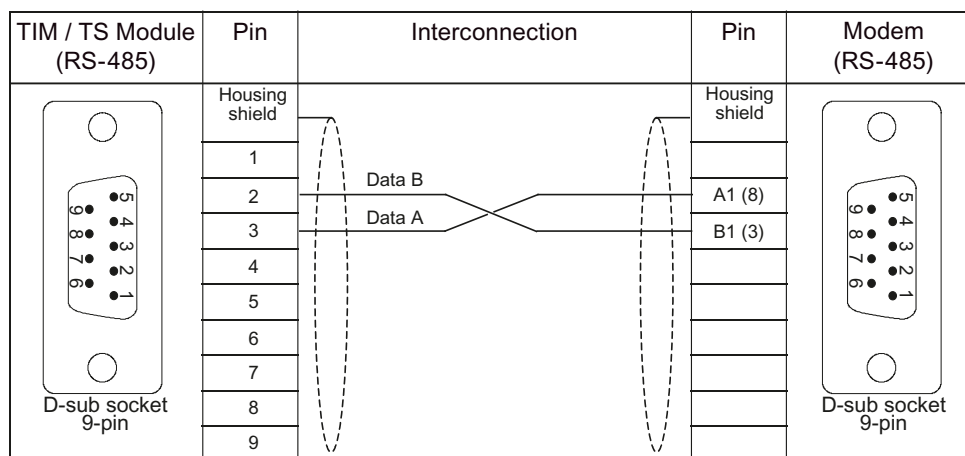


Figure C-10 Assignment of the RS-485 interfaces of the TIM 1531 IRC and an MDx modem

Encryption methods (Ciphers)

The following table lists the encryption methods (ciphers) used by the CP.

The specifications are valid for the CPU in the firmware version specified in the preface.

Meaning of the table columns

- **Category**
 - Cipher: Cipher suite (cryptographical method)
 - Group: ECC group (NamedGroup), IKE DH group or group parameter
 - SEA: Signature and encryption algorithm
 - DSA: Signature algorithm
 - KeyX: Key file
 - CM: Encryption method/mode
 - HA: Hash algorithm
- **Name**

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

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

TLS version with which the respective category is used.

- **Security**

- ✓
Ciphers considered secure
- Legacy
Ciphers no longer considered secure

- **Protocol**

The numbers indicate the communication protocols that use the respective category.

- 1: Telecontrol communication
 - DNP3 (TCP 19999, configurable)
 - IEC 60870-5-104 (TCP 19998, configurable)
- 2: HTTPS (TCP 443)
- 3: SMTP client (TCP 587) / Secure OUC client (TCP 2001) / openVPN client (UDP 1194) / SINEMA RC client (TCP 4443)
- 4: S7 communication (TCP 102), no security
- 5: SNMPv3 server (UDP 161)
- 6: STEP 7 security diagnostics (TCP 8448)
- 7: Secure OUC server (TCP 2000)
- 8: IPsec client/server (UDP 500)

TLS versions used by the CP

TLS version	Security
TLS Version 1.2	✓
TLS Version 1.3	✓

Ciphers used by the CP

Category	Name	Value	TLS	Security	Protocol
Cipher	TLS_AES_128_GCM_SHA256	0x13,0x01	TLS 1.3	✓	1, 3, 6, 7
Cipher	TLS_AES_256_GCM_SHA384	0x13,0x02	TLS 1.3	✓	1, 3, 6, 7
Cipher	TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS 1.3	✓	1, 3, 6, 7
Cipher	TLS_AES_128_CCM_SHA256	0x13,0x04	TLS 1.3	✓	1, 3, 6, 7
Cipher	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	0x00,0xA2	TLS 1.3	✓	1, 3
Cipher	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	0x00,0xA3	TLS 1.3	✓	1, 3
Cipher	TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x9E	≤ TLS 1.3	✓	1, 3, 6
Cipher	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9E	≤ TLS 1.3	✓	1, 3, 6
Cipher	TLS_DHE_RSA_WITH_AES_256_CCM	0xC0,0x9F	≤ TLS 1.3	✓	1, 3, 6
Cipher	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9F	≤ TLS 1.3	✓	1, 3, 6
Cipher	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xAA	≤ TLS 1.3	✓	1, 3, 6
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xC0,0xAC	≤ TLS 1.3	✓	1, 3
Cipher	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xC0,0x2B	≤ TLS 1.3	✓	1, 2, 3

Category	Name	Value	TLS	Security	Protocol
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xC0,0xAD	≤ TLS 1.3	✓	1, 3
Cipher	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xC0,0x2C	≤ TLS 1.3	✓	1, 2, 3
Cipher	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA9	≤ TLS 1.3	✓	1, 2, 3
Cipher	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC0,0x2F	≤ TLS 1.3	✓	1, 2, 3, 6, 7
Cipher	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC0,0x30	≤ TLS 1.3	✓	1, 2, 3, 6, 7
Cipher	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xCC,0xA8	≤ TLS 1.3	✓	1, 3, 6, 7
Group	X25519	0x001D		✓	1, 2, 3, 6, 7
Group	X448	0x001E		✓	1, 2, 3, 6, 7
Group	secp256r1 (prime256v1)	0x0017		✓	1, 2, 3, 6, 7
Group	secp384r1	0x0018		✓	1, 2, 3, 6, 7
Group	secp521r1	0x0019		✓	1, 2, 3, 6, 7
Group	modp768 (Group 1)			Legacy	8
Group	modp1024 (Group 2)			Legacy	8
Group	modp1536 (Group 5)			✓	8
Group	modp2048 (Group 14)			✓	8
Group	modp3072 (Group 15)			✓	8
Group	modp4096 (Group 16)			✓	8
Group	modp8192 (Group 18)			✓	8
Group	ffdhe3072	0x0101		✓	1, 3
SEA	ed25519	0x0807		✓	1, 3, 4
SEA	ed448	0x0808		✓	1, 3
SEA	sha256+rsaepss	0x0804		✓	1, 2, 3
SEA	sha384+rsaepss	0x0805		✓	1, 2, 3
SEA	sha512+rsaepss	0x0806		✓	1, 2, 3
SEA	sha256+rsapss	0x0809		✓	1, 3
SEA	sha384+rsapss	0x080A		✓	1, 3
SEA	sha512+rsapss	0x080B		✓	1, 3
SEA	hmac-MD5-96			Legacy	5
SEA	hmac-SHA-1			Legacy	8
SEA	hmac-SHA-96			Legacy	5
SEA	hmac-SHA256			Legacy	8
SEA	hmac-SHA384			✓	8
SEA	hmac-SHA512			✓	8
DSA	sha256+rsa	0x0401		✓	1, 2, 3
DSA	sha384+rsa	0x0501		✓	1, 3, 6
DSA	sha512+rsa	0x0601		✓	1, 3, 7
DSA	sha256+dsa	0x0402		✓	1, 3
DSA	sha384+dsa	0x0502		✓	1, 3
DSA	sha512+dsa	0x0602		✓	1, 3
DSA	sha256+ecdsa	0x0403		✓	1, 2, 3
DSA	sha384+ecdsa	0x0503		✓	1, 3
DSA	sha512+ecdsa	0x0603		✓	1, 3

Category	Name	Value	TLS	Security	Protocol
KeyX	ECDH $\geq$ 250 bit			✓	2
KeyX	DH, RSA $\geq$ 3000 bit			✓	2
CM	aes128-ctr			✓	8
CM	aes192-ctr			✓	8
CM	aes256-ctr			✓	8
CM	aes128-CCM			✓	8
CM	aes192-CCM			✓	8
CM	aes256-CCM			✓	8
CM	aes128-CBC			✓	5, 8
CM	aes192-CBC			✓	8
CM	aes256-CBC			✓	8
CM	aes128-GCM			✓	8
CM	aes192-GCM			✓	8
CM	aes256-GCM			✓	8
CM	3des-168-CBC			Legacy	8
CM	des			Legacy	8
CM	des-CBC			Legacy	5
HA	SHA1			Legacy	8
HA	MD5			Legacy	8
HA	SHA256			Legacy	8
HA	SHA384			Legacy	8
HA	SHA512			✓	8

Documentation references

Where to find Siemens documentation

- Article numbers
You will find the article numbers for the Siemens products of relevance here in the following catalogs:
 - SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI
 - SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70
 You can request the catalogs and additional information from your Siemens representative. You will also find the product information in the Siemens Industry Mall at the following address:
Link: (<https://mall.industry.siemens.com>)
- Manuals on the Internet
You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15247/man>)
Go to the required product in the product tree and make the following settings:
Entry type "Manuals"
- Manuals on the data medium
You will find manuals of SIMATIC NET products on the data medium that ships with many of the SIMATIC NET products.

E.1 /1/ S7-1200 system manual

SIMATIC
S7-1200 Automation System
system manual
Siemens AG
Link: (<http://support.automation.siemens.com/WW/view/en/34612486>)

E.2 /2/ CP 1243-8 IRC

SIMATIC NET
CP 1243-8 IRC
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21162/man>)

E.3 /3/ SINAUT ST7 system manual

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

E.4 /4/ TeleControl configuration manuals

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>)

E.5 /5/ SCALANCE M812/M816

SIMATIC NET
SCALANCE M812, M816
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15984>)

E.6 /6/ SCALANCE M874/M876

SIMATIC NET
SCALANCE M874/M876
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15987/man>)

E.7 /7/ SCALANCE S

SIMATIC NET
Industrial Ethernet Security
SCALANCE S
Commissioning and Installation Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15327/man>)

E.8 /8/ TS Adapter

SIMATIC
TS Adapter modular
Device Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/16006>)

E.9 /9/ SNMP

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

Index

A

Abbreviations/acronyms, 4
Article number, 3
Authentication, 16

C

CLOUDCONNECT, 90
Compatibility
 V1.0 - V1.1, 106
Connection abort, 109
Connection resources, 23, 161
Cross-references (PDF), 6

D

Data buffering, 24, 118
Data transmission (cloud), 101
Dimensions, 42
Direct communication, 15
Disposal, 8
DNS server - program-controlled change, 126

E

E-mail
 Configuration, 82
 Number of messages, 24
 Programming (OUC), 123
Encryption, 16
ES - engineering station, 21
Ethernet interface
 Assignment, 141

F

Firewall, 22
Firmware version, 3
Frame memory, 24

G

Gateway (VPN), 73
Glossary, 8

H

Hardware version, 3

I

Importing a certificate - e-mail, 78
Instructions (OUC), 123
Inter-station communication, 15, 160
IP address - fixed, 60, 70
IP address - program-controlled change, 126
IP configuration, 20
IP_CONF_V4, 126
IPsec, 24

L

Logging server, 81

M

MAC address, 3
MIB, 134
MSC, 16
MSCsec, 16

N

NTP server - program-controlled change, 126
NTP (secure), 56

O

Online diagnostics, 130
Online functions, 21, 54, 131
Operating statuses (LED displays), 31
OUC (Open User Communication), 123

P

Passive VPN connection establishment, 73
PG/OP connections, 24
Port 8448, 133
Program blocks, 18

PUT/GET

Enable in CPU, 18

Q

QoS, 118

QualityCode, 109

R

Recycling, 8

Replacing a module, 138

RS-485

Cable, 167

S

S7 connections

Resources, 23

S7 systems, connectable, 160

Safety notices, 37

Security, 22

Security diagnostics, 133

Send buffer, 24

Service & Support, 8

SIMATIC NET glossary, 8

SIMATIC PCS 7, 14

SINAUT system, 13

SINAUT ST7cc, 14

SMS

Number of messages, 24

Programming (OUC), 123

SMTPS, 77

SNMP, 21, 65, 134

SNMPv3, 23, 76

SSL/TLS, 77

ST7sc, 14

STARTTLS, 77

STEP 7

Version, 25

STEP 7 V5, 14

SYSLOG, 73

T

T_CONFIG, 126

TC_CONFIG, 126

TIM 3V-IE Advanced, 13

Time-of-day synchronization, 20

Training, 8

U

Uninstalling, 47

V

VPN, 24, 69

W

Web server, 62

Diagnostics data, 132

WinCC TC, 14